Available online at
www.mdl.mazedan.com

MJCEA

www.mazedan.com

www.mazedan.com/mjcea

TOWARD INDUSTRY 4.0: CHARACTERISTIC IMPLICATIONS OF THE INDUSTRIAL INTERNET OF THINGS IN MANUFACTURING

VIVEK SRIVASTAVA*, OJAS RATURI

MAZEDAN JOURNAL OF CIVIL ENGINEERING & ARCHITECTURE
e-ISSN:
Article id- MJCEA0102005
Vol.-1, Issue-2
Received: 30 Jul 2021
Revised: 27 Sep 2021
Accepted: 29 Sep 2021

Citation: Srivastava, V., & Raturi, O. (2021). Toward Industry 4.0: Characteristic Implications of the Industrial Internet of Things in Manufacturing. *Mazedan Journal of Civil Engineering & Architecture*, 1(2), 19-30.

Abstract

Manufacturing sector is migrating from present state to Industry 4.0 and Industrial Internet of Things (IIOT) is the leading medium to connect. Presented review study clearly elaborates the challenges and way forward to the things are perceived or considered in the production to shipping of product, and the way customer is connected to the Manufacturing company of product. IIOT is expected to bring considerably large societal and industrial impact by means of improved function and efficiency across industries. Since, it will be single architecture connecting sensor to cloud, vendor to OEM (Original Equipment Manufacturer) and range across different industries, hence it will be the replacement of present specialized standards which vary from industry to industry. Presented study deals with the smart manufacturing framework for IIOT components and development of IoT technologies and taxonomies along with the vulnerability on basis of security and involvement of human factor.

Keywords: IIOT, Smart Manufacturing, Industry 4.0 and Security

1. INTRODUCTION

The Industrial 3.0 is a concept that tells how the production of a company is increasing by using automation in the production line. Manufactures use sensors and actuators in a production facility to increase the production. Focus of Industry 3.0 is only on production and efficiency of machine. The Internet of Things was launched in 1999 [1] and has been extended to embedded devices in residential, commercial and industrial settings [2]. IoT is a system for communicating with other devices, collecting data, managing data, and analysing data. Each subject is equipped with a sensor and is capable of independently communicating its presence to another device. The term IOT applies to the use of emerging technology in industry as it hinders the study of alternate current system architectures [3]. The aim of this paper is to suggest a structure for the IIOT and the advancement of IoT technologies. Until creating a structure, we looked at current industry-focused taxonomies. IoT taxonomies offers a mechanism that enables IoT projects to be easily compared and classified [4].

IoT taxonomy provides a structure for the industry in the sense of IIOT, but the first three technological revolutions were powered by mechanical development based on water, steam, the use of mass labour and electrical energy, and the use of electronic, controlled production, respectively [5]. In this series, the fourth Industrial Revolution (Industry 4.0) was suggested in 2011 as part of the growth of the German economy [6]. Industry 4.0 is manufacturing culture or time where all machine and other factors of Industry should be working without human interaction. Industry 4.0 reliance on CPS increasing productivity and transparency. The term industrial internet is different from internet that we use in general lifestyle. The Industrial Internet concept is originated from United States. It is the idea of IoT Intelligent Manufacturing Process leveraging sophisticated data processing for transformational market results and redefines the landscape [3]. Each computer in the manufacturing unit must be capable of self-functioning. Big Data is the backbone of the Industrial Internet [3] network. For the first time invented by General Electric (USA). This definition specifically distinguishes the idea of the Internet and the Commercial Internet, while each structure offers a wide field of networking [7]. Based on the study of current research papers, the definition of the IIOT operates on two main features:

- On the technologies used in the IIOT environments.
- The distinctive goals and objectives to which certain innovations are directed [3].

From now on, a new working description of the IIOT may be defined and has the same framework as the basic term with which we began. Industry Internet of Things (IIOT) is concept that connect all assets (Machine, Human Resources, Product and Services) through internet and collect data, analysis data and gives informational changes in system and increase productivity and excellent services for customer [8] [9]. IIOT is a subset of IoT which requires higher level of safety, and reliable communication without

Department of Mechanical Engineering, DIT University, Dehradun, U.K. 248009 India
*Corresponding author email- reachtovivek@gmail.com

disruption of real-time data. The focus of IIOT is efficient management of industry and industrial operation. Figure 2, Figure 3 and Figure 4 shows the changes and development in concept of IIOT respectively. There is timeline diagram how the industry is developed in a year.

There is a graph shows that how the industry 4.0 concept is developed in time period of last decade.

After knowing the characteristics of the device, we can examine the vulnerability and recognise trends that reflect on the technologies used in the manufacturing field. This paper is structured as follows-Part 2 gives more history to IoT taxonomies. Section 3 provides framework system for Manufacturing Sector. Section 4 provides background of using protocol in system. Section 5 provides the knowledge of security issue in system. Section 6 provides what will be changes should be in industry for better work environment. Section 7 identifies challenges in future work.

