International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Risk Analysis on Industrial Internet of Things (Iiot) Integration with Enterprise Resource Planning(ERP) Inmanufacturing

Jose S, Vincent Herald Wilson

Abstract: ***At the onset of liberalization, privatization and globalization, enterprise resource planning has become an integrated part of any business. It has become imperative for businesses to go in for IIoT. With implementation of IIoT and analytics companies can become more profitable and productivity can increase constantly. With this comes the risk of data security in ERP due to real time capturing huge volume of data in manufacturing plants, which are under security risk. This has forced the companies to implement measures to ensure that the product design and customer data are stored securely without compromising on business. This paper presents the possible sources of risk in IIoT and presents the solutions for preventing the risk.***

Key words: Industrial Internet of Things, ERP, Manufacturing, risk analysis

I. INTRODUCTION

The Industrial Internet of things (IIoT) is a nascent technology where every product is at the testing stage. It is mandatory to understand the impact of IIoTon the economics of manufacturing industries. As manufacturing incorporates planning, execution and observing of movement of products, and inventory, implementation of IIoT in every area is to be monitored effectively. Another key region in the business is Supply Chain Management (SCM) which includes development and stacking of materials required for production and completed items moving from one location to the next. Both in hardcoremanufacturingandsupplychainmanagement IIoT and ERP have become an integral part and the securityof data is a major concern for every player in manufacturing sector. It is of paramount importance to know and deal with metaphoricallandminesandpittrapstoavoidanydatalossand breach of data. In business huge data is to be stored, received, transmitted and analysed. Similarly, different data formatsuchas pictures, drawings, texts, audio and video files are to be stored securely. Information technology plays an effective role in the implementation of successful and smart SCM. (Ross D. F 2016). Systems are expected to exchange information and assist in decision making in manufacturing industries. More than increasing productivity the systems are expected to be integrated and work to gether.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Jose S*, Professor and Associate Dean,VIT Business School,Vellore, Tamil Nadu,India. Email: assodean.vitbs@vit.ac.in.
Vincent Herald Wilson, School of Mechanical Engineering,Vellore Institute of Technology, Vellore, Tamil Nadu,India. Email: vincent.wilson@vit.ac.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

It is noticed that in many scenario in tegration fails, making it difficult for thes take holders to have right access to data, and to have a holistic picture to make appropriate decisions. Hitherto ERP helped the industries to host important data, to interpret and analyze for their sustainability.

In most of these industries ERP is used for critical planning and decision making. ERP also helps in implementing an effective supply chain management. However in data capture, due to human error or manipulation/suppression of data ERP may fail to project the real picture to the stakeholders. In standalone ERP system manipulation of data is possible and it is necessary to address this issue to stand in global competition. Fig 1 explains the necessity to have a smart supply chain management to overcome challenges in traditional SCM Error in manual data entering leads to loss in business and this could be overcome by the integration of ERP with IIoT. IIoT represents the objects networked together to communicate among themselves. Figure 2 presents the IIoT enablers in a typical ERP Enabled system. All the functions of the manufacturing unit including, like R&D, Sourcing, production, logistics, marketing, are connected to sensors, RFID, and smart devices by implementing an effective ERP system. On the flip side communication between objects need careful monitoring by human workforce. As the whole data of the company is captured and is available for all the stake holders, so extracare should be exercised to keep the data safe and make itavailable only to the respective stakeholders. As a part of the manufacturing industry SCM provides the complete flow ofinformation from the supplier to customer and also announces the time of arrival of goods. Ending inventory is equal to the beginning inventory + receipt of goods (in) – shipments (out). SCM provides the current information about the location, status and condition of the materials. A severe competitive environment is created due to globalization. It hordes the flow of business via supply chain because firmsarenotindividuallyself-adequate.Thesechains should synchronize their processes to convert them to be more competitive and achieve anticipated objectives of various partners in an industry (SC council 2012). Review of available literature on supply chain management, ERP and IIoT gives a clear picture projecting the necessity of tighter security measures to ensure safe business in a highly competitive environment.

