www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 04, April-2022, pp: 24-34

e-ISSN : 2583-1062
Impact Factor : 2.205

INTERNET OF THINGS (IOT) IN AUTOMATED PRODUCTION: A REVIEW

Deepak A. Kulkarni[*1]

[*1]Department of Electronics and Telecommunication, ISBM University.

ABSTRACT

The next generation industry requirements are not restricted only to efficiency, safety, operational productivity but beyond that individualized products in a short time are the key features. This challenge can be achieved only by a combination of technologies. In this review work, the internet of things (IoT) is studied with reference to industrial automation and for this other technology like RFID, WSN and cloud computing are also referred. The review work shows that Industry 4.0 is possible with coordination and cooperation among these technologies, but against that data security should not be at the stack.

Keywords: RFID, WSN, IoT, Industry 4.0., Internet of things (IoT), Industrial internet of things (IIoT), Radio-frequency identification (RFID), Wireless Sensor Networks (WSNs), Cloud Computing (CC).

1. INTRODUCTION

Challenges of producing increasingly individualized products with a short lead-time to address a dynamic and global market and along with this other competition driven factors like continuous improvement in terms of efficiency, safety, operational productivity, and, especially, return on investment are the requirements of next generation of industry, also called, Industry 4.0. For this typical resources are converted into intelligent objects so that they are able to sense, act, and behave within a smart environment. The impact of Industry 4.0 goes beyond simple digitization as it takes on a much more complex form of innovation based on a combination of multiple technologies such as intelligent manufacturing, Internet of Things (IoT)-enabled manufacturing, and cloud manufacturing. The main pillars of the intelligent industry are IoT, Cyber-Physical Systems (CPS) and Big Data. The term IoT refers to physical and virtual objects connected to the Internet. The IoT is also defined as the industrial internet, being a new technology in which global networks of machines and devices are capable of interacting with other networks [1], [2]. Thus, the connectivity between intelligent mobility, logistics, buildings, devices, and smart grids could form a form of a smart factory. Today, IoT is part of our daily lives. It is always present when we use the cell phone to turn on the television, switch on the kitchen oven outside the office, check the production of the power system, or find the fastest way to get from point A to point B, taking into account traffic conditions. To monitor and control production environments in real time, to check the conditions of equipment, and, if necessary, to schedule or let the equipment itself organize its maintenance, intelligent cars are monitored regularly and make safety decisions (i.e., stop, analyse road conditions, and self-adjust) or even request help [3]. This paper presents a detail review on IoT in automated production.

2. BACKGROUND AND EMPOWERING TECHNOLOGIES

The wide acceptance of IoT in manufacturing sector has a close connection with the development of IoT technologies. The core technologies are performing vibrant roles in IoT and benefit the manufacturing industry tremendously. This section is related to a brief explanation of some of these technologies.

2.1 Radio-frequency identification (RFID) technology

RFID practices electromagnetic fields to transfer data, for automated identification and tracking of tags attached to objects [4]. RFID systems comprise of RFID tags and readers. RFID tags are attached on the objects that have information about the objects. While RFID readers read the information (the unique IDs), and convey that information that to the enterprise information system. Therefore, the readers can track the tag's physical movement in real-time and thereby the objects to which the tags are attached. In manufacturing sector, RFID can be implemented in supply chain management [5], production planning [6], parts as well as vehicle tracking.

2.2 Wireless Sensor Networks (WSNs) technology

WSNs are consisted of spatially-distributed autonomous nodes. These nodes have the ability to sense the environment, to conduct computations of collected information, and communicate the computations with other nodes [7]. The sensor nodes function in a self-organized and work in decentralized fashion that sustains the best connectivity as long as possible and directs the data with multi-hop spreading to the base station. They have to work in cooperation and follow collective signal and information handling techniques to achieve the tasks. Every individual node is very tiny and limited-energy identity with weak processors and a restricted amount of memory. These features cause substantial

impact on the strategy and application of WSNs. WSNs have their own beneficial features like flexible deployment and configuration, convenient wireless integration. These features make them attractive prospective applicant in various setups of sensing-based manufacturing and decision-making.

RFID and WSNs symbolize two corresponding technologies [8]. RFID can be used to identify and recognize objects that are not easily noticeable or distinguishable by using traditional sensor technologies, but with the limitation that not monitor the condition of objects [9]. Relatively, WSNs can make available information regarding the condition of the objects and environment, and at the same time support multi-hop wireless communication. In some cases WSNs are prepared with actuators to achieve suitable physical activities. RFID and WSNs are competent technologies [10].