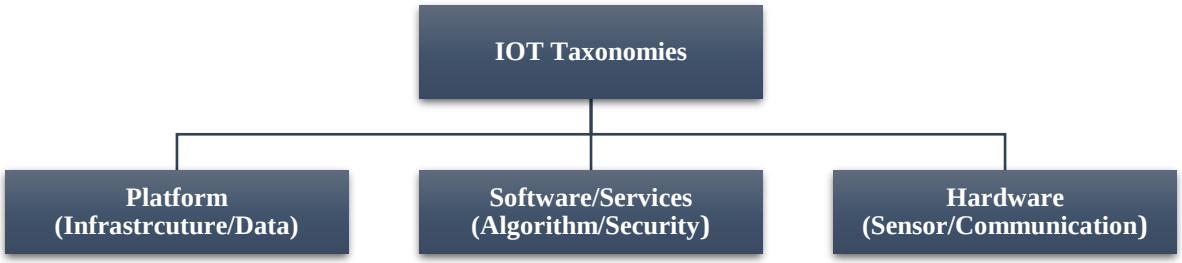

Figure 1 IoT Taxonomies

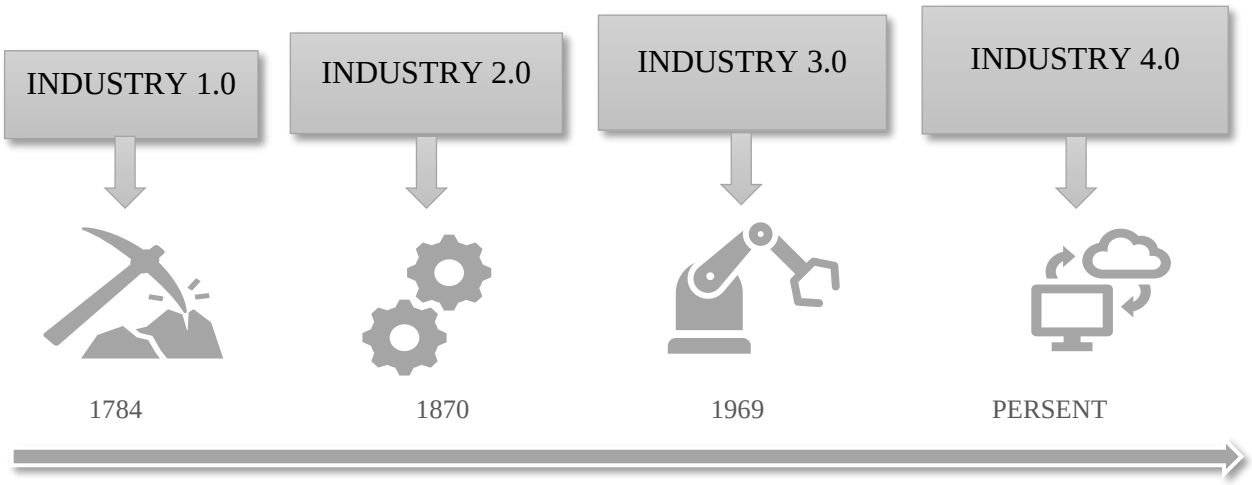

Figure 2 Industrial Revolution

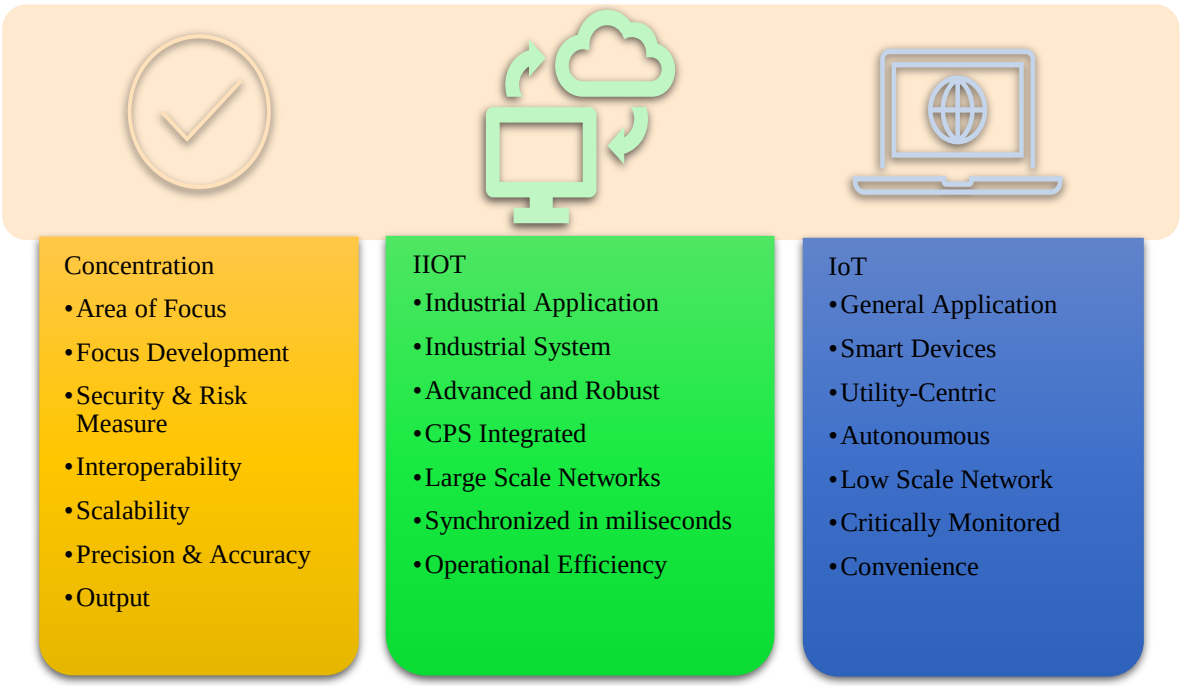

Figure 3 Concentration Between IIOT & IoT

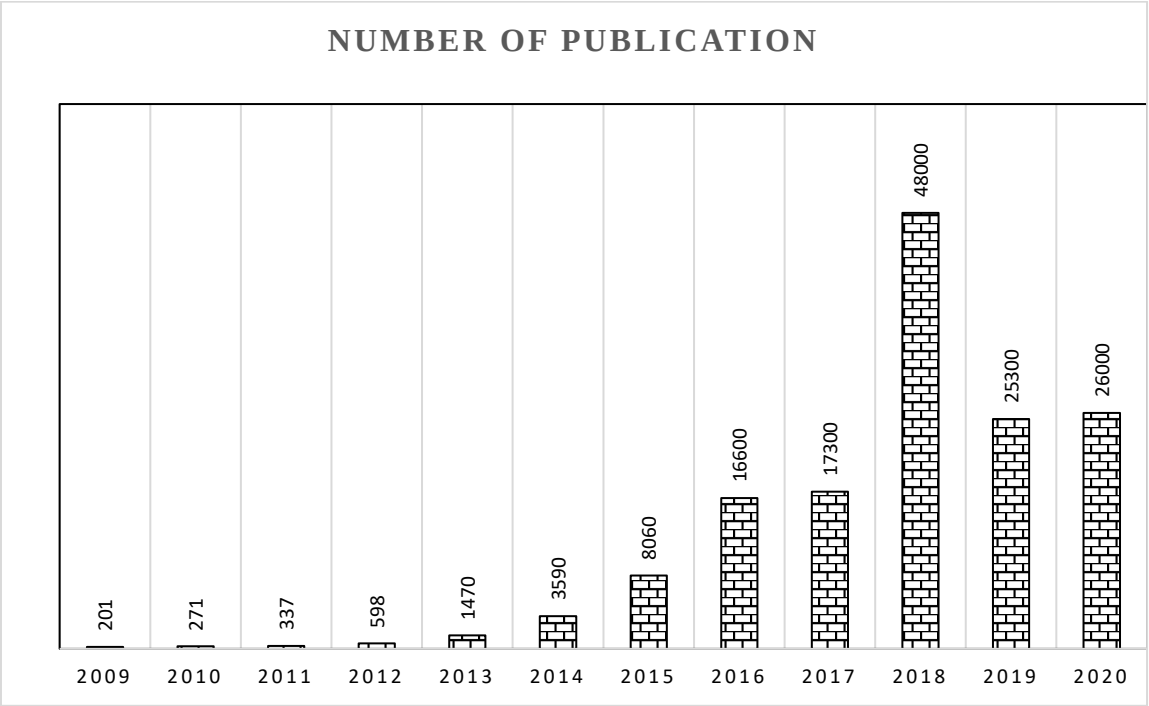

Figure 4 Graph Between Numbers of Publications Published in Last Decade

2. DIMENSIONS OF IOT TAXONOMY

There could be multiple classifications of existing taxonomies of IoT. For e.g. Device Centre Taxonomy is used in defining the role of device, location and where device is used [10],