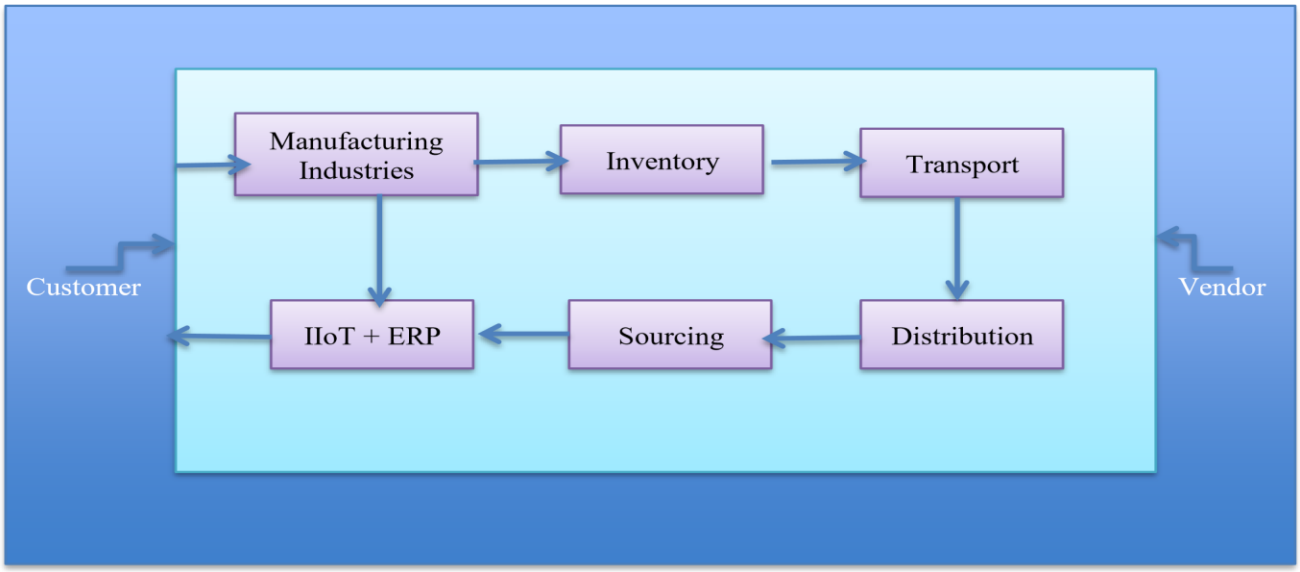

Fig. 1: Smart SCM

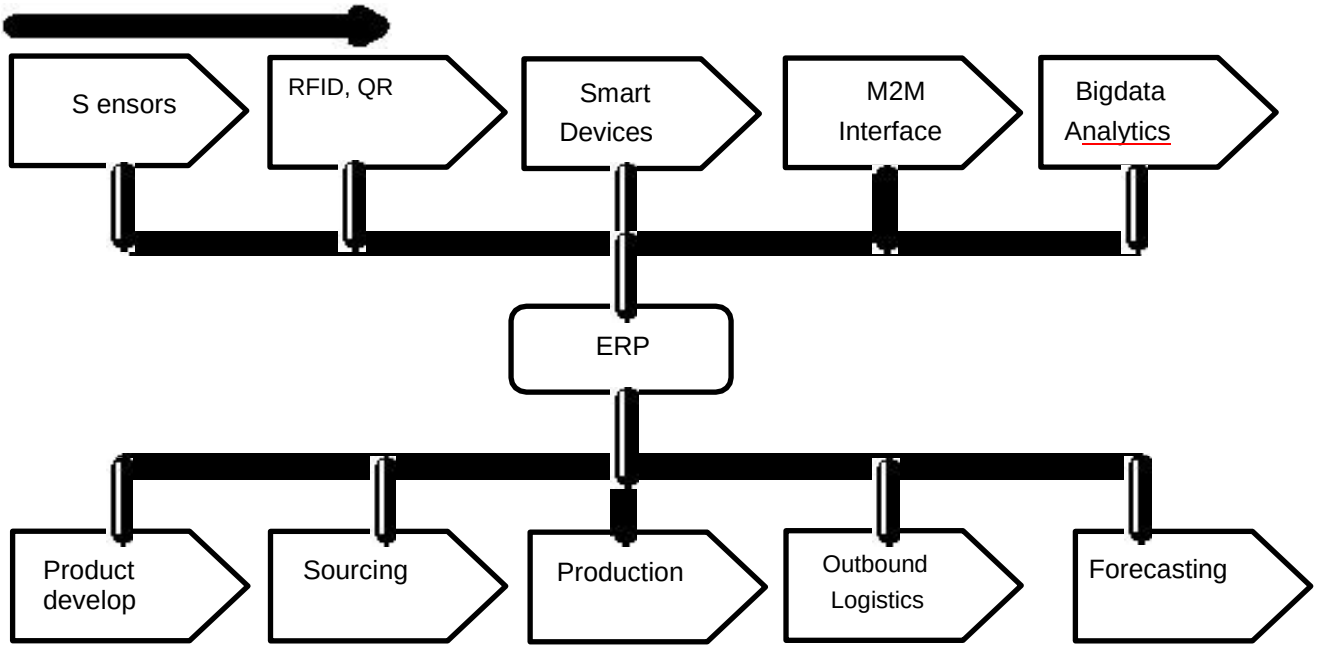

Fig. 2: IIoT Enablers

II. REVIEW OFLITERATURE

ERP and IIoT are here to stay, especially in manufacturing industries. Effect of the selatest technologies and especially the effect of IIo Ton smart SCM are not yet fully made available to the stake holders. Using RFID technology, mobile networks, interfacing devices and sensors make the entire industry vulnerable to attacks and data breach if the system is not thoroughly secured (Borgia,2014, S.Yuvaraj, M Sangeetha 2016, Petar Radanliev, et al 2018) Kinnunen et al (2016), in their research have published that the industrial internet of things with respect to data acquisition helps in managing industrial assets by developing a secure platform for safe operations. Many authors have agreed that major enablers in IIo Tandsmart supply chainare RFID and sensors.Ding Zhang et al (2018) have presented that information network can be connected via routers operating based computers and devices to build intelligent systems that would make interoperability a reality. The technologies which can be developed by IIoT applications, relevant to SCM make processes more effective and increase the visibility of products (T. Wang et al., 2016), management of innovative production networks as presented by Veza et al (2015), and smart intelligent design and production control (P.Zawadski., 2016) make the whole manufacturing process effective and efficient. How ever these technologies expose the industries to risk and security issues if data is not secured thoroughly at every stage of operation. A smart SCM helps in facilitating data collection process. This information will be shared between the agencies that supply the raw material and managers effectively using microchip Wi-fi module. Even though this system increases transparency inthe operations it increases the risk of insecurity in vital information. In the next stage, based on the input collected, after analyzing suppliers' goods and choosing the best, the process to procure material will be carried out.

After this process, as marttransporthas to be made a vailable for effective functioning, and the matter of paramount importance is data security and avoiding attacks on central distribution system. Both internal and external systems should be kept safe and secure to safeguard the business. Hugh Boyeset al., (2018) have brought up that in traditional computerized systems a zoned design was embraced and firewalls used to ensure the center control parts. But with the advent of IIoTand industry
4.0 these security layers are exposed and the manufacturing sector will be subjected to attacks if not secured properly with threat proof devices. Also it is necessary to have a control to record the interactions between human and machines and machine with machine and have control over that. Integration of operation technology with information and communication technology is not well known to many users thereby exposing sensitive gadgets and data to attacks and making the whole system vulnerable. Figure 3 presents the enhanced security measures introduced in a manufacturing setup.