2.3 Cloud Computing and Big Data

Founded on the technology of virtualization and the Service Oriented Architecture (SOA), Cloud Computing (CC) functions. It makes possible the well-organized management of an enormously huge joint pool of configurable computing resources like storage, networks, servers, applications, and services that can be swiftly provisioned and released with negligible organizational effort or service provider communication [11]. It has crucial features, like measured service e.g. pay-as-you-go model, on-demand access, rapid elasticity resource pooling (multi-tenant). CC have the potential of transforming the manufacturing sector [12]. Cloud Manufacturing (CMfg) is also attracting wide attention in manufacturing paradigm [13] [12]. The very existence of IoT depends on Big Data (BD). BD is a comprehensive term for complex and large datasets that traditional data processing technologies are inadequate to work [14]. BD has three characteristics that can be identified by alphabet "V", 1) volume of data, about terabytes of data, 2) variety of data. Data is heterogeneous, text of structured and unstructured type, video, images, etc.3) velocities i.e. speed of data formation and data processing. [15]. The lifecycle of BD comprises five phases of data acquisition namely extraction, integration, analysis and interpretation [16]. The demands from big data also speed up the advance of cloud computing. Specifically to manufacturing sector, big data can be useful in the products lifecycle, pointedly design improvement, quality, cost effectiveness, manufacturing intelligence and customer satisfaction [17]. Conclusively IoT's core technologies can re-shape the manufacturing sector.

3. LITERATURE REVIEW

The credit for taking the initial step towards building of industry 4.0, goes to the German government in the year 2010 and because of it, Germany maintains the status of becoming the most competitive manufacturing country over the globe. Industry 4.0 is a era of novel approach and to achieve results beyond possibilities over the past 10 years ago [18]. Industry 4.0 comprises of technological intervention with traditional manufacturing. This is similar to automation, which helps the manufacturers and consumers by involvement of large-scale Machine-to-Machine and Internet of Things (IoT) in communication and monitoring, along with self-diagnosis and new levels of analysis to provide a truly productive future. Industry 4.0, brings the evolution in the supply chain and production causing development of both automation and digitization. It is so broad term as it comprises self-optimization and self-configuration by machines and use of artificial intelligence to achieve complex tasks. This brings the new era of technology, known to be as industry internet of things (IIOT). [19].

The generalised components used in IoT can be mentioned as:

1) Industrial Control System: Industrial Control System is a general term used to define software and hardware integration to control critical infrastructure. They are generally developed using distributed control system(DCS), programmable logic control(PLC), supervisory control and data acquisition(SCADA) system, remote terminal units(RTU), control servers, human-machine interface(HMI), intelligent electronic device(IED) and many other industry-specific system[20].

2) Devices: Sensors, Interpreters, Translators, Transient Data Stores, Channels and Processors to provide data to the application user end. They provide machine to machine interaction, human to machine interaction and vice-versa capabilities to the Industrial Control System [21].

3) Transient Store: The Transient Data Store is a slave component to the master architecture where the transient representation of the data objects are stored temporarily ensuring to ensure durability during failure of the operation and system failure including networks.

4) Local Processors: They are low latency data processing system providing fast processing of data. And which can be integrated with the device itself for data processing. This processor can be classified into data filters, event managers, data processors, rule-based engine, signal detectors, algorithms, routers etc. [22]

5) Application: These provide insight to the field operations in real time, these applications help staff to manage the devices, interact with other systems, to manipulate the data. Notification, alerts, visualization help them to make effective and calculated decisions [23].

6) Channels: These are data exchange medium between the system and the application. It includes networks protocol, satellite communications, API, routers etc.

7) Gateways: Gateways provide a connection across various networks and protocols enabling data transfers between different IIOT devices. It includes intelligent signal routers, information transfer protocol etc.

8) Collectors: Collectors gather data from gateways using standard protocols. It can be of custom made, these kinds of devices vary from industry to industry depending upon the needs.

9) Processors: Processors are the heart in any kind of IIOT solutions. Their primary functions involve data transformations, signal detection, analytical models, complex event processing, etc.

10) Permanent Data Store: These are long-time data storage system connected to the IIOT system. They work as a historian for the devices along with data from different sources feeding data to the processors for advanced analytical processing and preparing models. It includes a massive amount of parallel processing data stores, cloud storage, data repositories, RDBMS, open source data etc. [24]

11) Models: There are basically two types of models in any IIOT solutions one is Analytical Model and another is Data Model. The data models provide a structure to the data while the analytical models are custom builds to meet industry specific needs. Models play a crucial role in any IIOT solutions; they are generally built by leveraging the data in permanent data stores, human experiences, and industry standards. The analytical models are trained using a historical data set or using advanced machine learning. For example clustering, regressions, mathematical, statistical etc. And some examples of data models are semantic models, entity relationship mapping, JSON, XML/XSD etc. [25].

12) Security: This is an important aspect of the IIOT based system. It runs through the pipelines from the source to consumption. It includes data authorization, encryption, authentication, user management, firewalls, masking etc. [26].

13) Computing Environments: The mentioned environment vary from industry to industry depending upon the business need and its landscape.

