Benefits, challenges, and opportunities in adoption of Industrial IoT

Abishi Chowdhury[a], Shital A Raut[a]

[a]*Department of Computer Science and Engineering, Visvesvaraya National Institute of Technology, Nagpur, Maharashtra, India 440010.*

Corresponding email : abishi.chowdhury@gmail.com

Abstract:

The accelerated advancement of Internet of Things (IoT), ubiquitous computing, and sensing technologies, is gaining immense attention from a wide range of industries. Consequently, a huge number of industries are integrated with IoT and form Industrial IoT (IIoT) in order to build their applications with more improved functionalities like scalability, flexibility, time and cost savings, efficiency, and connectivity. This article presents an overview of IIoT architecture, its basic elements, and protocols. In addition, the article also highlights the key benefits and application areas of IIoT. Despite all the advantages an IIoT can grab, there are many industries that are worried to integrate their organizations with IoT. This article addresses some of the major challenges that still prevent certain organizations to adopt IIoT.

Keywords: Industrial Internet of Things, Heterogeneity, Ubiquitous Connectivity, Industry 4.0.

1. Introduction

Internet of Things (IoT), first coined by technology pioneer, Kevin Ashton in the year 1999 is indeed one of the biggest emerging technology rebellions, that aims to transform the daily surrounding objects into programmable networked devices with the aid of Ubiquitous connectivity, Radio Frequency Identification (RFID), and sensor network technologies (Ashton, Kevin, 2009, Rowland, Claire, et al., 2015). As a result, IoT is changing our daily objects in such a way that they are accomplishing our need with or without our little concern or interventions; phones became smart phones, TV became a smart TV, home became smart home, the city became a smart city, and so on. Gradually, IoT extends well beyond the city, home and consumer-level apparatus. Several asset heavy industries such as logistics, manufacturing, mining, utilities, oil, agriculture, and so many others have also initiated to use IoT. IoT standardization needs to be developed in order to bring tremendous economic benefits. In accordance with GE-Digital (Columbus, Louis, 2016), it is expected that the investment in the industrial IoT (IIoT) will reach $60 trillion within 15 years and more than 50 billion assets will be linked to the Internet by 2020. IIoT incorporates a series of advanced technologies, such as machine learning and big data analytics, M2M communication, sensor data utilization and automation technologies to provide leading IoT applications for industries. Especially, for manufacturing industries, IIoT holds great potential for quality control, sustainable and green practices, supply chain traceability and overall supply chain efficiency (Da Xu, Li, Wu He, & Shancang Li, 2014). Thus, there is an enlarging curiosity and attraction towards involving potential IoT technologies in various industries. An IoT eco-system can be considered as the encapsulation of numerous tiny networked devices that interact through different sensing and communication technologies; thereby forms a global networking system (Y. Li, M. Hou, H. Liu, and Y. Liu, 2012). The most elementary and prerequisite technology for IoT is RFID that automatically aids machines or computers to identify and track objects, monitor and record metadata, and control solitary target through radio waves. The RFID readers allow an individual to automatically identify, track, and monitor any objects globally in real time (Jia, Xiaolin, et al., 2012). Due to the visible, flexible and reliable way of tracking objects, RFID is widely used in logistics and supply chain management, manufacturing, transportation and retailing, pharmaceutical production, since 1980 (C. Sun, 2012). On the other hand, in order to provide an efficient interconnection among the intelligent sensors, wireless sensor networks (WSNs), one of the core technologies of IoT, are adopting emerging standards 6LoWPAN or IPv6, which is the pivotal influence of the connectivity between WSN and IoT (Castellani, Angelo P., et al., 2010). It serves an extensive range of IoT applications starting from healthcare monitoring system to environmental monitoring, defense monitoring, traffic monitoring, industrial monitoring, and so on and so forth (W. He and L. Xu, 2014). With the rapid growth and advancement of wireless and sensing technologies, a greater number of smart devices are connected to the IoT network. Accordingly, a regular enhancement of related technologies is occurring as well, which in turn show a great influence on enterprise systems and information and communications technology (ICT) by means of improved connectivity, efficiency, scalability, time savings, and cost savings. However, the complex system structure and heterogeneity for integrating several hardware platforms and software technologies have resulted in several challenges which are the main motivation for this study.