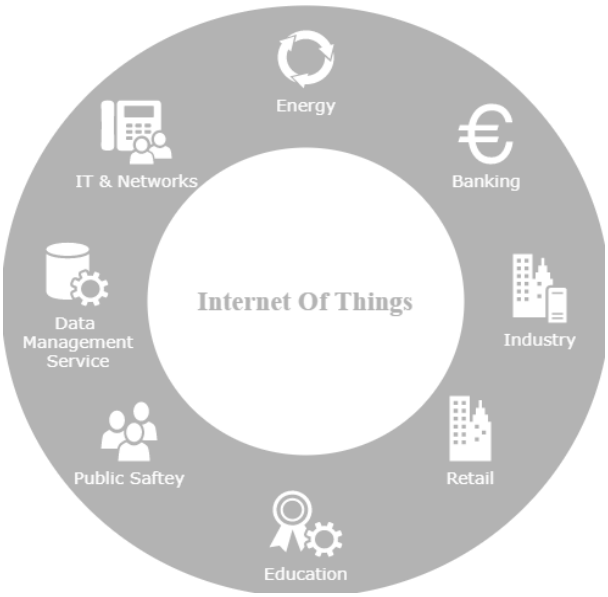

Figure 5 Internet of Things Sectors

IoT Stack Centric Taxonomy is useful in fulfilment of business objectives [11] & [12], IoT Sensor Taxonomy for sensing capabilities which are not the wide range subset of IIOT devices [13], IoT Smart environment Taxonomy for security perspective though it has higher cost implications involved [14] , IoT Architecture Taxonomy is combination of business objective and technical objective [15], Domain or Sector-based IoT Taxonomy is often used in industry to discuss what sort of device is used in the system [2], Industrial Internet of Things Taxonomy has several requirements (real time, data object size, durability, module scale, runtime compatibility, delivery focus, collection focus) for a device or system [16]. Each criterion has limitation and implementation of each criterion is difficult in both the system and device [16]. Given the limitations of available literature on taxonomies we have derived and proposing a IIOT framework particularly in manufacturing sector. Below in the figure 5 showing uses of IoT in various sectors and figure 6 shows the various taxonomies that are part of IoT.

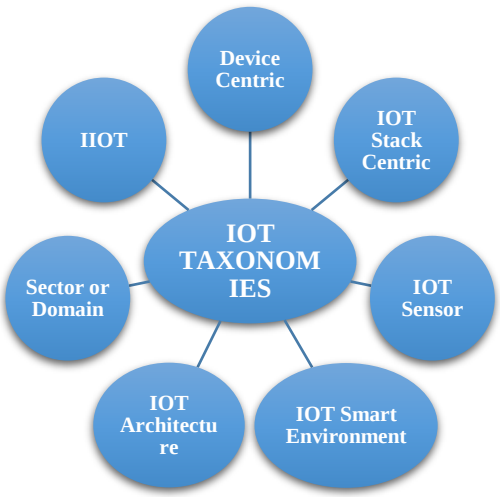

Figure 6 IoT Taxonomies

3. IIOT IN MANUFACTURING SECTOR (PRODUCTION TO SHIPPING)

In a Manufacturing company production system is a major concern of improvement while applying IIOT concept. Industrial Automation Control System (IACS) or Industrial Control System (ICS) helps the companies to understand different kind of system shall be used in the production system. For better knowledge we elaborated

the IACS or ICS system. Industrial control system (ICS) includes devices, systems, controls, and networks. Earlier, in its traditional form ICS was placed in isolated system in which using special software and hardware it run proprietary controls. Various ICS modules used to be mounted independently in protected locations and not connected to the central network, although the proprietary approach is now being replaced by a low-cost Internet Protocol (IP) device that is now generally appropriate. While being installed at protected sites, ICS products are now focused on common embedded device platforms that are involved in routers, cable modems, etc. They also use commercial off-the-shelf applications and command and control networks and systems expressly designed to serve the manufacturing process [17, 18] . In IACS concept there are several systems which should be used in industry for the better performance of production system taking IIOT concept under consideration. One of the systems is Cyber Physical System (CPS). According to H. Boyes "A system comprising a set of interacting physical and digital components, which may be centralised or distributed, that provides a combination of sensing, control, computation and networking functions, to influence outcomes in the real world through physical processes." [19]. It is a system that uses physical data and control physical process that uses sensor to receive information and determine whatever change in state of actuator occurs and draws an operator attention. Data and/or information processed by CPS systems are the subject of CPS on physical process control [3]. What sets CPS apart from more traditional information and communication systems are the real-time data of their encounters with the physical world [3].To integrate CPS in the production unit we require a better system which can be done by with the help of PLC's. Programmable Logic Controller was invented by Dick Morley in 1964. Since then, PLC has revolutionized the industrial and manufacturing sector. It uses a logical computer language in machine to perform suitable work. It is also known as central processing unit CPU of machine which performs on Input/Output system [20].

The most basic function of a programmable controller is to simulate the function of an electromechanical relay. The discrete input has a unique address, and PLC instructions can test whether the input status is on or off. Just as a series of relay contacts perform a logical "AND" function, unless all contacts are closed, current is not allowed to flow, so if all input bits are open, a series of "Check for Continuity" commands will output Storage bit power supply [21]. PLC's system is very important to a manufacturer in order to implement any program in production, it also has some disadvantage as in PLCs at times it is hard to communicate with all the machines in one platform and thus specialized operator is required for controller. For manufacturing companies, there are two main types of PLC which are fixed / compact PLC and modular PLC [20], that are used in production facility. The Compact PLC is within a single case, there would be many modules. It has a fixed number of I/O modules and external I/O cards. So, it does not have the capability to expand the modules. Every input and output would be decided by the manufacturer. Modular PLC, this type of PLC permits multiple expansion through "modules", hence referred to as Modular PLC. I/O components can be increased. It is easier to use because each component is independent of each other. Working Platform of PLC-Operating a PLC (machine) in production facility we require a system that is helpful for workers and manufactures based on the concept of IIOT that connect all machine with internet and better understand the machine performance. It can be done by using HMI system in production facility.

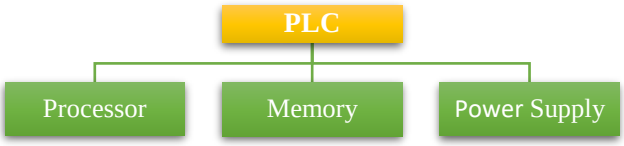

Figure 7 PLC Structure

Figure 8 Working Platform of PLC

Human Machine Interface (HMI) is also known as OIT (Operator Interface Terminal). It is a software and hardware system. Operator depend on HMI to controlling the machine and gives informational changes in machine. HMI varies upon device configuration. Components use in HMI is Panel Board, ON/OFF Switch, Computer. HIM gives output about the machine condition and what changes are required in machine to increase efficiency. There is some disadvantage in HMI as this is not flexible. Specialized operator is required for operating. It is costly system and difficult to change process when machine is breakdown and replace [22]. Below is the figure 9 depicting the structure of production system in Manufacturing company in the context of IIOT

Figure 9 Production System

4. CONTROL SYSTEM

Controlling of system is another concern and it is very important for a manufacturer to get a best control system in the industry. To implement IIOT concept in industry we reviewed some controlling system that could be used by the manufacturer for better controlling of machine, among which SCADA was found more useful and better suitable. It is known as Supervisory Control and Data Acquisition. It is a platform to gives control on machines and what will be set point to be changes (open or close, monitor alarms, controllers) in machine or system [23]. SCADA system is built on demand by machine specification and gives additional control over a particular machine. A method that enables the operator to use a widely dispersed procedure at the central position and to collect measurement information [3]. SCADA systems employ concepts like information modelling and data virtualization to consolidate and organize data from these disparate devices and systems [24].