14) Fog Computing: Brings the analytics near to the source.

15) Cloud Computing: Scaling analytics globally across the industry.

16) Hybrid Computing: Mix of fog and cloud computing optimizing operations tailored for specific fields need [27].

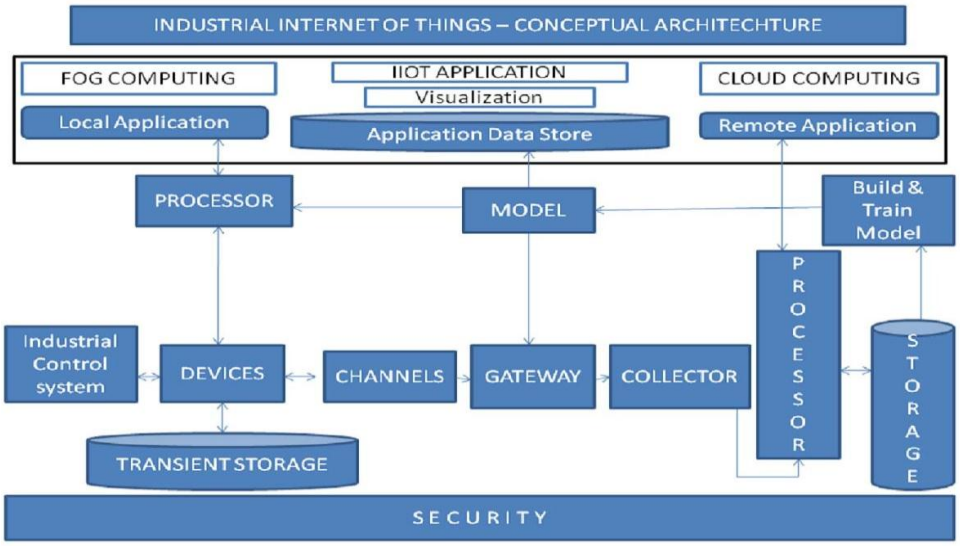

Fig.1. Conceptual architecture of IIOT

In another study on Supply chain management (SCM) in manufacturing sector, [28] in which object tracking was identified as a fundamental problem. The target of any logistics solution is to provide transparency and integrity control to ensure the delivery of the goods at the right time, place, quantity, condition and at the right cost. Smart logistics should provide some facility to the customers to know the status of the sensitive goods. So, it requires intelligent tracking of objects in transit. The focus was to eradicate the complications in old-style approach like manual counting, locating the object, and data management. For this Radio Frequency Identification (RFID) is identified as a perfect solution technology. Implementation of RFID in SCM increases the visibility of real-time object

movement and provides solutions for anti-counterfeiting. RFID is a chief precondition for the IoT, it facilitates the connection between physical objects to the Internet. Though lot of research work is conducted for object tracking by means of wifi technology, GPS and video cameras, the limitation of these technologies is that they just see the actual object, but not the characteristic changes of the object. The procedural steps are as below:

1. An object is attached with RFID tag embedded with sensor nodes. Sensor node collects data and writes in RFID tag.
2. An RFID reader in driver's mobile reads sensor data stored in the RFID tag and forwards it to cloud server.
3. Cloud Server (CS) stores reader, tag, user details and sensed data.
4. User / Application can access data stored in the cloud server for object tracking.

But after reviewing, it is estimated that the security and privacy risks in large-scale IoT systems are to be eliminated. In this work, architecture is proposed for a fine-grained IoT-enabled online object tracking system. Cloud storage used in this architecture enhances the scalability and data management. The proposed authentication protocol, registration phase, login and authentication protocol are discussed below:

Proposed Authentication Protocol

Table.1. List of notations and its description

Notation	Description	Notation	Description
I	Identity of the tag	K_R	Secret key of the reader
OW	Owner of the tag	$\|\| X_S CS_u$	String concatenation
T_{id}	Pseudo identity of the tag	⊕	Secret value of the CS
h(·)	One way hash function		Cloud to reader association
E[M, K]	Symmetric key encryption of the mes-		XOR operation
0, 1, 2, 3, 4, 5	Random numbers	UID	Hashed user identity
S_{UR}	Session key between user and reader	UPW	Hashed user password
S_R	Secret between reader and CS	TR	Tag—reader association
i	Identity of the ith reader	$TS_1, TS_2,$	Timestamps
R_i	Session key between reader and CS	TS_3	User reader association
S_{RC}	Session key between CS and user	R_u	Manufacturer's ID for the tag
S_{CR}		TID	

1. Registration Phase This phase is important for sharing the credentials within participating entities which are used in the authentication process. Reader Registration Phase In this phase, the RFID reader is registered with the cloud server.

Step RRP1: Reader sends Ri to the cloud server.