1.1. Motivation

A typical IIoT ecosystem application comprises distinct heterogeneous devices that cooperate with the help of prominent sensing and communication technological solutions. In a broader perspective, different IIoT ecosystem applications may need to communicate frequently in order to achieve some complex integrated industrial solutions. Thus, there are intercommunication/message passing takes place among a diverse range of heterogeneous IIoT devices or machines. Above all, most of the IIoT applications are built on the heterogeneous hardware and software platforms.

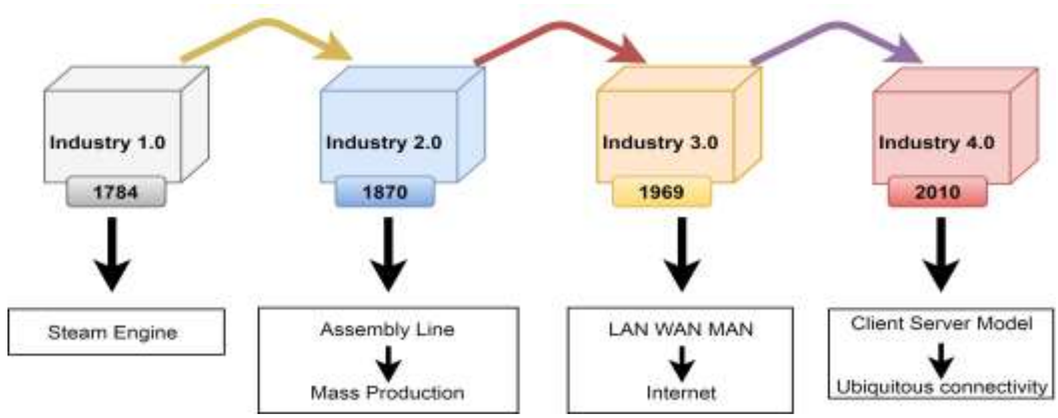

Fig. 1- Evolution of IIoT

Hence, heterogeneity is a big concern/challenge for the application developer as it provokes several other challenges like lack of standardization, integration with legacy technology, etc. in the complex IIoT applications. Also, security and risk management, and incompetent manpower are also the anxiety for the developers. Therefore, in this study, we briefly explain about IIoT and the typical IIoT architecture. Later, we summarize the key applications of IIoT and its potential benefits. Our primary contribution in this paper is to highlight challenges due to the heterogeneity of IIoT applications as well as devices/machines.

1.2. Paper Organization

The rest of the paper is organized as section 2 demonstrates the overview of IIoT; section 3 presents the basic IIoT architecture; the uses and applications of IIoT are discussed in section 4; section 5 highlights the key challenges; finally, section 6 concludes the paper.

2. Background of Industrial Internet of Things (IIoT)

2.1. What is IIoT?

A group of heterogeneous internet-connected or networked devices/machinery (from miniature sensors to composite industrial robots) along with the sophisticated heterogeneous software and hardware platforms that effectively produce the information from the data they generate, together form the IIoT (Lin, S. W., Miller, B., Durand, J., Joshi, R., Didier, P., Chigani, A., ... & King, A., 2015). Basically, IIoT is a small yet significant portion of a greater well-known concept called as the Internet of Things (IoT), the network of intelligent networked devices, computers, or things that share a massive amount of data through advanced wireless sensing technologies (WSNs) and store and process the data through cloud computing services. These two are the fundamental enabling technologies of IoT and with the help of these technologies; IoT provides automation in a series of smart ecosystems, like home, city, healthcare, and many industries. When these competencies are realized in the industrial environment, it has emerged as IIoT. A fusion of various technologies such as big data, machine learning, automation, and M2M communication that have lasted in the industrial place for several years, is needed for IIoT development (Mumtaz, Shahid, et al., 2017).