There is some disadvantage in SCADA system have not proper connectivity and data analytics found in IIOT [25]. For better controlling of machines manufacturer should be

use DCS with SCADA. Distributed Control System (DCS) is used for eliminating the disadvantage of SCADA system and it has own SCADA system to perfectly control PLC and gives one single controller for all machines. There is some disadvantage in DCS is that it is not flexible because of when there is need in change of process of machine it is required all changes in controller and required special operator to operate machine and it is also costly when manufacturing facility is big [26].

For additional control and execution of program in machine, manufacturer should be gone for MES. Manufacturing Execution System (MES) is connected with SCADA system and gives additional control in facility and gives output about how many products is made and what is amount of waste produce in production. It is use for production management and control data generate from machines. It is also use for quality management and delivery of products. There is some disadvantage in MES system it is not connected directly with machine and it is difficult to identify the condition of machine, condition of machine handle by the operator [27]. Controlling of machine with MES, DCS and SACDA we require a server which connect all control system with machine and gives better control in production unit. OEE is better option for communication between controlling system and machines. Overall Equipment Effectiveness (OEE) is use to eliminate connectivity issue between machines and MES system. This server is used for connectivity. It is connected between in SCADA system and MES system. Server collect data from SCADA system and provides output about machine's condition and how many products are made and what is rate of waste material. It works on standard rate set by the manufacturer. It works on three principles:

- Availability,
- Quality and
- Performance.

There is some disadvantage of server it is costly, and this require more people to handle data between SCADA system and MES system [27].

Figure 10 Control System

5. MANAGEMENT SYSTEM

Management system in any industry or organization is required to manage every activity or tasks performed by human resources or machineries. Management system ensures the proper functioning of assigned task by the workforce in various manners starting from inception to the end-delivery or consumption of any product. The major role of any management system is to monitor the efficiency of set up workforce or machines in any given circumstances, and to address the challenges faced by them at any time. Therefore, for an improved management system in the context of IIOT we require Enterprise Resource Planning System (ERP). It is connected with MES system. This system is use for managing workorder and schedule of production. It has data about demand of product. It has real time data about production. This system is use in accounting, resource planning, workflow management and quality management. AL Fawaz [28] Esteves [29] Zhang [30] have identified user participation and involvement as one the important factors for successful ERP implementation. User participation is defined as the assignments, activities, and behaviours that users or their representatives perform during the systems development process [31]. There is some disadvantage in system traceability of product. It does not have accurate real time data about production facility due to human error and connectivity between system and production floor [32]. ERP works only for internal operations of the industry which also includes management of the industry whereas a system is needed to maintain the relation between management and customer hence we require another system known as CRM. Customer Relationship Management (CRM) software is used by the company to maintain the contact with their customer. It is connected with ERP system for better handling of real time data and management of production facility. It is further connected with Cloud system for data storage. Many organizations use CRM as set of tools, technologies, and procedures to support the relationship with the customer to enhance sales [33]. The importance of customer satisfaction cannot be denied as happy customers are like free advertising for the company [34]. CRM is built a better mutual understanding between companies and their customers. CRM influences customer satisfaction and loyalty regarding companies. CRM has also some disadvantage it is require specialised worker and data handling little bit complicated and privacy of data is always a concern. Although ERP and CRM are connected to each other but are not much useful in management of workshop and inventory, and to do so we require a better system that is connected with ERP and CRM and could manage the workshop, and it is done by the WMS system.

Workshop Management System (WMS) is very useful in warehouse design, control, and data management of the product, and this makes warehouse management lot easier. Warehouse inventory management refers to the reflection of a variety of storage and ensures flow of material in a timely manner. It has provision of the basis for production management and cost accounting according to management of warehouse, cargo and other account and type and data of in / out library into / storehouse [35]. WMS has a disadvantage of collecting data in one place [32]. Below is the figure 11 depicting the structure of management system in Manufacturing company in the context of IIOT.

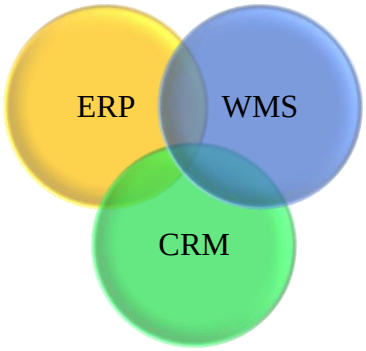

Figure 11 Management System

6. SHIPPING SYSTEM

Shipping of any product by manufacturer using IIOT concept, manufacturer require better system to get physical condition and location of product, and it can be done with the help of RFID and WSN system. For better knowledge we elaborated the RFID & WSN system.

7. RFID

Radio Frequency Identification (RFID) is used in distributed and process control, traceability management and real time location of product and data control of product. It is very useful in warehouse management. An RFID system includes five components as per following [36].

1. Marks located on the identifying object,
2. Readers who may be reading or writing/reading devices,
3. Radio-emitting antennas to enable the mark and read/write data,
4. A local control room sends read/write instructions to all readers and read back tagged information.

In addition, the signpost is a new component applied to some schemes. Signs allow tags only in their immediate surroundings at 123 kHz, so that tagged objects can be detected precisely in those locations. One tag is a mini-small label which preserves data in fixed format that includes antenna and wireless ICs as large as seam. RFID tags are added to tagged objects to announce the reader's presence.

The RFID reader consists of parts for transmission and reception. It sends a carrier signal, collects the back dispersed signals from the tag and processes data. The readers themselves address all contact information, including communication establishment, collision avoidance and authentication. The reader can also interact with an external host computer. It is not capable of providing real time condition of product [37] [38] [39].

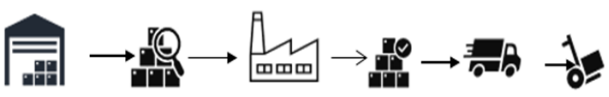

Figure 12 RFID SYSTEM

8. WSN (WIRELESS SENSOR NETWORK)

It is sensors that collects the product physical condition and obtain real time data of product and improve the supply chain management of company. The sensor nodes work in a self-organized, decentralised manner that preserves the best possible communication for as long as possible and transmits their data to the base station through multi-hop delivery.

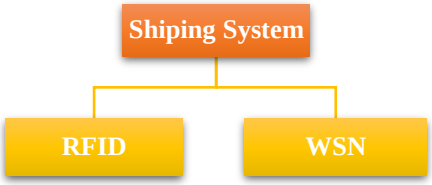

Figure 13 Shipping System

They have to cooperate and use collaborative signal- and information-processing techniques to full fill their tasks since a single node is not always capable of sensing the whole environment. However, individual nodes are tiny, energy-constrained devices with weak processors and a small amount of memory, which exerts significant influence on the design and implementation of WSN [39]. WSN eliminate redundancy of data effectively. WSN system use in RFID to make more efficient data collection system of RFID because RFID incapable of providing the detailed information about condition of product [32].