Step RRP2: Cloud server computes SRi = h(Ri ||Xs). Stores Ri and SRi in its database and sends ⟨Ri , SRi ⟩ to the reader in a secure channel. Now the reader possesses identity of the owner OW, the identity of the reader Ri and its secret value SRi .

User Registration Phase In this phase, user is registered with the cloud server and user to reader association is also established.

Step URP1: User selects its identity ID and Password PW and computes UID = h(ID) and UPW = h(PW). User sends ⟨UID, UPW, Ri ⟩ to the cloud server CS.

Step URP2: The cloud server extracts SRi corresponds to Ri from its DB. CS computes Ru = h(UPW||SRi) and CSu = h(UPW||Xs). Stores UID and UPW in its DB. CS sends Ru and CSu to the user in a secure channel.

2. Login and Authentication Protocol The user sends a login request to the cloud server. Cloud server checks the stored credentials with the received login request. Only if the user is authenticated, the request is forwarded to the reader. The reader does not possess any tag details, cloud server sends detail of the reader tag association information.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 04, April-2022, pp: 24-34

e-ISSN : 2583-1062
Impact Factor : 2.205

From that, the reader sends a request to the tag. The tag verifes the reader with the stored TR. Whenever the user wants to know the status of the object, the user sends a login request to the cloud server. The cloud server checks the stored credentials with the received login request. The steps involved in the login and authentication phase are as follows.

Step LAP1: User selects random number r0, r1 and computes and then sends M0 = ⟨UID, C, L0, L1, L2, L3, L4, TS1⟩ to the cloud server. The user prepares L3 and L4 messages for reader.

C = h(UID||UPW),

L0 = I ⊕ h(CSu||Ri ||r0),

L1 = CSu ⊕ r0, L2 = Ri ⊕ h(r0||CSU),

L3 = h(OW||Ru) ⊕ r1,

L4 = h(r1||h(OW)||h(UPW)||TS1||I)

And then sends M0 = ⟨UID, C, L0, L1, L2, L3, L4, TS1⟩ to the cloud server. The user prepares L3 and L4 messages for reader.

Step LAP2: Cloud server checks for the timestamp diference |TS2 − TS1| < Δt, in order to prevent the replay attack. Then it fetches UPW corresponds to UID from DB. Computes C∗ = h(UID||UPW) and verifes C∗ ? =C. Hence user is authenticated.

Cloud server computes

CS∗ u = h(UPW||Xs),

r0 = L1 ⊕ CS∗ u,

Ri = L2 ⊕ h (r0||CS∗ u) ,

I = L0 ⊕ h (CS∗ u||Ri ||r0)

It extracts SRi from DB corresponds to Ri . Fetches E[(Tid||Ri), KR] from DB, which indicates the tag-reader association. This fragment informs the reader that the tag to be connected is Tid, because reader does not store the tag details in its memory. Now the cloud server prepares the messages to be transmitted to the reader. It selects a random number r2 and computes

L5 = r2 ⊕ h(Ri ||SRi),

L6 = h(r2||Ri ||SRi ||TS2),

L7 = UPW ⊕ h(r2||Ri),

L8 = E[(Tid||Ri), KR] ⊕ UPW,

L9 = L6 ⊕ I ⊕ h(Ri ||SRi)

Cloud server sends the prepared message and part of the message received from the user as M1 = ⟨L3, L4, L5, L6, L7, L8, L9, TS1, TS2⟩ to the reader Ri .

Step LAP3: Reader checks for the timestamp diference |TS3 − TS2| <Δ t, in order to prevent the replay attack. Computes r2 = L5 ⊕ h(Ri ||Sri) and L∗ 6 = h(r2||Ri ||SRi ||TS2). Checks L∗ 6 ? =L6, if it is verifed, then cloud server is authenticated. Reader computes.

UPW∗ = L7 ⊕ h(r2||Ri),

R∗ u = h (UPW∗||SRi) ,

r1 = L3 ⊕ h (OW||R∗ u) ,

I = L9 ⊕ L6 ⊕ h(Ri ||Sri),

L∗ 4 = h(r1||h(OW)||h(UPW)||TS1||I)

It checks with received L4. If it is true then the user is authenticated. Reader then computes E[(Tid||Ri), KR] = L8 ⊕ UPW. Decrypts it and extracts Tid. Then , it selects a random number r3 and computes L10 = h(Tid||Ri) ⊕ r3, L11 = h(OW) ⊕ r3. Reader sends M2 = ⟨L10, L11⟩ to the tag Tid.

Step LAP4: Tag computes r3 = L10 ⊕ h(Tid||Ri) , L∗ 11 = h(OW) ⊕ r3. Tag then verifes L∗ 11 ? =L11. With this the tag can ensure that the request is from the authenticated reader which belongs to the same owner. Tag selects a random number r4 and computes

T'_{id} = r3 ⊕ r4 ⊕ Tid, L12 = h(Tid||Ri) ⊕ r4, L13 = T'_{id} ⊕ r4.