2.2. Evolution of IIoT

Starting from the first industrial revolution in the 18th century, IIoT has revamped as today's marketing industry. Fig. 1 shows the four stages of industrial evolution.

a) **First evolution: Industry 1.0** - With the invention of steam engines, a revolution began that boot started the Industry 1.0 in the year 1784. This was basically a manufacturing labor-oriented industry that further led to the industrial movement in terms of society with trains, and automation of manufacturing.

b) **Second evolution: Industry 2.0** - There was a great relief for the industrial workforce as their labor was reduced up to a satisfactory level when the father of mass production and the founder of Ford Motor Company, Henry Ford, developed the first automobile using the assembly lines in the year 1870. This era of mass production to some extent of automation is called Industry 2.0.

c) **Third evolution: Industry 3.0** - With the advancement of computers, networking technologies like LAN, WAN, MAN, etc., miniaturization of circuit boards, electronic technology, industrial robotics, and on the top of everything, the birth of Internet started Industry 3.0 in the year 1969 with much more automation.

d) **Fourth evolution: Industry 4.0 -** The integration of several assets heavy industrial objects with the smart devices through internet introduced the fourth industrial evolution; Industry 4.0 in the year 2010. From this period onwards, we have moved from the client-server model to the ubiquitous connectivity, a bridge between digital and physical environment. The devices b

Fig. 2- 9 technological components of Industry 4.0

n
ough to communicate with each other and construct strong visions. The enabling technologies of Industry 4.0 are IoT, cloud computing, big data and analytics, cognitive computing and artificial intelligence, advanced robotics, additive manufacturing, horizontal/vertical integration, cyber-security, and augmented reality and simulation which accelerate the automation and optimization of Industry 4.0 to the succeeding level (see fig. 2). Thus, Industry 4.0 stimulates a variety of opportunities in case of predictive maintenance, end-to-end supply chain, collaborative paradigms, new interesting business models, security models for cyber-physical systems, etc. (Upadhayay, J., 2017).

3. IIoT Architecture

3.1. Elements of IIoT

A conventional IIoT is a network of devices/machines interconnected through sensing and communication technologies that collect, track/monitor, and exchange valuable data, analyze the data to extract meaningful information in order to carry out faster and smarter business decisions (Lin, S. W., Miller, B., Durand, J., Joshi, R., Didier, P., Chigani, A., ... & King, A., 2015, Ungurean, Ioan, Nicoleta Cristina Gaitan, and Vasile Gheorghita Gaitan, 2016]. Fig. 3 depicts the basic referential architecture of IIoT.

An IIoT system is composed of 4 basic elements:

- intelligent assets - the smart applications, sensors and security components, and controllers
- data storage and processing infrastructure (e.g. cloud platform)
- application and analytics for producing business information from raw data
- agents

3.2. Drivers of IIoT

- **Technologies:** Robotics and automation, smart sensors, big data and analytics, cloud, scalability of IPv6-3.4X 10^38 IP address, low power hardware devices, software platforms, RFID tags, etc. are the major drivers for IIoT.
- **Customer behavior:** After all, to achieve the overall satisfaction of the customer is the main intention of an enterprise as it promotes the reputation of the service provider.
- **Macroeconomic Drivers:** Smart factories, Make In India, Fiscal or Monetary Policy, Consumer Price Index (CPI), Government policies like Industry 4.0, Policies by regulatory bodies, etc. act collaboratively for the IIoT evolution.