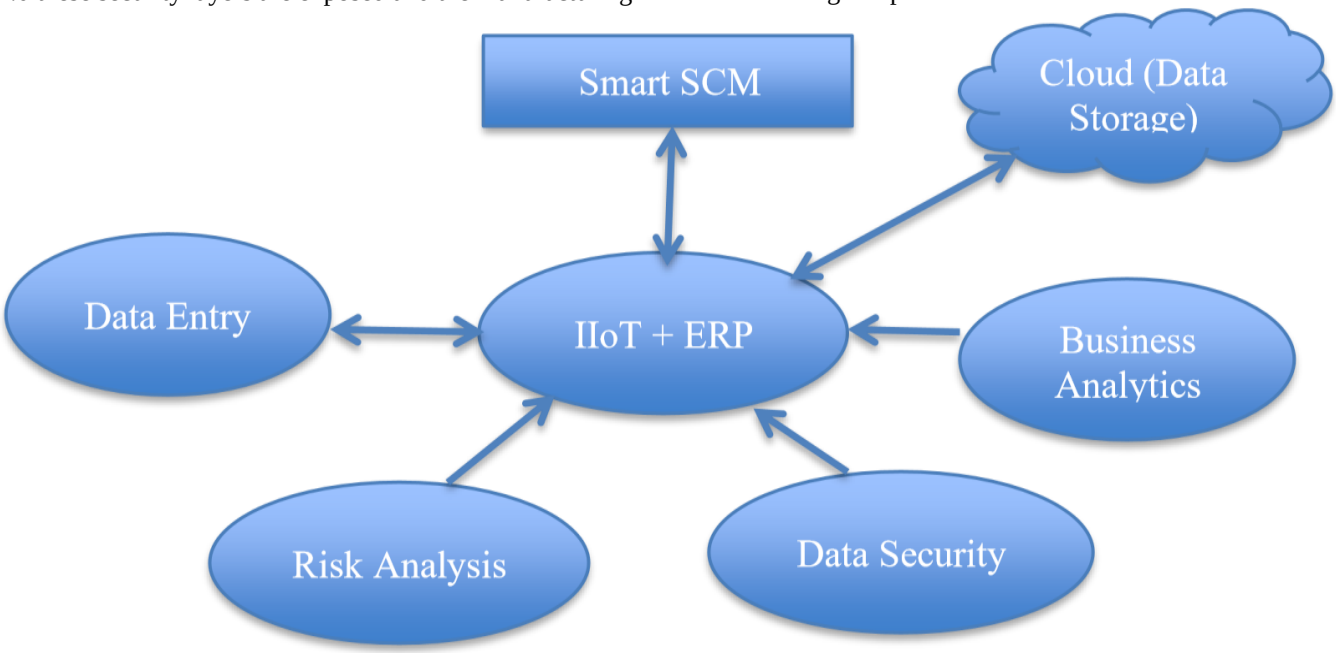

Fig 3: Security Enhanced using IIoT& ERP in Manufacturing Industries

III. RISKS INVOLVED IN INTEGRATION OF IIOT WITH ERP

Risks involved in integration of IIoT with ERP and proposed solution in two industries If the manufacturing industries have to keep track of all data generated by company and rely on external parties for storage and retrieval of data, probability of security breachis more. A study on avoiding the internet of insecure industrial things (Lachlan et al., 2018) points out that the depth of penetration of attacks on IIoT enabled system may be very deep and if it is not noticed at the early instance revival of business under attack may be bleak. It is also pointed out that there is always a possibility of a competitor sabotaging the system to obtain commercial intelligence about a new product/process and cause down time. Another possibility is organized criminal groups hacking into industrial systems to get trade secrets, intellectual properties, etc for business advantages or to sell to the competitors. In the plant 1 exhibited in figure 4 with its manufacturing facility in a remote spot and the conveyance framework spread over the world, it is fundamental for the organization to monitor all information produced. Depending intensely on a customer server brought together model to recognize, approve and convey between various IIoT hubs in a system, loses unwavering quality when there is a failure in one solitary point. To handle the huge information and various gadgets a decentralized engineering including Peer to Peer (P2P) correspondence utilizing IPFS to store and provide complete and safe information is proposed. Risks involving sensors is another area to be addressed. Data management, the costs involved to store, study and utilize that data, costs involved to funnel down the data to the required level of the ERP system and fine tune the data that is generated with respect to time also needs to be studied and addressed to enable a safer environment for manufacturing industries. IPFS helps in improving the security of the huge data that available by integrating IIoT with ERP. Single Page Applications (SPA) using developing frame works such as Angular, React and Node JS help in reducing therisk.