Tag sends M3 = ⟨L12, L13⟩ to the reader.

Step LAP5:

r4 = L12 ⊕ h(Tid||Ri),

T' $_{id}$ = r3 ⊕ r4 ⊕ Tid,

L∗ 13 = T'$_{id}$ ⊕ r4

Reader verifes L∗ 13 ? =L13, if it is true, then tag is authenticated to the reader and a new value for tag reader association is established and updated in the cloud server as

TR = E[(T'$_{id}$||Ri), KR]. Reader selects a random number r5 and computes

L14 = r1 ⊕ h(OW) ⊕ r5 ⊕ I,

L15 = L14 ⊕ SRi ⊕ r2,

L16 = I ⊕ r2,

L17 = TR ⊕ r2

Reader sends M4 = ⟨L14, L15, L16, L17⟩ to the cloud server. In this step reader authenticates the tag and updates TR in the DB. Also it prepares the message L14 for the user to authenticate the tag with the user.

Step LAP6: Cloud server computes L∗ 15 = L14 ⊕ SRi ⊕ r2 and verifes L∗ 15 ? =L15, if it is true, then the reader is authenticated. Cloud server computes I = L16 ⊕ r2, TR = L17 ⊕ r2 and updates TR in EHT. Also it computes L19 = L14 ⊕ r0 and sends M5 = ⟨L19⟩ to the user.

Step LAP7: After updating EHT, cloud server sends an acknowledgement to the reader as a challenge response. Then, reader sends a confirmation message to the tag to indicate that the pseudo id Tid in the tag's memory can be updated. This prevents the de- synchronization attack.

Step LAP8: User computes L14 = L19 ⊕ r0 andr5 = L14 ⊕ r1 ⊕ h(OW) ⊕ I. Now the user computes session key between the user and reader as SUR = h(r5||r1||UPW||Ri) and session key between the cloud server and user as SCU = h(r0||UID||CSu). Finally, session key between the cloud server and the reader is computed as SCR = h(r2||TR||Sri.

Proposed Object Tracking Protocol:

Step OSR1: The user prepares sensor data request messageSDreq = h(OW||T1) and sends N0 = ⟨UID, SDre, I, T1⟩it to the cloud server.

Step OSR2: The cloud server extracts TR corresponds to the I from its DB and sends N1 = ⟨TR, SDreq, T1⟩.

Step OSR3: The reader decrypts TR and extracts Tid. Then, reader computes SD∗ req = h(OW)||T1) and verifes SD∗ req ? =SDreq. If it is verifed reader ensures that it is not replay attack and it is from authenticated owner. It selects R1 and computes C0 = h(OW) ⊕ r1, C1 = SDreq ⊕ Tid ⊕ R1. Then, reader sends N2 = ⟨C0, C1⟩ to the tag.

Step OSR4: The tag computes R1 = h(OW) ⊕ C0. Tag prepares sensed data SDres = (SD||T2) ⊕ R1 ⊕ h(Tid||Ri)||h(SD||T2). Tag sends N3 = ⟨SDres⟩ to the reader.

Step OSR5: The reader prepares (SD||T2) = SDres ⊕ R1 ⊕ h(Tid||Ri). It encrypts sensed data as C2 = E[((SD||T2)||h(SD||T2)), SCR] and sends N4 = ⟨C2⟩ to the cloud server.

Step OSR6: The cloud server computes C3 = E[C2, SCU] and sends N5 = ⟨C3⟩ to the user. The sensed data is encrypted and transmitted to the user in a confdential manner.

Step OSR7: The user decrypts and gets the SD prepared at T2. It computes h(SD||T2) and checks it with the received hash value. Only if it verifed the user obtains data integrity. User ensures the freshness of the message by checking the time diference |T1 − T2| < Δt.

Where Δt is an acceptable time delay between the sensed data request and the response received by the user. In the conclusion, performance analysis shows that the proposed protocol achieves security with less computation and communication cost regarding RFID tag. Formal security analysis is carried out to prove that the proposed protocol meets the security and privacy requirements.

In another study, industrial Internet-of-Things hub (IIHub) is proposed [29]. As we know that smart manufacturing is increasingly becoming the common goals of various national strategies. Smart interconnection is one of the most important issues for implementing smart manufacturing. However, Current solutions are not yet ready to realize smart interconnection in dealing with heterogeneous equipment, quick configuration and deployment, online service generation. To solve the issues, industrial Internet-of-Things hub (IIHub) is proposed, which consists of customized access module (CA-Module), access hub (A-Hub) and local service pool (LSP). A set of flexible CA-Modules can be configured or programed to connect heterogeneous physical manufacturing resources (PMRs). Besides, the IIHub supports manufacturing services online generation based on the service encapsulation templates, and supports quick

configuration and deployment for smart interconnection. Furthermore, related smart analysis and precise management have the potential to be achieved. Finally, a case study is given to illustrate the functions of the proposed IIHub, and to show how IIHub realizes smart interconnection.