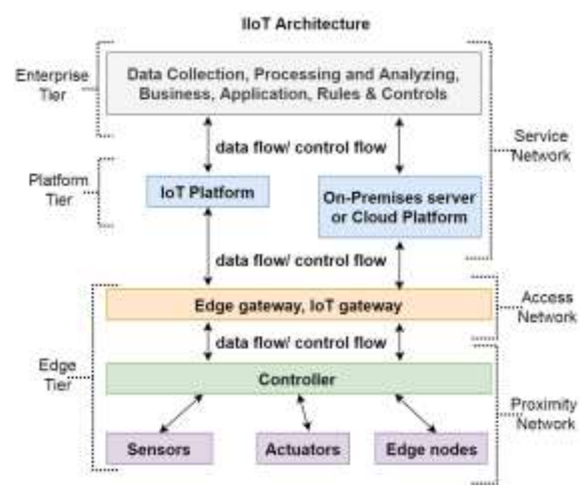

Fig. 3- A 3-tier architecture of IIoT

3.3. IIoT Protocols

One of the challenges faced in the progress of IIoT is its adopted protocols that are being used historically by the edge network for communication purpose. However, the light-weight and publish/subscribe protocol: Message Queueing Telemetry Transport (MQTT) protocol, the M2M communication protocol: OPC Unified Architecture (OPC UA) protocol, AMQP (Advanced Message Queuing Protocol), DHTP – The DataHub Transfer Protocol, REST (REpresentational State Transfer)

Table 1: Comparison among some important IIoT protocols

Criteria	Protocols				
	MQTT	**OPC UA**	**AMQP**	**DHTP**	**REST**
Real-time	Partial	Yes	Partial	Yes	No
Scalability	Yes	Partial	Yes	Yes	No
Closed Firewalls	Yes	No	Yes	Yes	Yes
Interoperability	No	Yes	No	Yes	No
Low bandwidth and low latency	Yes	Partial	Yes	Yes	No
Quality of Service (QoS)	Weak	Partial	Weak	Yes	No
Intelligent overload handling	No	No	No	Yes	No
Failure notification	Weak	No	Weak	Yes	No
Support daisy-chained servers	Weak	No	Weak	Yes	No

protocol, etc. are currently used for industrial automation (Meng, Zhaozong, et al., 2017). Table 1 shows a brief comparison among different protocols of IIoT.

4. Uses, Applications, and Benefits of IIoT

4.1. Why IIoT?

The IIoT can be immensely beneficial for industrial organizations by offering enhanced scalability, connectivity, reliability, time savings, cost savings through predictive maintenance, improved security and safety measures, and far more operational capabilities (Lu, Yang, 2017).

- **Production Industry –** Nowadays, most of the IIoT technologies are being employed in production industries for predicting potential threats or faults and rectifying them by self-monitoring IIoT-enabled equipment. Thus, it achieves a lower downtime and higher efficiency.
- **Supply chain –** With the automation of sensor-based inventory management system, it has been possible to check the overall ordering supplies right before they become out of stock. As a result, the overall waste produced can be minimized up to a great extent and the workers can focus on other jobs.
- **Retail –** The fast and intelligent decision-making power of IIoT technology enables the storefronts to automatically update as per the consumers' interest which in turn increase the overall revenue of the individual stores.
- **Healthcare –** Even IIoT technology can remotely monitor the health-related issues of patients and notify for preventive measures when there is a sudden change in normal readings. With the advent of AI technologies, it becomes easy for the doctors to provide correct diagnosis and necessary precautions quickly.
- **Building management –** The overall security and safety of buildings can be improved with modern IIoT technologies. The overhead of guesswork and irritation involved in modifying the building's atmosphere manually can be abolished; thus, overall management of buildings can simpler.