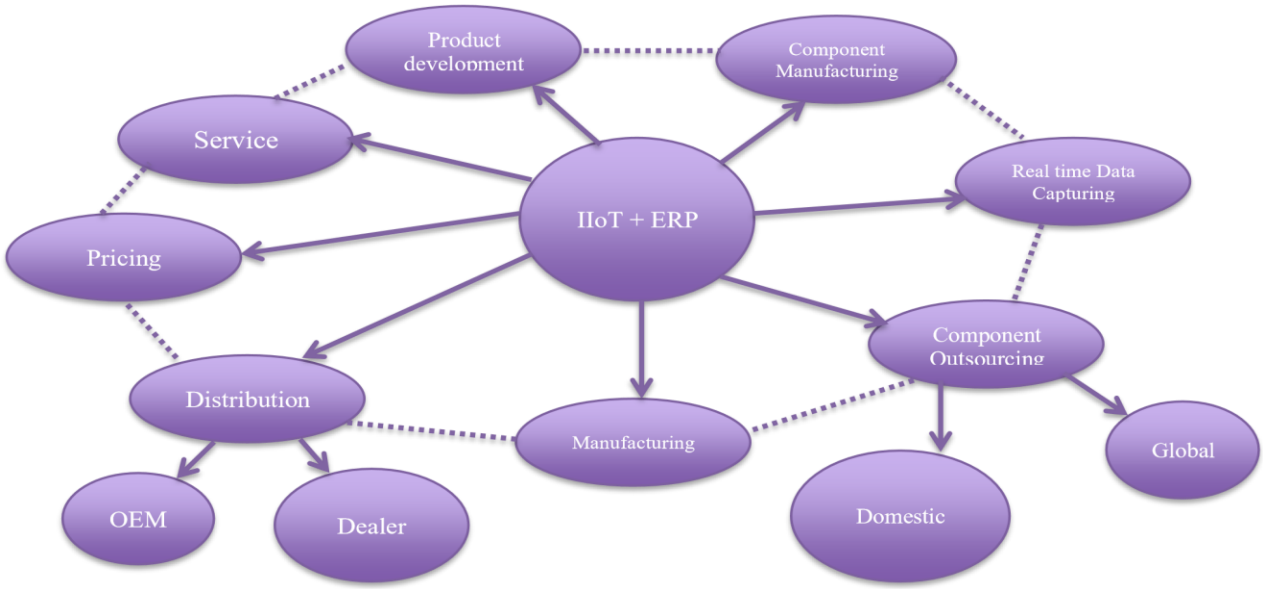

Fig. 4: IIoT enabled Manufacturing value Chain

Another method for overcoming security issues is to utilize encryption standard cryptography. It utilizes a solitary key called symmetric key created by AES calculation. Number of such keys are made and circulated among nodes statically to avoid the requirement for authorization of security. Each time a correspondence happens between different nodes, encryption at getting side and decoding at target side happen utilizing the key provided securely (Vinay 2019). "Big data analytics" are driving extra productivity in the manufacturing unit with the utilization of simulation methods to the officially generated enormous volume of information n that the business creates.The usage of the "IIoT" is likewise enabling producers to utilize continuous information from sensors to track parts, screen hardware, and guide real tasks. For manufacturing industries, openings empowered by enormous information can drive profitability by improving effectiveness and the quality of items produced. Diminishing pointless emphasis in item production cycles helps in improving the value chain there by increasing efficiency. The genuine yield estimation of items is expanded by improving their quality and making items that better match clients' needs.

Some of the most powerful impacts of big data apply across entire manufacturing ecosystems. Big data plays a pivotal role in ensuring that these ecosystem webs function well and continue to evolve. Indeed, new data intermediaries or data businesses could begin to emerge. They could, for example, capital izeon the economic value of data that describes the flow of goods around the world. Figure 5 presents the case of the second manufacturing plant under study to increase the security of huge data collected. While securing data and introducing various technologies, it is also necessary to bring in the cost involved in implementation. As the margin of profit is limited in these industries it is necessary to work outaviable solution, and at the same time not compromising on security of vital data.