The research work [30] is made with the intention of creation of a manufacturing cell at the shop floor level based on the concepts of Industry 4.0.

The current industry setup uses the following structure for establishing advanced automation:

(i) Level 1 (I/O): shows the inputs and outputs of devices installed on the factory floor;

(ii) Level 2 (Programmable Logic Controller - PLC): shows the controllers that establish the control logic of machines and devices;

(iii) Level 3 (Supervisory): shows the systems that monitor and supervise the information inherent in the machines and devices of the factory floor;

(iv) Level 4 (MES): refers to the management system of information flow in the production process and is related to the production system; and

(v) Level 5 (ERP): refers to the management system of the production chain and involves sales, purchasing, human resources, quality, engineering, production, and logistics, among others.

Fig. 1 illustrates the automation technology of modern plants, control devices, I/O modules and operator terminals in the control level; and then the process management level with computers for engineering, supervisory control and data acquisition (SCADA) and MES systems. Finally, there is the enterprise level with business processes and ERP systems, typically located on servers in the IT data center. Each of these levels is relatively well structured; individual devices can be clearly mapped to one of the levels.

The present research is relevant because it intends to automate a didactic manufacturing cell, which is installed in the Federal Institute of São Paulo, Campus São Paulo, Brazil. The proposed system allows implementation of the data acquisition process of the field level via PLC and supervisory systems, storage of the obtained data in the cloud computing, and making them available to the related MES and ERP systems and various users via the Internet of Things (IoT). Fig. 2 illustrates the Smart Factory vision proposed.

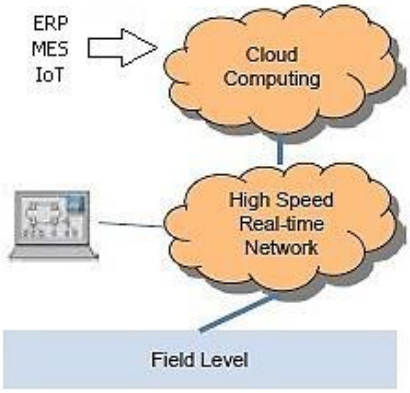

Fig.2. The Smart Factory vision.

Fig.3. Manufactured didactic mini-cell installed in the laboratory

To perform the practical tests of this work, a laboratory environment compatible with the concept of Industry 4.0 was developed: (i) IoT, (ii) CPS and, (iii) connectivity between the shop floor and IT levels.

Fig3 shows the manufacturing didactic mini-cell used for experimental testing of the developed system.

The system consists of: (i) PC Microcomputers, (ii) PLC, (iii) Human Machine Interface, (iv) Supervisory System, and (v) Switch/Router. To automate the production line and integrate the communication networks and embedded computers, an IoT based on the PLC was initially created. A CPS was then developed to allow simulation of the data exchange between the factory floor and Big Data (the cloud). The main function of the implemented CPS was to integrate IT systems (i.e., MES and ERP systems), communication networks, PLCs, and physical processes. The CPS was developed using Grafcet language, which is usually applied to program PLCs, and Ethernet TCP/IP network technology was used to monitor the various parameters of the manufacturing cell based on the SCADA supervisory system. The SCADA supervisory system employed in the CPS allowed monitoring and tracking of information related to the production process. The OPC-UA was the industry standard adopted for the interconnectivity of manufacturing cell devices. This standard allows industrial applications with different protocols to exchange data between each other and enables data access by one or more computers that use a client/server architecture.

Research Gaps

1. **Findings and future research directions**

Main themes & Description
Correlation analysis **Findings**: most studies are conducted in isolation, neglecting the global character of IoT and the correlations of the environmental, network-related and organizational levels **Future research**: conducting a correlation analysis based on the conceptual model to understand the relationships among levels and single aspects for a holistic view
Practical point of view **Findings** literature focus on challenges, identification of a scarcity of practical IoT applications in SCM with the food SC as pioneer because of perishable products and high requirements **Future research**: implementation of IoT projects for in-depth insights (e.g. reverse SC), evaluation of research findings and identification of practical influences
Technological **Findings:** research focus on technological aspects, particularly security issues, lack of standards and interoperability and hardware and software issues which 1) act as key enablers and 2) have high influence on further challenges and risks **Future research**: advancements of technological aspects to improve security and interoperability with special attention to RFID and connectivity
Organizational **Findings**: limited research regarding the influence of IoT on organizational structures, system implementation, employees and processes, with a variety of potential risks as well as the identification of high implementation barriers, especially for SMEs **Future research**: evaluation of the impact of IoT on organizational structures, employees and processes
Network-related **Findings**: identification of trust as crucial and complex prerequisite for the development of IoT projects and applications with relation to security issues, privacy concerns as well as lack of research regarding the SC reconfiguration and new competitors **Future research**: 1) development and influence of trust for IoT projects in regard to end customers, business partners or organizations and the SC 2) foundation, coordination and cooperation within SC networks and influence of SC innovation networks on IoT realization
Environmental **Findings**: missing business models beyond traceability-centric values and requirement for quantification of benefits (e.g. cost-benefit analysis), need for legal regulations and reduction of privacy concerns **Future research**: 1) derivation and evaluation of income-centric business models for IoT applications in SCM