IoT in Inventory

Intelligent Inventory Management based on IoT, in terms of hardware, consist handheld electronic tags, RFID tag; in terms of software, consist of a host management system and shelf electronic tag. Handheld Electronic tag is recording equipment operation of in/out of storage in inventory. Handheld reader to scan barcode of goods and then store information in RFID tag to complete the inventory of goods, reader is connecting with host management system to read real-time inventory data and update the database. Host management system consists of information management module, storage operation management module, handheld device management module, inventory operation module each module works together to help with Intelligent Inventory Management [40].

Dimension of Application Based Protocols

IoT Protocol sets the standards for the methods with which device and server transmit the data between device to device, device to server, device to people, server to server. Message Queuing Telemetry Transport (MQTT) protocol is used for transmitting data between device (system) to server. This protocol work on top of TCP (Transmission Control Protocol). MQTT control and analysis data generate from small device with the help of Cloud System. MQTT used in oil industry, manufacturing facility for controlling and analysis of data [16]. It is a lightweight communication protocol designed for connecting devices to controlled network. It is uses 2-byte header and binary in nature [41]. In MQTT, clients can subscribe to multiple topics and accept every message issued by each topic. MQTT is designed for low band width and constrained devices, MQTT support only subscribe pattern communication, which hardly covers all examples of IoT. MQTT gives three levels of Quality of Services for delivery for message [42]. It is not designed for device-to-

device transfer, and not for multicast data to any receivers [43]. MQTT is defined as shown in figure 14.

Extensible Messaging and Presence Protocol (XMPP) is also known as JABBER. This protocol is use for transmitting data between device to client. Devices are connecting with people and transmit informational data. XMPP is work on XML text format and HTTP on top of TCP. XMPP offers easy way to address device [16]. XMPP is IP based communication protocol with Extensible Mark-up Language (XML) support. It is used for real time communication and tele presence. XMPP is support Response architecture. XMPP allows heterogenous devices to interact with each other by send instant message over the internet perspective of the basic operation systems [41]. XMPP is secure protocol, supports encryption and control for addition of new applications on top of current protocols [44] . Data Distributed System (DDS) protocol is use for transmitting data between device to device. It has a data centric standard with high performance in industrial application. It is very fast standard because device data demand data different than IT infrastructure [16]. DDS is real-time communication protocol which also supports Publisher/Subscriber protocol architecture. DDS doesn't support broker-based architecture, it uses multicast Quality of Service guarantees [41]. DDS offers 23 Quality of Service security levels and it's allowed variety of quality services which contents security, priority, reliability, performance, interoperability, resource requirement etc [45]. DDS defines two sublayers: Data-Centric Publish- Subscribe (DCPS) which distributes information to subscribers and Data-Local Reconstruction Layer (DLRL) which is an elective and is an interface to the DCPS functionalities and share data among distributed objects [44],as shown in the figure 15.

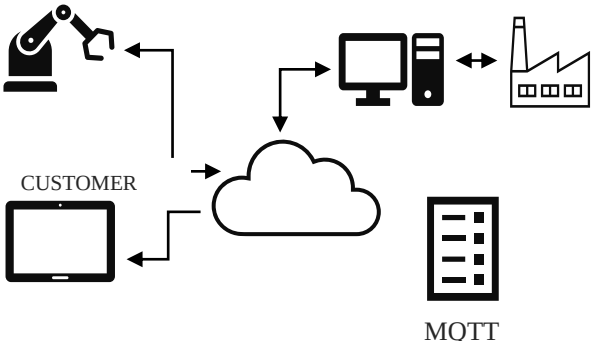

Figure 14 MQTT PROTOCOL

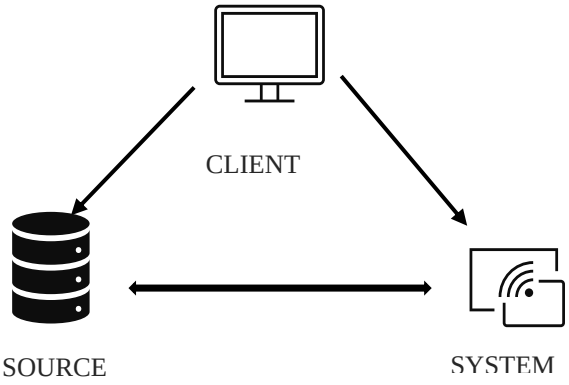

Figure 15 DDS PROTOCOL

Advanced Message Queuing Protocol (AMQP) is use for transmitting data between server to server. It uses point to point connection. It is message centric middleware. It is reliable because of point-to-point connection. It is use in Banking Industry [16]. AMQP is corporate messaging protocol design for security, performance, reliability [46]. It's supporting both request/response and publisher and subscriber architecture [47]. It is a binary protocol and requires fixed header of 8 bytes with small messages to maximum size dependent on the programming technology [48] [49]. AMQP offers 2 level of QoS. AMQP uses series formats such as Protocol Buffers, Message Pack to serialize structured data in order to print it as the message payload [46]. AMQP offers highest level of security from other than protocols and it is mostly use protocol in business industry [42]. Open Platform Communication Unified Architecture (OPC-UA) is use for transmitting data between device(machine) to server. It is open architecture protocol anyone can access data, anywhere, anytime, when they need it. It uses point to point connection, when there is any update in the system its updates the data. In existing Industry facility use OPC-UA server connect their ERP, MES, WMS with OPC-UA server with the help of application server (Factory Studio, Ignition). Now some system or machine have own OPC-UA server and they are connected to directly cloud for controlling and analysis data. There is some disadvantage of OPC-UA protocol. It is open architecture but limited access for people because access for your data you need to pay for it. It is costly server for companies, as shown in above figure 16 [16].

9. JIT INVENTORY

Just-in-time methods are generally carried out in the manufacturing company with the key purposes of tracking the timeliness of product production and distribution while preserving or enhancing product quality [50].JIT allows producers to manage tasks within exceedingly short intervals and has a large effect on the timetable of production. IoT will connect and document its output and improve the production schedule with physical elements of production processes such as work in progress, finished goods, labour, machinery etc. In a distributing manufacturing environment focused on RFID and cloud technology [51] Guo built a framework with remote control and production planning functions. With strong extensibility and scalability, the device meets the decision-making criteria in a very short time. In order to

track the progress of production in manpower plants and their manufacturers, a system has been set up to capture the production status of machines and operators in real time. The knowledge obtained from plants is used to remotely track the planning decisions at various levels [52]. In a shop floor setting allowed for IoT (RFID) Zhong have considered another manufacturing planning model [53].