4.2. IIoT Applications

With the fast growing of industrial evolution, the IIoT enabled applications are spreading in every sector of the social and economic world rapidly. Some of the eminent IIoT enabled applications are discussed as follows (Lee, In, & Kyoochun Lee, 2015):

a) Digital/connected factory

IIoT enabled devices/machinery can deliver functional information to the primary manufacturers and to the field engineers to remotely handle the factory units through automation. Thus, an optimized digitally allied unit can be established.

b) Inventory management

IIoT applications allow overseeing the events throughout the supply chain. Thus, complete inventory can be monitored and managed on a line-item level across the globe. This process can provide a realistic estimation of usable material, arrival of upcoming goods, the current progress of work, and notification to the customers of any substantial change. Essentially, the overall supply can be optimized and the cost in the value chain can be limited.

c) Plant Safety and Security

The combination of big data analytics and AI techniques with IIoT can improve the personal health and safety of the workers of a plant through supervising key performance indicators. Thus, health-related issues, accidents, injuries, loss or damage in the daily life of the workers can be efficiently monitored; hence it ensures overall safety and security.

d) Logistics chain management

In IoT, logistics chain is a leading composite problem. To make it simple, it can be treated as several service provider pools, each of which accommodates multiple enterprises that produce related services (Yin, Jie, Jun Li, & Peichao Ke, 2013). When a job is directed to logistics chain, the logistics chain manager will check whether the available service providers fulfill the request or not. If the request is accepted, then it is analyzed and is sent to corresponding pools. As each pool has several service providers, it is a vital task to find the suitable one. Thus, it effectively improves the overall reputation of logistics chain.

e) Packaging optimization

In order to meet the increasing demand of a controlled production system such as packaging and printing industry, an industrial IoT system can be treated as packaging and printing manufacturing system that can sense, transmit and process sensor data with effective IoT techniques and intelligent subtask scheduling methods can be applied for optimized objective gain. The system can handle multiple simultaneous production tasks and transportation of raw materials. The overall task cannot be implemented in a single facility. Therefore, several subtasks are formed and each of these is handled in one facility. In this context, AI-based subtask scheduling schemes try to minimize the cost and delay by overall cost optimization scheduling method and overall delay optimization scheduling method corresponding to the respective fitness function. This results in better production cost, production delay and average utilization for IoT-assist packaging and printing manufacturing system (Li, Wenxiang, et al., 2015).

f) Quality control

The sensors collect, analyze, and aggregate the business data and other third-party prudential plan or confidential data from different stages of business life cycle. At the early stage, this data contains raw materials of typical sensor readings which in the final stage comes out as the worthwhile information used in the final product. Therefore, a correct quality control mechanism can analyze all these inputs efficiently.

g) Cyber manufacturing system

From the Cyber-physical system (CPS), the notion of Cyber manufacturing has been derived. Big data analytics along with cloud computing, and AI technology enabled IIoT takes a significant role in designing the system and handling issues for efficient data management (Conway, John, 2016).

h) Facility management

The utilization of IoT enabled sensors in manufacturing apparatus endows maintenance alerts based on unforeseen conditions as there may be some critical machinery that is designed to operate under certain environmental condition. The sensors can dynamically check the proper working condition of the machines; thus, overall energy can be minimized, and operational efficiency will be enhanced.

Besides the above-mentioned application areas, IIoT is actively involved in the area of predictive and remote maintenance, smart environment, asset tracking, energy consumption optimization, smart farming, and agriculture, etc.

4.3. IIoT Benefits

After the evolution of Industry 4.0, the manufacturing and other associated industries became faster, more reliable, more user-centric, and efficient enough to explore outstanding business schemes which resulted in reduced downtime, maximize asset utilization, remote diagnosis, predictive and proactive maintenance, etc. The main advantages of IIoT have been listed down as follows (Lu, Yang, 2017):

a) Enhanced productivity through optimization and automation

Industry 4.0 enables the factories more flexible, and dynamic, furnished with intelligent sensors, actuators, and autonomous systems. As a result, the machines and parts have become capable enough for self-optimization and automation in the field of complex manufacturing processes. Hence, an optimized and qualified end product as per the expectation of providers can be achieved. Agent paradigm is an acceptable and recognized tool for smart manufacturing.