and quantification of potential benefits (e.g. derivation of findings from RFID literature) 2) investigation of privacy issues of IoT applications and examination of the correlation of privacy concerns, security issues, trust and technological conditions as well as development of approaches for reduction of privacy issues				
Sr.No.	Author Name	Paper Title/ Journal	Conclusion	Research Gaps
01	H. S. Birkel and Evi Hartmann	Impact of IoT challenges and risks for SCM Supply Chain Management: An International Journal © Emerald Publishing Limited [ISSN 1359-8546] [DOI 10.1108/SCM-03-2018-0142]	Disruptive nature of this technology.	Holistic technology will be used
02	Debasish Mondal	The internet of thing (IOT) and industrial automation: a future perspective World Journal of Modelling and Simulation Vol. 15 (2019) No. 2, pp. 140-149	The real barriers in IoT implementation are cost, identification of competent vendors and training of employees. Adequate controller and computer capacity has to be installed. The software to run the process is a key factor for a successful implementation	Cost effective product will be made
03	S. Anandhi	IoT Enabled RFID Authentication and Secure Object Tracking System for Smart Logistics Wireless Personal Communications https://doi.org/10.1007/s11277-018-6033-6	Propose an end to end authentication protocol which prevents various known attacks.	end to end authentication protocol will be adopted
04	Fei Tao	IIHub: an Industrial Internet-of-Things Hub Towards Smart Manufacturing Based on Cyber-Physical System IEEE Transactions on Industrial Informatics	limitations in this paper are also existed for smart interconnection	will focus for smart interconnection
05	Chen Yang	Internet of Things in Manufacturing: An Overview	Privacy and security issues are crucial	Privacy and security issues be focussed
06	Mohamed Abdel-Basset	Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems	More involvements from more companies will make our	Will try to involve more companies

		Future Generation Computer Systems	research better.	

4. IOT ADVANTAGE

Among the various important and turbulent applications, Predictive monitoring maintenance is an important one. It comprises of many sensor data as possible, such as vibration, temperature, humidity, density, current, voltage etc. by the use of machine learning. Some machine learning algorithms can predict failure in advance. Every company wants to minimize the number of accidents, environmental incidents, zero safety incidents, and zero break downs. Sensors on any machine can check the machine health data points and give warnings accordingly, but what this type of devices can't do is to tell why or when the system will fail. The idea of predictive maintenance is to build a system which can provide accurate probability predictions on the data, rather than only reporting it. For example, the whole manufacturing unit of a company can be controlled by an automated system. The system can predict when a component is going to fail and it can place an order for the component so that the order arrives in time for the maintenance crew to replace within a time schedule, so the overall efficiency of the unit remains unchanged. This creates a productive output with high-cost efficiency [31].

5. CONCLUSION

Internet of Things and Industrial Internet of Things has immense power to provide various applications across different commercial and industrial domains. This review provides a research and application roadmap with its broad visions. All industrial systems need to be very much sensitive about the safety and security of the IIOT devices to prevent harm to the assets and personnel. Further research work needs to be carried out related to security issues surrounding IIOT.

6. REFERENCES

[1] J. Wan, S. Tang, Z. Shu, D. Li, S. Wang, M. Imran, and A. V. Vasilakos, "Software-Defined Industrial Internet of Things in the Context of Industry 4.0," IEEE Sensors Journal, vol. 16, no. 20, pp. 7373-7380, 2016.

[2] T. Y., Chen, Y. M. Yang, D. L. Chen, and Y. C, "New Method for Industry 4.0 Machine Status Prediction - A Case Study with the Machine of a Spring Factory," 2016 International Computer Symposium (ICS), pp. 322-326, 2016.

[3] J. Bohuslava, J. Martin, H. Igor, "TCP/IP Protocol Utilization in Process of Dynamic Control of Robotic Cell According Industry 4.0 Concept," 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), pp. 217-222, 2017.

[4] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381-394, 2006.

[5] A. Sarac, N. Absi, and S. Dauzère-Pérès, "A literature review on the impact of RFID technologies on supply chain management," International Journal of Production Economics, vol. 128, no. 1, pp. 77-95, 2010.

[6] G. Q. Huang, Y. F. Zhang, and P. Y. Jiang, "RFID-based wireless manufacturing for real-time management of job shop WIP inventories," The International Journal of Advanced Manufacturing Technology, vol. 36, no. 7-8, pp. 752-764, 2008.