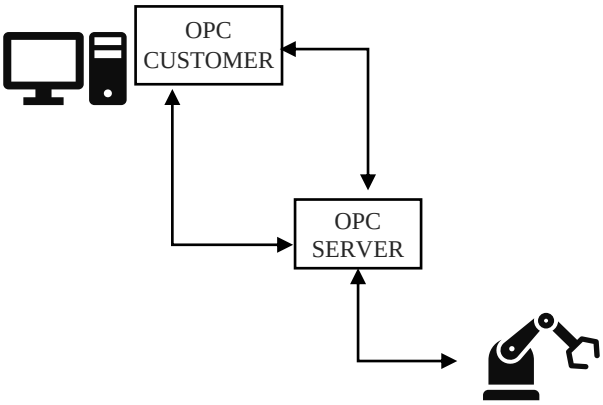

Figure 16 OPC UA PROTOCOL

[52] The model is based on forecasting and planning of development at two stages. For materials preparation and local processes, the Business uses ERP as MES. The ERP system stores customer data, provider data and customer order obtained to specifications for appropriate materials. The information on the development process is retained in the local networks and the system will give the breakdown schedules to each unit and the operators. The local system in a mounted machine has the function to track development. There are still open issues like failures in exchanging details or manufacturing coordination, cross-functional conflict, Improper resource controls and risks of manufacturers' on-time supply of materials. These matters require immediate technological intervention to get the JIT process better streamlined.

10. SECURITY AND PRIVACY

Security and privacy of any industry is a concern lead through its vulnerable machines or associated systems which are used in the complete process. Through introducing a strong defence mechanism in the industry one can address potential physical or software attacks. Security of IIOT is generally classified into four categories which are Physical Attacks, Network Attacks, Software Attacks and Data Attacks. Various attacks administered through physically for example being in contact with the system and server are defined as Physical Attack, it includes Tampering (modification in system or device physically) [54], Malicious Code Injection (injecting malicious code in the system and device leading in launch of another attack on system) [55], Jamming (creates and send noise signal in Radio Frequency (RF) to launch Denial of Service in RFID and WSN) [55]. Thus, to prevent attack a defence mechanism in the hardware or software form can be used in manufacturing sector. [56] Manufacture must use PUF (Physically Unclonable System) system to protect from physical attack. PUF (Physically Unclonable System) system has variability integrating in small devices and it is use Integrated Chip. In this system exact clone of the system is difficult to create and eliminates the Tampering and Malicious Code Injection threats. and thus, secure the devices. Another type of attack is Network Attack, it can easily launch without being physically present nearby any network. In this attack, attackers manipulates the IIOT networks, it includes Traffic Analysis Attack (information and data flowing in the system is obtain by the attacker without going close to the network) [54],RFID Spoof attack,(attackers use the original RFID tag and send the data in RFID tag and obtain the information from the RFID) [55],RFID Unauthorized Access attack (attackers able to modify or delete data in RFID without authorized access) [54]. Thus, to prevent attack a defence mechanism in the hardware or software from can be used in production system. [57] Efficient and Privacy Preserving traffic obfuscation (EPIC) framework is provided protect against Traffic Analysis Attack. This framework provides differential privacy by unviability of Traffic Flow. [58]Another framework is based on SRAM, PUF which produce unique device footprint as device ID. This framework reduces the spoofing and unauthorized access. On the other hand software attack can launch by attacker by taking advantage of vulnerability of system and device, it includes Virus, Worms, Trojan Horses, Spyware and Adware (through these malicious software attackers can obtain information and data form system or device) [54], Malware (affect the data centre and device, which contaminate the cloud and data centre) [59]. Thus, to prevent software attacks follow system could be used for e.g., [60] High Level Synthesis (HLS) system is use for preventing network from hardware trojan. [61] Another framework is Malware Images Classification System (MICS), MICS converts the suspicious program into grey scale image and capture and then captures hybrid local and global malware features to perform malware family classification.

Lastly, Data Attack is a measure concern in the industry and with the help of Cloud Computing the number of attacks are being minimized, it includes Data Inconsistency (In IIOT, attack on data integrity leading inconsistency on data transit and data stored in database is referred as Data Inconsistency) [62], Unauthorized Access (In unauthorized access, malicious users can obtain data from system and device) [62]. Thus, to prevent data attacks follow system could be used for e.g., [62] Message Authentication Code (MAC) system is use for secure data transmission in system and MAC use Chaos-based privacy preserving cryptographic scheme. [63]Another framework is Attribute Based Encryption (ABE). ABE provides integrity of data and preserves privacy of data.

11. IMPACT OF IIOT IN HUMAN WORKFORCE

Advanced automation has the potential to improve the manufacturing technique. New technology may provide the following economic benefits [64]: -

- Lower manufacturing cost,
- Reduce Workforce,
- Improved product or service quality,
- Enhanced flexibility of production.

Introduction of new technology brings many unknown fears such as reduced human workforce, changes in way of work and pay reductions. A major work fear is that the advanced machine might take more jobs than expected; and introduction of new technology also challenges existing knowledge and skill set required to operate the technology. Therefore, to implement IIOT in manufacturing industrial workforce will require skill and knowledge to administer IIOT operations. Manual tasks might be replaced by advanced machines and thus to take over management-related task workforce will need stronger personal skills such as communication and coordination regarding higher responsibilities and high-level decisions. At an engineering level, in addition to software and programming skills more specialist is required having operational knowledge and skills of system' interface to disseminate anticipated results. Meanwhile, to deliver expected output to end users balancing the innovation and human workforce is a big challenge. Thus, to do so following could be done.

12. ISSUES

There are key challenges that are reflected in the industrial application of IOTs as well as severity of consequences of failures where flawless operations are expected due to the huge capital investment. Considering the general challenges first, data and service security is always a major issue due to the large vulnerability of information theft faced by IOT based large scale applications and services [65]. To combat this situation, it becomes imperative to provide multi-level data protection and security mechanisms to ensure service continuity and required Quality-of-Service (QOL) [66]. In addition, the storing of data is another area of concern which is generated by a growing number of sensed high speed data sources. The collection and delivery of data is also a difficult activity involving a great deal of work [67]. Additionally, the interoperability and connectivity in an industrial automation also need to be taken well care of [65]. The scale and structure complexity of the control systems that are connected and integrated with large engineering efforts involves a costly operation to achieve interoperability [68] [69]. As a result, high stringent timing and reliability requirements on timely collection data and proper control are a challenging task to monitor. Lastly, the energy consumption of various IIOT applications calls for the demand of creating energy efficient designs with low power sensors that do not need battery replacement over lifetimes [70]. Trust in the IIOT framework is related directly to the performance of every technology; customer confidence in these innovations has great effects. Confidence in these IIOT programmes would also impact

the successful operation of the IIOT based systems by industrial consumers (e.g., owners of the individual industry). The IIOT scheme is at its first stage and customer protection and privacy is essential. Protection and privacy are tightly associated with the customer's confidence, and the stronger interaction between device and user. Therefore, customer trust models are necessary and further study is required in customer trust models for an effective adaptation of the IIOT framework in the industry.

13. IIOT STRUCTURE

Apart from the above future research related work in IIOT, because this concept is a major requirement for companies in future and we proposed a stable structure of IIOT concept can be implemented in the industry. In current scenario there are lot of issues regarding hardware and software like to make every device sensor based for e.g., in biometric machine one has faced issue with finger prints sensing (or touch) which often have created issues for human workforce employed in any manufacturing or production unit. Therefore, to ease the challenges this paper proposes a framework which tells about necessary modifications to be done in the Industrial IoT system for efficient and effective functioning.