b) Cost savings

One of the primary goals of industry 4.0 is to reduce the overall cost by reducing waste production and increasing profitability. In this era of digitization and automation, errors due to uncertainty have been diminished, which in turn enhance the entire value chain. In the year 2016, there was an extreme profit of $102.5 billion on $178 billion for all the use cases of manufacturing.

c) Real-time monitoring

The ultimate demand of the customer is the speed and from a provider's perspective, it is the optimization of productivity. The reputation of the provider depends on how fast he fulfills the expectations of the users. Reputation is an important factor in the entire business world as it further increases the demand for the products which is the first goal of any marketing organization. Through real-time monitoring of production system, the overall speed of the productivity can be improved which impacts on the whole supply chain.

d) Better working conditions and sustainability

With the aid of modern ubiquitous computing and other enabling technologies of IIoT; real-time HVAC system, safety and security, cleanliness, humidity and radiation detection, communication and collaboration facilities have been advanced which provide a better and comfortable working environment for the factory people. Accordingly, the overall productivity and quality are also improved to a certain extent.

e) Improved agility

The industry manager needs to handle the scalability, flexibility, and agility in order to gain a total competitive benefit. Factory people anticipate this exact support from cloud and related technologies. Big data, robotics, AI, and CPS are there to meet these needs of flexibility, scalability along with agility to influence gains in optimal production demand from a better time and scale standpoint.

5. Challenges and opportunities of IIoT

Even though a wide range of applications with potential benefits, the adoption of IIoT still poses several challenges. According to the Morgan Stanley-Automation World Industrial Automation Survey in April, 2016, there are mainly nine threats that cause the barriers to the adoption of IIoT (Morgan Stanley, 2016). Fig. 4 illustrates the challenge percentage for each category. In this section, we list down some of the major challenges/barriers for IIoT adoption as follows (Da Xu, Li, Wu He, & Shancang Li, 2014, Mumtaz, Shahid, et al., 2017, Lu, Yang, 2017):

a) Heterogeneity of underlying machinery and enabling technologies

An amalgamation of a numerous heterogeneous devices/machines, complex system structure, and heterogeneous hardware and software platforms of IIoT have affected in challenges while communicating through sensing technologies and ubiquitous access to the machine generated shared data. Thus, heterogeneity is a big issue for IIoT applications as well (Ning, Huansheng, Hong Liu, & Laurence Yang, 2013).

b) Data integration challenges

Data is the key entity in IIoT. IoT enabled sensors collect the raw industrial data from various parts/sector of the enterprise. This data is very complicated as it can be structured or unstructured big data with varying dates. Thus, a complex relation lies between the data of different sectors. In order to use the data for the organizational benefits, it is necessary to integrate the data. Here, the challenge of data integration takes place because of the heterogeneity distinct sources.

c) Cybersecurity and data security

Cybersecurity and data security are one of the most challenging concerns in context of IIoT. The current Industry 4.0 and IoT together pledge to serve with robust business models through stable connectivity and efficient use of next generation ubiquitous embedded systems. These systems produce, analyze, and share critical and sensitive business data that needs to be more secure and protected from Cyber-attacks as this may severely damage the organization as well as it can be life threatening. Therefore, security and privacy together are the inherent challenge in IIoT eco-system. Through several a) pre-active phase security like symmetric and asymmetric key generation, key distribution techniques of cryptography; b) active phase security like authentication, secure routing, access control, group signature algorithms; and c) post-active phase security like intrusion detection, intrusion tolerance, and threshold cryptography; Cybersecurity and data security and privacy can be maintained (Sadeghi, Ahmad-Reza, Christian Wachsmann, & Michael Waidner, 2015). IEC62443 security standards and other existing industrial standards are evolving in order to include security prospect, e.g. DNP3 has become DNPV5 (Jeschke, Sabina, 2017).

