Chapter 30
Securing the Internet of Things Applications Using Blockchain Technology in the Manufacturing Industry

Kamalendu Pal
https://orcid.org/0000-0001-7158-6481
City, University of London, UK

ABSTRACT

The manufacturing industry tends to worldwide business operations due to the economic benefits of product design and distribution operations. The design and development of a manufacturing enterprise information system (EIS) involve different types of decision making at various levels of business control. This decision making is complex and requires real-time data collection from machines, business processes, and operating environments. Enterprise information systems are used to support data acquisition, communication, and all decision-making activities. Hence, information technology (IT) infrastructure for data acquisition and sharing affects the performance of an EIS significantly. The chapter highlights the advantages and disadvantages of an integrated internet of things (IoT) and blockchain technology on EIS in the modern manufacturing industry. Also, it presents a review of security-related issues in the context of an EIS consisting of IoT-based blockchain technology. Finally, the chapter discusses the future research directions.

INTRODUCTION

Modern manufacturing has got a long history of evolution for several hundred years. The first industrial revolution began in the last part of the 18th century (Lukac, 2015). It symbolized production systems powered by water and steam, followed by the second industrial revolution, which started in the early part of the 20th century with the characteristics of mass labour deployment and manufacturing systems based on electrical power. The third industrial revolution began in the early part of the 1970s with automatic

DOI: 10.4018/978-1-6684-7132-6.ch030

production or manufacturing based on electronics and computer data communication technology. The concept of Industry 4.0 was put forward for developing the German economy in 2011 (Roblek et al., 2016) (Vogel-Heuser & Hess, 2016). Industry 4.0 is characterized by cyber-physical systems (CPS) production based on heterogeneous data and knowledge integration. It is closely related to the Internet of Things (IoT), CPS, information and communication technology (ICT), enterprise information systems (EIS), and integration of EIS. This way, a new generation of CPS controls industrial manufacturing and supply chain management (SCM).

Moreover, because of changes in the economic, environmental, and business environments, the modern manufacturing industry appears to be riskier than ever before, which created a need for improving its supply chain privacy and security. These changes are for several reasons. First, the increasingly global economy produces and depends on people's free flow, goods, and information. Second, disasters have increased in number and intensity during the recent decades. Natural disasters such as earthquakes, floods, or pandemic (e.g., coronavirus) strike more often and have a more significant economic impact. Simultaneously, the number of human-made disasters such as industrial sabotage, wars, and terrorist attacks that affects manufacturing supply networks has increased (Colema, 2006). These factors have created significant challenges for manufacturers, the country, and the global economic condition. Manufacturers must also deploy continuous improvement in business processes, which improve supply chain activities execution and security enhancement.

Besides, today's manufacturing industry inclines worldwide business operations due to the socio-economic advantage of the globalization of product design and development (Pal, 2020). For example, a typical apparel manufacturing network consists of organizations' sequence, facilities, functions, and activities to produce and develop an ultimate product or related services. The action starts with raw materials purchase from selective suppliers and products produced at one or more production facilities (Pal, 2019). Next, these products are moved to intermediate collection points (e.g., warehouse, distribution centers) to store temporarily to move to the next stage of the manufacturing network and finally deliver the products to intermediate storages or retailers or customers (Pal, 2017) (Pal, 2018).

This way, global manufacturing networks are becoming increasingly complicated due to a growing need for inter-organizational and intra-organizational connectedness that enabled by advances in modern Information technologies (e.g., RFID, Internet of Things, Blockchain, Service-Oriented Computing, Big Data Analytics) (Okorie et al., 2017) and tightly coupled business processes. Also, the manufacturing business networks use information systems to monitor operational activities in a nearly real-time situation.

The digitalization of business activities attracts attention from manufacturing network management purpose, improves communication, collaboration, and enhances trust within business partners due to real-time information sharing and better business process integration. However, the above new technologies come with different types of disruptions to operations and ultimate productivity. For example, some of the operational disruptions are malicious threats that hinder the safety of goods, services, and customers' trust to do business with the manufacturing companies.

As a potential solution to tackle the security problems, practitioners and academics have reported some attractive research with IoT and blockchain-based information systems for maintaining transparency, data integrity, privacy, and security related issues. In a manufacturing communication network context, the Internet of Things (IoT) system integrates different heterogeneous objects and sensors, which surround manufacturing operations (Pal, 2019) and facilitates the information exchange within the business stakeholders (also known as nodes in networking term). With the rapid enlargement of the data communication network scale and the intelligent evolution of hardware technologies, typical standalone IoT-based