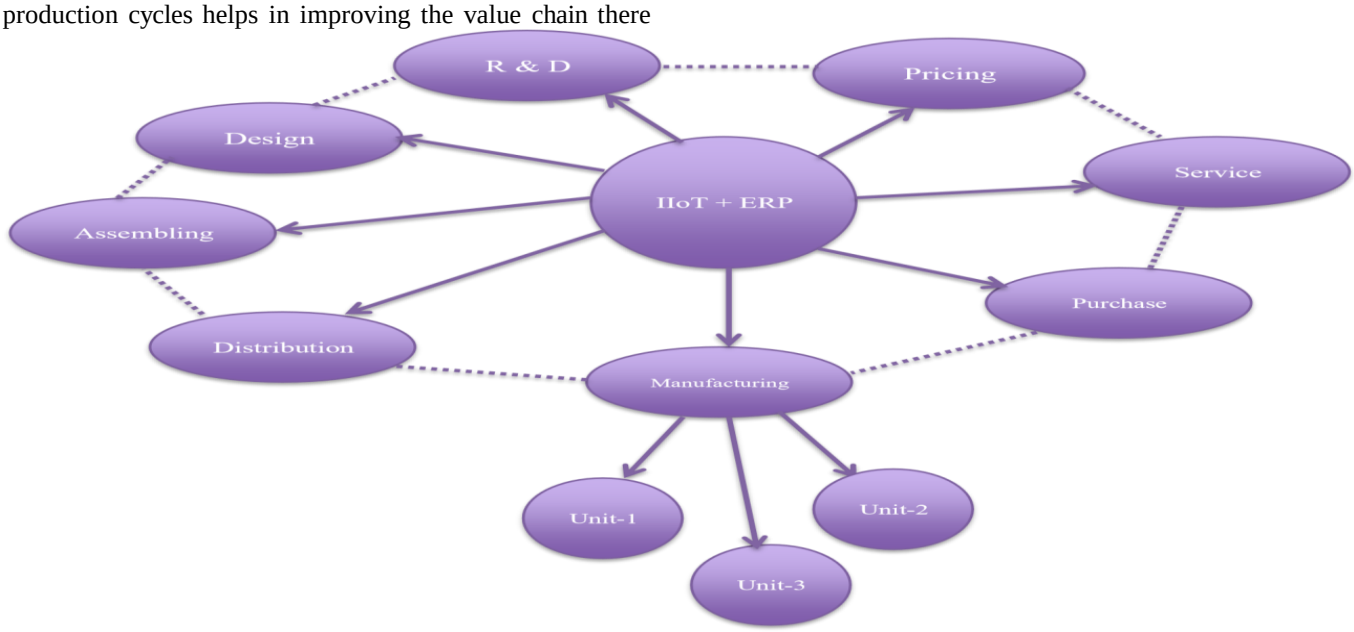

Fig. 5: Enhanced Security in Manufacturing Industry under study

IV. RESULT AND DISCUSSION

The Industrial Internet of Things will make it necessary to have a wide range of new and advanced techniques, including new equipment, new systems, new working frameworks, newkinds of high-volume information handling, new cloud administrations, new endpoint managing instruments, and new measures and working environments. In the two industries under study to capture the huge data available ERP is in place. But due to human error there are occasions where data was found missing either by unintentional or willfully. And also data was suppressed/mis- interpreted to save the interest of an individual. Results are presented in Table 1.

Table. I: Results

Description	Industry 1	Industry 2	Proposed Model
High Volume of Data	ERP	ERP	IIOT
Cloud Administration	Local Server	Cloud	Cryptography/IPFS
Forecasting	With human interference	With human interference	System generated data, Scientific analysis, Secured

To avoid these issues IIoT is introduced. With that come the concern of data security and too many interactions between machine and machine and machine with humans. It is proposed to introduce IPFS in one of the industries and cryptography in another industry of study. Advantages of these technologies are the data generated will be secured, forecasting will be scientific, interactions will be controlled and risk will be minimized/eliminated

V. CONCLUSION

With IIoT,gadgetsatthe edge won't just interact with one another, they will follow up on information collected through analytics. The analytics can be figured locally, or over the cloud when more profound investigation with bigger informational collections and progressed process framework are required. Every industry will discover better approaches to utilize the intelligence collected by IIoT, for example, improving assembling, handling clients effectively, and increasing productivity. IPFS and cryptography will provide the needed security to the data that is available in the industries. With the proposed model it is possible to usher in a new paradigm shift in ERP and IIOT integration in manufacturing industries.