d) Lack of standardization

As an effort to implant recent technology onto former, it encounters a wide range of dissimilar standards and design principles in each entity from transmission protocol to other actors in the IIoT eco-system. Most of the protocols designed to serve IIoT applications are new and lacking standardization (Palattella, Maria Rita, et al., 2013). A seamless communication is required between machines, regardless of operating system platforms, connectivity framework, or protocol standards as the industry needs a perfect collaboration to build ubiquitous IIoT interoperability paradigm. Therefore, standardization acts an important role in accomplishing this.

e) Integration with legacy technology

Integration of Industrial setting with IoT is more intricate than traditional M2M and networked devices as there is a requirement to modernize legacy devices fitness inadequacy and older protocols that are not affiliated with IIoT environment as well as implementation of state-of-the-art technologies (Breivold, Hongyu Pei, and Kristian Sandström, 2015). According to International Data Corporation (IDC), it is reported that almost 85 percent of installed machines and sensors that are in working state, cannot be able to connect to the Internet and send data to the cloud frequently. So, the industrial challenge is to integrate legacy devices with recent sophisticated technologies to overcome these flaws.

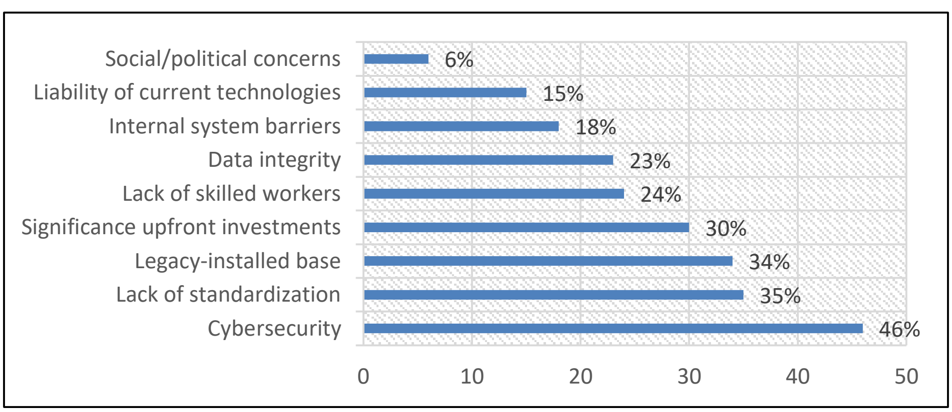

Fig. 4- Percentage challenges in implementing IIoT

f) Lack of skilled industry people/workers

A major reason why business organizations are still not eager to adopt IIoT as reported by survey is a lack of skilled workers. 36 percent of panels are in the dilemma due to bounded access to the appropriate skills and expertise which further affects the data integration and other necessary function for IIoT. According to (Morgan Stanley, 2016), 24 percent of the panel reported a lack of skilled labors. One thing that is for sure in this modern age of ubiquitous connectivity of the IIoT, companies cannot perform the entire task all alone. Thus, they must depend on current networking technologies, ecosystems, and operating platforms which are very critical to prevail.

g) Money

In order to automate everything, and to achieve optimization, it is essential to embrace modern technologies with skilled professionals and workers. So, organizations need to invest for up-front costs intelligently reminding the future profit. Unfortunately, a lot of industry people evidently anxious by the up-front costs.

6. Conclusion

In the age of automation, modernization of applications is essential in order to meet the expectations of users as well as to enhance the reputation of the organizations. Therefore, the organizations are shifting towards involving IIoT as the demand for IIoT applications is growing very fast nowadays. Through the industrial evolution, currently, Industry 4.0 plays a significant role in maximizing outcomes and managing successful pilots. However, a few potential threats like security, interoperability, heterogeneity are affecting industrial business today. So, in future, industries need to deal with disruptive technologies and meet new regulations.

References

Ashton, Kevin. That internet of things thing. RFiD Journal 22.7 (2009): 97-114.