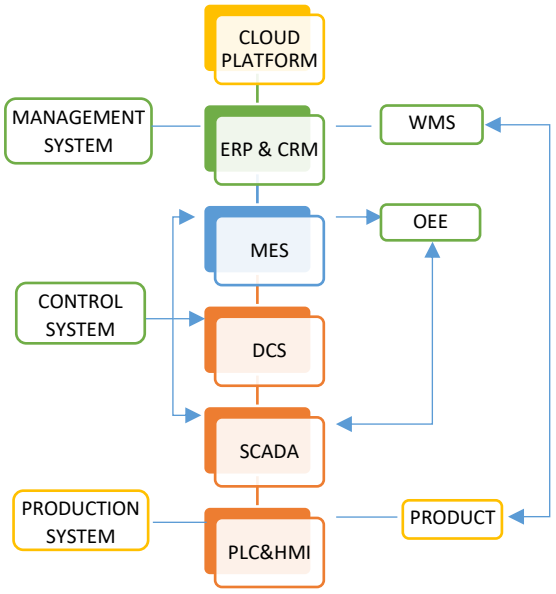

Figure 17 IIOT Structure

14. CONCLUSION

The IIOT framework enables the industry to gather and store, evaluate a vast volume of data that enhances the efficiency of the Organization with the aid of the Internet system and allows employees who work in the enterprise, and also helps consumers to communicate with the Enterprise everywhere, at any time, and to capture their real-time service data. Understanding of necessity of satisfied, unstressed workforce for the most effective application of advanced automation, there are some critical job design considerations that should be incorporated in the system using advanced technology: -

- Control of work,
- Involving employees in the decision process of selection and implementation of the new technology,
- Maintaining an on-going process of employee participation in the production process,
- Establishing the supervision process,
- Providing employee learning and growth throughout a career,

- Designing the job for employee self-steam and self-worth.

Authors would strongly suggest that companies should go for "One defined space" for each system use in their facility and position all data of manufacturing facility at one place so that customer could access their (own) data any time whenever needed. Due to its "secure" nature it restricts the third person access to the data. Therefore, by acknowledging all the traditional and latest innovations in the field of IIOT Industrial companies must work towards the betterment of performance indicators of IIOT to provide better services to all connected end users. We found several possible fields for future research which are as follows:

1. Efficient data management, robust and flexible big data analytic technologies, protocols in IIOT and public safety in IIOT [67].
2. IIOT data storage is much complicated; when there is a no facility of data storing in an industry and companies goes for other provider to store their data in their facility centre it could be a major security concern for a company to trust other provider and provide access to their customer (confidential) data.
3. Tracking of data and product is a field of scope although company has started some research but still there is some gap in existing system. There is a no efficient real time data system where company gets information about real physical condition of product and monitor that product. WSN (Wireless Sensor Node) can be a system used to track down the actual condition of product.
4. Controlling system of management of companies are not that efficient but companies still implement those system in their facility centre. ERP and CRM are the system where companies get efficiency and can manage their internal and external affairs.
5. In IIOT system, plant floor of companies wants more independent system, and in present time companies are working on those system, perform work independent from human work force and get that amount of precision like human labour in plant floor. In production system CPS, PLC, HMI and for controlling this system SCADA, DCS can be those systems. These systems are dependent on the human, but they can lot of work without human workforce involvement in the system.
6. JIT inventory system needs more real-time data management system to work effectively in production line. Company's real time inventory management system in the present time is not much secure and independent. OEM can use both management and shipping systems in their inventory management to meet the industry 4.0 concept.
7. Impact of IIOT in human workforce is a considerable problem, but manufacturers are not much focusing on this factor, how they balance their relationship with the workers, in present time the companies are focusing implementation of IIOT concept in their industry. IIOT general concept is that work independent from human workforce and improves the productivity of Company. Manufacturers requires IIOT concept in their facility for work progressively in the market for better profit, companies also focused on that point their workers also know about the systems and better understanding of systems and work more efficient with IIOT concept. That's why manufacturers should work with workers and skill them and increase their knowledge about IIOT concept and work efficiently.

15. ACKNOWLEDGMENTS

The authors are great-full to all the personals for their time and contribution to this paper. And a special thanks to the Department of Mechanical Engineering for supporting this study. The authors declare that there is no conflict of interest.

Funding

Not applicable for that section.

Conflict of interest/Competing interests

The authors declare that there is no conflict of interest.

Availability of data and material- Not applicable for that section.

Code Availability- Not applicable for that section.

Authors Contributions

First Author is responsible for research and guiding for research work.

Second Author is responsible for drafting and writing of research paper and finding.

Third Author is responsible for checking and reviewing the paper for submission.

REFERENCES

[1] K. Rose, S. Eldridge and L. Chapin, "The internet of things: an overview," *Internet Soc.* , 2015.

[2] B. Research, "M2 M Sector Map".

[3] H. Boyes, B. Hallaq, J. Cunningham and W. Watson, "The industrial internet of things (IIoT): An analysis framework," vol. 101, pp. 1-12, 2018.

[4] "Zero Outage Industry Standard," [Online]. Available: https://zero-outage.com/the-standard/security/security-taxonomy-for-iot/taxonomy-for-the-internet-of-things-iot/ .

[5] D. Lukač, "The fourth ICT-based industrial revolution," in *23rd Telecommunications Forum Telfor*, 2015.

[6] "Industrie 4.0," [Online]. Available: https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html.

[7] J. Leber, "General Electric's San Ramon Software Center Takes Shape MIT Technology Review," 2012.

[8] L. Aberle, "A Comprehensive Guide to Enterprise IoT Project Success," 2015.

[9] J. Conway, "The Industrial Internet of Things: An Evolution to a Smart Manufacturing Enterprise," 2015.

[10] B. Dorsemaine , J. Gaulier, J. Wary , . N. Kheir and P. Urien, " Internet of things: a definition and taxonomy," 2016.

[11] L. Puschel, M. Rogelinger and H. Schlott, "What is Smart Thing? Development of a Multilayer taxonomy".

[12] Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, CISCO Systems, Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, (2013) Available: https://www.cisco.com/c/en/us/td/docs/solu, 2013.

[13] V. Rozsa, " An Application Domain-Based Taxonomy for IoT Sensors," pp. 249-258, 2016.

[14] E. Ahmed, "Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges," vol. 23, no. 5, pp. 10-16, 2015.

[15] I. Yaqoob, "Internet of things architecture: recent advances, taxonomy, requirements, and open challenges," vol. 24, no. 3, pp. 10-16, 2017.

[16] S. Schneider, The industrial internet of things (IIoT) and (In) Internet of Things and Data Analytics Handbook, 2017.

[17] K. Stouffer, "Guide to Industrial Control Systems (ICS) Security," p. 1, 2015.

[18] "ENISA," 2017. [Online]. Available: https://www.enisa.europa.eu/ topics/critical-information-infrastructures-and-services/scada..

