


Chapter 9

Blockchain With the Internet of Things: Solutions and Security Issues in the Manufacturing Industry

Kamalendu Pal

 <https://orcid.org/0000-0001-7158-6481>

City, University of London, UK

ABSTRACT

The internet of things (IoT) is ushering a new age of technology-driven automation of information systems into the manufacturing industry. One of the main concerns with IoT systems is the lack of privacy and security preserving schemes for controlling access and ensuring the safety of the data. Many security issues arise because of the centralized architecture of IoT-based information systems. Another concern is the lack of appropriate authentication and access control schemes to moderate the access to information generated by the IoT devices in the manufacturing industry. Hence, the question that arises is how to ensure the identity of the manufacturing machinery or the communication nodes. This chapter presents the advantages of blockchain technology to secure the operation of the modern manufacturing industry in a trustless environment with IoT applications. The chapter reviews the challenges and threats in IoT applications and how integration with blockchain can resolve some of the manufacturing enterprise information systems (EIS).

INTRODUCTION

As a result 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 both 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

DOI: 10.4018/978-1-7998-5839-3.ch009

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. Simply put, manufacturers must deploy continuous improvement in business processes, which improve both supply chain activities execution and its security enhancement.

Besides, today's manufacturing industry (e.g., apparel, automobile) inclines to worldwide business operations due to the socioeconomic 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 the 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 ultimately customers lose 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 data communication network context, the Internet of Things (IoT) system integrates different heterogeneous objects and sensors, which surround manufacturing operations 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 applications may no longer satisfy the advanced need is for efficiency and security in the context of the high degree of heterogeneity of hardware devices and complex data formats. Firstly, burdensome connectivity and maintenance costs brought by centralized architecture result in its low scalability. Secondly, centralized systems are more vulnerable to adversaries' targeted attacks under network expansion (Pal & Yasar, 2020).

Intuitively, a decentralized approach based on blockchain technology may solve the above problems in a typical centralized IoT-based information system. Mainly, the above justification is for three reasons. Firstly, an autonomous decentralized information system is feasible for trusted business partners to join the network, improving the business task-processing ability independently. Secondly, multiparty coordination enhances nodes' state consistency that information system crashes due to being a single-point failure is avoidable. Thirdly, nodes could synchronize the whole information system state only by

25 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/blockchain-with-the-internet-of-things/280851

Related Content

The CyberSecurity Audit Model (CSAM)

Regner Sabillon (2022). *Research Anthology on Business Aspects of Cybersecurity* (pp. 77-139).

www.irma-international.org/chapter/the-cybersecurity-audit-model-csam/288674

ETP-AKEP Enhanced Three Party Authenticated Key Exchange Protocols for Data Integrity in Cloud Environments

Kalluri Rama Krishnaand C. V. Guru Rao (2022). *International Journal of Information Security and Privacy* (pp. 1-15).

www.irma-international.org/article/etp-akep-enhanced-three-party-authenticated-key-exchange-protocols-for-data-integrity-in-cloud-environments/310515

Risks and Impacts of Children's Engagement in Solid Waste Management Activities in Hawassa City, Ethiopia

Akalewold Fedilu Mohammed (2016). *International Journal of Risk and Contingency Management* (pp. 1-17).

www.irma-international.org/article/risks-and-impacts-of-childrens-engagement-in-solid-waste-management-activities-in-hawassa-city-ethiopia/158018

An Alternative Framework for Research on Situational Awareness in Computer Network Defense

Eric McMillanand Michael Tyworth (2012). *Situational Awareness in Computer Network Defense: Principles, Methods and Applications* (pp. 71-85).

www.irma-international.org/chapter/alternative-framework-research-situational-awareness/62376

Inducing Six-Word Stories From Curated Text Sets to Anticipate Cyberwar in 4IR

Shalin Hai-Jew (2018). *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (pp. 406-477).

www.irma-international.org/chapter/inducing-six-word-stories-from-curated-text-sets-to-anticipate-cyberwar-in-4ir/206792