


Chapter 8

The Industry 4.0 for Secure and Smarter Manufacturing

N. S. Gowri Ganesh

 <https://orcid.org/0000-0001-9627-0416>

Malla Reddy College of Engineering and Technology, India

N. G. Mukunth Venkatesh

Panimalar Engineering College, Chennai, India

ABSTRACT

Industry 4.0 and smart manufacturing are expected to transform current practices into new milestones of exponential growth with high intensity of velocity, scope, and system impact. Technological advancements in the fields such as artificial intelligence, internet of things (IoT), blockchain technology, and cyber physical systems have resulted in a breakthrough in capturing the potential to boost income levels and an improvement in the quality of life of various sectors of people worldwide. A continuous stream of input data generated by IoT devices can assist to closely monitor an industry's various production phases. Edge computing and AI process these data at the end node, while blockchain technology provides a distributed secure data environment for both financial and non-financial applications. Security measures must be built into all manufacturing systems, allowing for failsafe production and cyber threat protection. In this chapter, the authors look at how these technologies can be used in a variety of scenarios to boost productivity in the industry and its environmental elements.

INTRODUCTION

Contemporary industry has witnessed major impetus from the early 18th century due to the impact of great innovations in technology. The ultimate goal in each phase of the industry changes is to improve the efficiency of manufacturing reducing the wastage resulting into more production. Industry 4.0 or the 4th industrial revolution also sometimes referred to as Industrial Internet of Things (IIOT) in the manufacturing sector is the conglomeration of physical production and technology with that of smart digital technology using AI and machine learning, big data, cloud computing, IoT, blockchain Technol-

DOI: 10.4018/978-1-7998-8367-8.ch008

ogy, cyber physical systems and Edge computing. Always Industry works in tandem with the desired process, partners, products and the people. The challenge in the day to day operations of the company is to produce effective output to maintain the connectedness and obtain the insights of the real time data across all these entities. The interconnectivity is possible for the smart manufacturing in Industry 4.0 with these Industrial IoT devices connected to the cloud working with the assistance of Artificial Intelligence and is secured with the aid of blockchain technology. A continuous stream of input data generated by IoT devices can assist to closely monitor an industry's various production phases. The sensors at these locations can be linked to applications that can provide a visual representation of the operations. These applications are capable of not only presenting the data as it is in sequence towards being insightful, but also of displaying intelligence by predicting the output in the future in order to make the necessary decisions using the appropriate machine learning algorithms. Edge computing and artificial intelligence process these data at the end node and intermediate node levels, while blockchain technology provides a distributed secure data environment for both financial and non-financial applications. Blockchain technology is now a tried-and-true method for tracking goods in logistics. It is critical in smart manufacturing to discern among machine health tracking, predictive maintenance, and production scheduling. Deep learning algorithms are used in smart factories to control machines using time-series data. Edge computing in smart manufacturing has thus proven to improve processing time for the machine environment with a large number of tasks. Traditional manufacturing plants were not designed to work in conjunction with cybersecurity arrangements. When these industries transition to the new paradigm of IoT devices with IP-based systems, they are more likely to be attacked by hackers. There is a greater risk of cybercrime, which can result in unauthorized remote access, theft of intellectual property, data manipulation, signal interference, and data loss. Security measures must be built into all manufacturing systems from the start, allowing for failsafe production and cyber threat protection. Because manufacturing equipment has a long life cycle, it is also critical that the solutions chosen have built-in flexibility and advanced over-the-air updating solutions to prevent threats today and in the future. A suitable secure architecture can generate, distribute, and authenticate devices in order for them to interact with users and applications

BACKGROUND

Industry4.0 was first coined in 2011 by three engineers: Henning Kagermann (physicist and one of the founders of SAP) (Henning Kagermann, 2011), Wolfgang Wahlster (professor of artificial intelligence), and Wolf-Dieter Lukas (physicist and senior official at the German Federal Ministry of Education and Research) in the German language 'Industrie4.0' in an industrial fair at Hannover Messe. Since then, the term Industrie 4.0 has sparked a vision of a new Industrial Revolution and has sparked a vigorous, ongoing debate about the future of work, and hence society, among the German public. In 2013, Industry4.0 manifesto ("Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0. Final Report of the Industrie 4.0 Working Group," n.d.) was prepared by German National Academy of Science and Engineering (acatech). The discussion around this future vision eventually extended to other countries, with public awareness peaked in 2016 when the World Economic Forum met in Davos under the banner Mastering the Fourth Industrial Revolution. Industry 4.0-related issues are addressed and developed by the Public-Private Partnership (PPP) for Factories of the Future (FoF). The evolution of Industry4.0 is described as application of inventions and discoveries from time to time as tools and techniques with

21 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/the-industry-40-for-secure-and-smarter-manufacturing/291164

Related Content

Trust in Cognitive Assistants: A Theoretical Framework

Md. Abul Kalam Siddique and Yoji Kohda (2019). *International Journal of Applied Industrial Engineering* (pp. 60-71).

www.irma-international.org/article/trust-in-cognitive-assistants/222796

"Lex Lata" and "de lege Ferenda" for the R&D Law of Turkey

Serdar Türkeli (2013). *Industrial Dynamics, Innovation Policy, and Economic Growth through Technological Advancements* (pp. 307-331).

www.irma-international.org/chapter/lex-lata-lege-ferenda-law/68366

Practitioner's View on the Future of Economic Decision-Making in Project Management: A Research Note

Brian J. Galli (2019). *International Journal of Applied Industrial Engineering* (pp. 33-55).

www.irma-international.org/article/practitioners-view-on-the-future-of-economic-decision-making-in-project-management/233848

Facility Layout Planning

Hossein Hojabri and Elnaz Miandoabchi (2013). *Graph Theory for Operations Research and Management: Applications in Industrial Engineering* (pp. 212-223).

www.irma-international.org/chapter/facility-layout-planning/73160

Aircraft Development and Design: Enhancing Product Safety through Effective Human Factors Engineering Design Solutions

Dujuan B. Sevillian (2013). *Industrial Engineering: Concepts, Methodologies, Tools, and Applications* (pp. 858-886).

www.irma-international.org/chapter/aircraft-development-design/69319