REFERENCES

1. D.F.Ross,Introductiontoe Supply Chain Management:Engaging Technology to Build Market-Winning Business Partnerships, CRC Press,2016.
2. S.C.Council,Supply chainoperationsreferencemodel:Revision11.0, Chicago, IL,2012.
3. E.Borgia,Theinternet ofthingsvision: Keyfeatures,applicationsand open issues, Computer Communication. 54 (2014)1–31.
4. S. Yuvaraj, M. Sangeetha, Smart supply chain management using internet of things (IoT) and low power wireless communication systems, in: Wireless Communications, Signal Processing and Networking,WiSPNET,InternationalConferenceon,2016,pp.555-558.
5. S.K. Kinnunen, S. Marttonen-Arola, A. Ylä-Kujala, T. Kärri, T. Ahonen, P. Valkokari, et al., Decision making situations define data requirements in fleet asset management, in: Proceedings of the 10th World Congress on Engineering Asset Management, WCEAM2015, 2016, pp.357–364.
6. T. Wang, Y. Zhang, D. Zang, Real-time visibility and traceability framework for discrete manufacturing shopfloor, in: Proceedings of the 22nd International Conference on Industrial Engineering and Engineering Management 2015, 2016, pp.763–772.I.
7. Veza, M. Mladineo, N. Gjeldum, Managing innovative production network of smart factories, IFAC-PapersOnLine 48 (2015), pp. 555– 560.
8. P. Zawadzki, K. Zywicki, Smart product design and production control for effective mass customization in the industry 4.0 concept, Manage. Prod. Eng. Rev. 7 (2016), pp. 105–112. PetarRadanliev, et al., 2018 "Futuredevelopmentsincyberriskassessmentfortheinternetofthings, Computers in industry, 102,pp.14-22.
9. Boyes, Hugh, Hallaq, Bilal, Cunningham, Joe and Watson, Tim (2018), "The industrial internet of things (IIoT): an analysis framework". Computers in Industry, 101. pp. 1-12.2018.
10. LachlanUrquhartandDerekMcAuley(2018),"Avoidingtheinternet of insecure industrial things" , computer law & security review 34 (2018), pp.450–466
11. Ding Zhang et al (2018), "Enabling Industrial Internet of Things(IIoT) towards an emerging smart energy system, Global Energy Interconnection", Vol. 1 No. 1 Jan.2018
12. Vinay Nathan., 2019 Improve ERP with IIoT,https://www.efficientplantmag.com/2019/05/improve-erp-with-iiot/
13. https://www.i-scoop.eu/internet-of-things-guide/industrial-internet- things-iiot-saving-costs- innovation/cybersecurity-industrial-internet- things/

AUTHORS PROFILE

Jose S, at present he is employed as Associate Dean of business school of VIT, Vellore, India. He has published many papers in Journals and conferences. He is also the president of Chennai chapter of American Society of Heating Refrigerating and Air-conditioning engineers (ASHRAE)He has 27 years of teaching experience in various Engineering and Management Schools. For a decade he was the Principal of Anna University affiliated colleges. One of his patents got published recently and he is working on 3 more patents. He is a consultant to 4 industries and is developing a product for EID Parry. He has vast international experience and interacted with visiting professors and visited USA, UK, Germany, France, Belgium, Switzerland, Spain, Malaysia, Thailand, Indonesia, Singapore, Sri Lanka, Turkey and Jordan on various academic assignments. He has produced 3 PhDs.

Vincent Herald Wilson, M E, Ph D, is a Professor of Department of TechnologyManagement in School of Mechanical Engineering (SMEC), Vellore Institute of Technology (Institute of Eminence -IoE), Vellore-632 014, India. He has completed his Doctorate degree from NIT Trichy. He haspublished several papers in international and national journals and presented conference papers
in the area of IC Engines, Solar Desalination, Alternate fuels, Solar Hybrid driers andEmissions. His research interest includes Optimization Techniques, Total Qualitymanagement, Emission reduction for Automobiles and Product Development and Disruptivetechnologies.
He has two patents awarded by the Government of India. He has undertaken consultancy workfrom Singapore. He has participated in a number of conferences in India and abroad and is amember in many professional societies like Indian Society of Technical Education (ISTE),American Society of Engineering Education, (ASEE), Computer Society of India (CSI) andIndian Welding Society (IWS). He has guided two Doctorates. He is also a reviewer andeditorial member of a few journals. He has visited China, US, UAE, Srilanka, BangladeshOman and Bahrain, Ethiopia on various assignments