[7] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer networks, vol. 52, no. 12, pp. 2292-2330, 2008

[8] L. Wang, L. Da Xu, Z. Bi, et al., "Data cleaning for RFID and WSN integration," IEEE Transactions on Industrial Informatics, vol. 10, no. 1, pp. 408-418, 2014.

[9] H. Liu, M. Bolic, A. Nayak, et al., "Taxonomy and challenges of the integration of RFID and wireless sensor networks," IEEE Network, vol. 22, no. 6, pp. 26-35, 2008

[10] P. Mell and T. Grance, "Perspectives on cloud computing and standards," National Institute of Standards and Technology (NIST). Information Technology Laboratory; 2009.

[11] W. He and L. Xu, "A state-of-the-art survey of cloud manufacturing," International Journal of Computer Integrated Manufacturing, vol. 28, no. 3, pp. 239-250, 2015.

[12] B. H. Li, L. Zhang, S. L. Wang, et al., "Cloud manufacturing: a new service-oriented networked manufacturing model," Computer Integrated Manufacturing Systems, vol. 16, no. 1, pp. 1–7, 2010.

[13] X. Wang, Y. He, "Learning from Uncertainty for Big Data: Future Analytical Challenges and Strategies," IEEE Systems, Man, and Cybernetics Magazine, vol. 2, no. 2, pp. 26-31, 2016.

[14] V. Mayer-Schönberger and K. Cukierl, "Big data: A revolution that will transform how we live, work, and think," Houghton Mifflin Harcourt, 2013.

[15] H. V. Jagadish, J. Gehrke, A. Labrinidis, et al., "Big data and its technical challenges," Communications of the ACM, vol. 57, no. 7, pp. 86-94, 2014. [22] J. Li, F. Tao, Y. Cheng, et al., "Big data in product lifecycle management," The International Journal of Advanced Manufacturing Technology, vol. 81, no. 1, pp. 667-684, 2015

[16] https://www.arcweb.com/blog/what-are-iot-iiot-industry-40.

[17] https://www.automationworld.com/business-intelligence/article/21565035/utilizing-automation-to-improve-marketing-for-industry-40

[18] K.Y. Shin and H. W. Hwang, "AROMS: A Real-time Open Middleware System for controlling industrial plant systems ", International Conference on Control, Automation and Systems. Year 2008.

[19] J. DeNatale , R. Borwick , P. Stupar , R. Anderson , K. Garrett , W. Morris and J.J. Yao,"MEMS high resolution 4-20 mA current sensors for industrial I/O applications",TRANSDUCERS '03, 12th International Conference on Solid-State Sensors, Actuators and Microsystems. Digest of Technical Papers , Volume: 2,Year 2003.

[20] L. Zhou , D. Wu , J. Chen and Z. Dong,,"When Computation Hugs Intelligence: Content-Aware Data Processing for Industrial IoT", IEEE Internet of Things Journal , Volume: 5 , Issue: 3 , June 2018

[21] V. Domova and A. Dagnino, " Towards intelligent alarm management in the Age of IIOT ", 2017 Global Internet of Things Summit (GIoTS).

[22] I. A. Brusakova , A. D. Borisov , G. R. Gusko , D. Y. Nekrasov and K. E. Malenkova," Prospects for the development of IIOT technology in Russia", IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) Year: 2017.

[23] A. Jayaram, "An IIOT quality global enterprise inventory management model for automation and demand forecasting based on cloud", 2017 International Conference on Computing, Communication and Automation (ICCCA).

[24] L. Zhou and H. Guo, " Anomaly Detection Methods for IIOT Networks", IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI),Year: 2018.

[25] "Cloud Computing Innovation in India: A Framework and Roadmap", White Paper 2.0 ,IEEE, Dec. 2014

[26] Hendrik Sebastian Birkel and Evi Hartmann, Impact of IoT challenges and risks for SCM Supply Chain Management, Friedrich-Alexander-Universität Erlangen-Nürnberg, Nürnberg, Germany

[27] S. Anandhi et.al. IoT Enabled RFID Authentication and Secure Object Tracking System for Smart Logistics Springer Science+Business Media, LLC, part of Springer Nature 2018

[28] IIHub: an Industrial Internet-of-Things Hub Towards Smart Manufacturing Based on Cyber-Physical System Fei Tao, Jiangfeng Cheng, and Qinglin Qi, : DOI 10.1109/TII.2017.2759178, IEEE Transactions on Industrial Informatics

[29] Internet of Things in Automated Production Cleiton Mendes, Raphael Osaki, and Cesar da Costa EJERS, European Journal of Engineering Research and Science Vol. 2, No. 10, October 2017

[30] The benefits of the industrial internet of things : lee teschler ,GE digital, april 22, 2016.