Rowland, Claire, et al. Designing Connected Products: UX for the Consumer Internet of Things. O'Reilly Media, Inc., 2015.

Columbus, Louis. Roundup of Internet of Things Forecasts and Market Estimates, 2016. Forbes. Forbes, 27 Nov. 2016. Web. 14 Dec. 2016.

Da Xu, Li, Wu He, and Shancang Li. Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics 10.4 (2014): 2233-2243.

Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things," Inf. Technol. Manage., vol. 13, no. 4, pp. 205–216, 2012.

Jia, Xiaolin, et al. "RFID technology and its applications in Internet of Things (IoT)." Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. IEEE, 2012.

C. Sun, "Application of RFID technology for logistics on internet of things," AASRI Procedia, vol. 1, pp. 106–111, 2012.

Castellani, Angelo P., et al. Architecture and protocols for the internet of things: A case study. Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on. IEEE, 2010.

W. He and L. Xu, "Integration of distributed enterprise applications: A survey," IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 35–42, Feb. 2014.

Lin, S. W., Miller, B., Durand, J., Joshi, R., Didier, P., Chigani, A., ... & King, A., Industrial internet reference architecture. Industrial Internet Consortium (IIC), Tech. Rep, 2015.

Mumtaz, Shahid, et al. "Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation." IEEE Industrial Electronics Magazine 11.1 (2017): 28-33.

Upadhayay, J. (2017). The Evolution of Industrial IoT | Hitachi Vantara Community. [online] Community.hitachivantara.com. Available at: https://community.hitachivantara.com/community/iot/blog/2017/10/10/the-evolution-of-industrial-iot [Accessed 15 Nov. 2018].

Ungurean, Ioan, Nicoleta Cristina Gaitan, and Vasile Gheorghita Gaitan. "A Middleware Based Architecture for the Industrial Internet of Things." KSII Transactions on Internet & Information Systems 10.7 (2016).

Meng, Zhaozong, et al. "A Data-Oriented M2M Messaging Mechanism for Industrial IoT Applications." IEEE Internet of Things Journal 4.1 (2017): 236-246.

Lu, Yang. "Industry 4.0: A survey on technologies, applications and open research issues." Journal of Industrial Information Integration 6 (2017): 1-10.

Lee, In, and Kyoochun Lee. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." Business Horizons 58.4 (2015): 431-440.

Yin, Jie, Jun Li, and Peichao Ke. A provenance based scheduling algorithm for logistics chain in IOT. 2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering. Vol. 1. IEEE, 2013.

Li, Wenxiang, et al. "A scheduling method for IOT-aided packaging and printing manufacturing system." Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE), 2015 11th International Conference on. IEEE, 2015.

Conway, John. "The Industrial Internet of Things: an evolution to a smart manufacturing enterprise." Schneider Electric (2016).

Morgan Stanley. (2016). IIoT & the New Industrial Revolution. [online] Available at: https://www.morganstanley.com/ideas/industrial-internet-of-things-and-automation-robotics [Accessed 15 Nov. 2018].

Ning, Huansheng, Hong Liu, and Laurence Yang. "Cyber-entity security in the Internet of things." Computer (2013): 1.

Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. "Security and privacy challenges in industrial internet of things." Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015.

Jeschke, Sabina, et al. "Industrial internet of things and cyber manufacturing systems." Industrial Internet of Things. Springer, Cham, 2017. 3-19.

Palattella, Maria Rita, et al. "On optimal scheduling in duty-cycled industrial IoT applications using IEEE802. 15.4 e TSCH." IEEE Sensors Journal 13.10 (2013): 3655-3666.

Breivold, Hongyu Pei, and Kristian Sandström. "Internet of Things for Industrial Automation--Challenges and Technical Solutions." Data Science and Data Intensive Systems (DSDIS), 2015 IEEE International Conference on. IEEE, 2015.