[19] H. Boyes, " A security framework for cyber-physical systems," 2017.

[20] V. Muthukrishnan, "Electrical 4U," [Online]. Available: https://www.electrical4u.com/programmable-logic-controllers/.

[21] A. Amin and M. Mridha, "A mini view of PLC".

[22] "Inductive Automation," [Online]. Available: https://inductiveautomation.com/resources/article/what-is-hmi.

[23] S. A. Boyer, SCADA: Supervisory Control and Data Acquisition, North Carolina: Instrument Society of America.

[24] J. Falco, "IT Security for Industrial Control Systems," 2015.

[25] R. Hunzinger, SCADA FUNDAMENTALS AND APPLICATIONS IN THE IoT, H. Geng, Ed., 2016.

[26] M. Fahrion, "Evolving from SCADA to IoT. Remote Monitoring and Control Conference".

[27] Intellic Integration.

[28] K. A. Fawaz, Z. A. Salt and T. Eldabi, "Critical Success Factors in ERP Implementation: A Review. European and Mediterranean Conference on Information Systems," 2008.

[29] J. Esteves, J. Pastor and J. Casanovas, "A goal/question/metric research proposal to monitor user involvement and participation ERP implementation projects. Information Resources Management Association Conference (IRMA)," 2003.

[30] L. Zhang, M. Lee and P. Banerjee, "Critical Success Factors of Enterprise Resource Planning Systems Implementation Success in China. Proceedings of the 36th Hawaii International Conference on System Sciences," 2003.

[31] H. Barki and J. Hartwick, " Measuring User Participation, User Involvement, and User Attitude. MIS Quarterly," pp. 59-82, 1994.

[32] Intellic Integration.

[33] G. Dowling, "Customer relationship management: in B2C markets, often less is more," no. 3, pp. 87-104.

[34] P. Kotler, "Marketing management," 2012.

[35] J. Wan, S. Tang, S. Zhaogang, D. Li, S. Wan, M. Imran and A. V. Vasilakos , "Software-Defined Industrial Internet of Things in the Context of Industry 4.0".

[36] K. Finkenzeller, " RFID technology- The theory and application of wireless radio inductional transponder and contactless IC card.," 2001.

[37] C. Yang, S. Weiminig and X. Wang, "The Internet of Things in Manufacturing Key Issues and Potential Applications," vol. 4, no. 1, pp. 6-15, 2018.

[38] L. Zhang and Z. Wang , "Integration of RFID into Wireless Sensor Networks: Architectures, Opportunities and Challenging Problems".

[39] D. Estrin, L. Giro, G. Pottie and M. Srivastavat, "Instrumenting the World with Wireless Sensor Networks, Acoustics, Speech, and Signal Processing," 2001.

[40] W. Deng, "Study of Smart Warehouse Management System Based on the IOT," in *Advanced in Intelligent Systems and Computing*, vol. 180.

[41] S. P. Jaikar and K. R. Iyer, "A Survey of Messaging Protocols for IoT Systems," 2018.

[42] N. Naik, "Choice of Effective Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP".

[43] T. Jaffey, "MQTT and CoAP, IoT protocols," Feburary 2014.

[44] A. A. Fuqaha, M. Guizani, M. Mohammadi and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," vol. 17, no. 4, 2015.

[45] T. Salman, "Networking Protocols and Standards for Internet of Things".

[46] A. Foster, "Messaging technologies for the industrial internet and the internet of things," 2015.

[47] N. S. Han, "Semantic service provisioning for 6LoWPAN: powering internet of things applications on web," 2015.

[48] J. E. Luzuriaga, M. Perez, P. Boronat and J. C. Cano, "A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks," 2015.

[49] G. Marsh, A. P. Sampat, S. Potluri and D. K. Pand, "Scaling advanced message queuing protocol (AMQP) architecture with broker federation and infiniband," 2008.

[50] R. Fullerton and C. McWatters, " The production performance benefits from JIT implementation," vol. 19, no. 1, pp. 81-96, 2001.

[51] Z. Guo, E. Ngai , C. Yang and X. Liang , " An RFID-based intelligent decision support system architecture for production monitoring and scheduling in a distributed manufacturing environment," pp. 16-28, 2015.

[52] Y. Xua and M. Chena, "Improving Just-in-Time manufacturing operations by using Internet of Things based solutions".

[53] R. Zhong, G. Huang , S. Lan, Q. Dai, T. Zhang and C. Xu, "A two-level advanced production planning and scheduling model for RFID-enabled ubiquitous manufacturing.," vol. 29, no. 4, pp. 799-812, 2015.

[54] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," pp. 180-187, 2015.

[55] M. M. Ahemd, M. A. Shah and A. Wahid, "Iot security: A layered approach for attacks and defenses," 2017.

[56] M. N. Aman, K. C. Chua and B. Sikdar, "A light-weight mutual authentication protocol for iot systems," 2017.

[57] J. Liu, C. Zhang and Y. Fang, " A differential privacy framework to defend smart homes against internet traffic analysis," vol. 5, no. 2, pp. 1206-1217, 2018.

[58] U. Guin, A. Singh, M. Alam, J. Ca˜nedo and A. Skjellu, "A secure low-cost edge device authentication scheme for the internet of things," 2018.

[59] P. Varga, S. Plosz, G. Soos and C. Hegedus, "Security threats and issues in automation iot," 2017.

[60] C. Liu, P. Cronin and C. Yang, "A mutual auditing framework to protect iot against hardware trojans," 2016.

[61] H. Naeem, B. Guo and M. R. Naeem, "A light-weight malware static visual analysis for iot infrastructure," 2018.

[62] J. Sengupta, S. Ruj and S. D. Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," vol. 149, 2020.

[63] Y. Rahulamathavan, R. Phan, M. Rajarajan, S. Misra and A. Kondoz, "Privacy-preserving blockchain based iot ecosystem 1285 using attribute-based encryption".

[64] M. J. Smith and P. Carayon , "New Technology, Automation, and Work Organization: Stress Problems and Improved TechnoIog y ImpIementation Strategies".

[65] H. P. Breivold and K. Sandström, "Internet of things for industrial automation--challenges and technical solutions," 2015.

[66] T. Heer, O. G. Morchon, R. Hummen, S. L. Keoh, S. S. Kumar and K. Wehrle, " “Security challenges in the ip-based internet of things,” Wireless Personal Communications," vol. 61, no. 3, pp. 527-542, 2011.

[67] W. Z. Khana, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi and K. Salah, "Industrial Internet of Things: Recent Advances,enabling technologies and open challenges," vol. 81, 2020.

[68] P. Agrawal, A. Ahlen, T. Olofsson and M. Gidlund, "Long term channel characterization for energy efficient transmission in industrial environments," vol. 62, no. 8, p. 3004–3014, 2014.

[69] T. Olofsson, A. Ahlen and M. Gidlund, "Modeling of the fading statistics of wireless sensor network channels in industrial environments," vol. 64, no. 12, p. 3021–3034, 2016.

[70] E. Sisinni, A. Saifullah, S. Han and U. Jennehag, "Industrial Internet of Things: Challenges, Opportunites, and Directions".