Chapter 9
Challenges to Industrial Internet of Things (IIoT) Adoption

V. Shunmughavel
Computer Science & Engineering, SSM Institute of Engineering and Technology, India

ABSTRACT

The industrial internet of things (IIoT) has made its development within a short span of time. Initially it was considered as a novel idea and currently it is a major driver in industry applications. It has created productivity and efficiency for industries worldwide. This innovative technology can become a practical reality if engineers overcome a variety of challenges. They are connectivity, cost, data integration, trust, privacy, device management, security, interoperability, collaboration, and integration. In this chapter, several facts behind the above-mentioned challenges are being explored and addressed.

INTRODUCTION

The rapid development of IIoT within a short span of time has benefited industry applications. There are certain prime challenges in the adoption of IIoT. In the absence of a secure and properly encrypted network, the adoption of IIoT could lead to brand new security challenges and vulnerabilities (Gudlur, et al., 2020). The prime concern of IIoT is to focus on connecting more and more devices together. This leads to more entry points for malware. Each of these entry points need to be adequately protected against malware and malicious hacking, as well as accidental damage and penetration due to digital damage. The sensitive personal data gathered from devices must be protected from unauthorized access. The users have to be provided with required tools that help them to define the policies for sharing their personal data with authorized persons and applications for data privacy.

Due to the connection of different systems through IIoT, a difficulty to create real cross-domain services that will allow continuous movement of devices and data arises. The problem identified is that various protocols are being utilized and there is no standardization that will lead to interoperability (Phan, & Kim, 2020).There are multiple platforms, numerous APIs, and protocols available for IIoT integration. This leads to the inability of industry workers to operate the new solutions and over all productions process effectively due to their lack of understanding. Device management becomes a big challenge

DOI: 10.4018/978-1-7998-3375-8.ch009

since the usage and number of sensors, gateways and devices will be very large and populated over large geographical areas. The key to enable the Industrial Internet of Things will be connecting all the devices over long distances using cellular and satellite technology. A constant and reliable connectivity is the entire focus of IIoT. Thus, unreliable source of connectivity causes problems in implementing IIoT. When deploying an IIoT application, streams of data move from different sources such as sensors, contextual data from mobile device information, and social network feeds and other web resources. To preserve the semantics of the data in such cases of the data integration from multiple sources is very important.

The close collaboration between individuals and industries with diverse skills and domain knowledge is required to build an IIoT solution. Expertise in two different domains – Information technology (IT) and Operations Technology (OT) is required to build IIoT infrastructure. The major concern for most industries is the huge investment towards the cost of implementing an IIoT infrastructure and obtaining Return on Investment (ROI). Adopting more efficient production processes, and achieving better productivity might also result in increased economic sustainability (Nagy, et al., 2018).In IIoT, things usually move around and are not connected to a power supply, so their smartness needs to be powered from a self-sufficient energy source. Power saving is another challenge since radio frequency identification transponders do not need their own energy source. Their functionality and communications range are very limited. Trust management in IIoT is a major issue for integrating any advanced and automated technological solutions into the manufacturing process.

BACKGROUND

Many detailed studies, regarding vital Challenges and open research issues regarding the implementation of Industry 4.0, have been carried out. Several challenges and fundamental issues in various circumstances that occur throughout the implementation of Industry 4.0 were addressed (Wang, et al., 2016; Vaidya, et al., 2018). They were: 1) decision-making and negotiation, 2) industrial wireless network (IWN) protocols, 3) big data and its analytic, 4) system modelling and analysis, 5) cyber security issues and 6) interoperability, 7) Investment issues. Some of the technology challenges concerning the implementation of Industry 4.0 involve the development of smart devices, the establishment of network environments, big data analysis and processing and digital production (Zhou, Liu, & Zhou, 2015). Currently the volume of data collected by industrial internet of things (IIoT) applications is very huge, making it a challenge to offer platforms with adequate capacity and performance. It is essential to make a detailed analysis of several IIoT platforms in the market and before making the decision of which one to adopt (Moura, et al., 2018).

The lack of a digital strategy in line with resource shortage as well as the lack of standards and poor data security is the main obstacle for the technological implementation of Industry 4.0 (Schroder, 2016). The three greatest challenges connected with implementing Industry 4.0 proposed are standardization, work organization and product availability (Kagermann, et al., 2013).There are still issues and challenges to be coped with in regard to equipment intelligent requirements, deep integration networks and knowledge-driven manufacturing (Chen, et al., 2017).Interoperability is the main open issue in Industry 4.0.Accessibility, multilingualism, security, privacy, the use of open standards, open source software and data integration are the major facts to ensure high accuracy and efficiency of processes (Lu, et al., 2017). An interoperability framework is implemented in this research in which the system components can cooperate and offer the seamless operation from the device to the backend framework. The overall