Chapter 93
Cybersecurity Issues and Challenges in Industry 4.0

Ravdeep Kour
https://orcid.org/0000-0003-0734-0959
Luleå University of Technology, Sweden

ABSTRACT

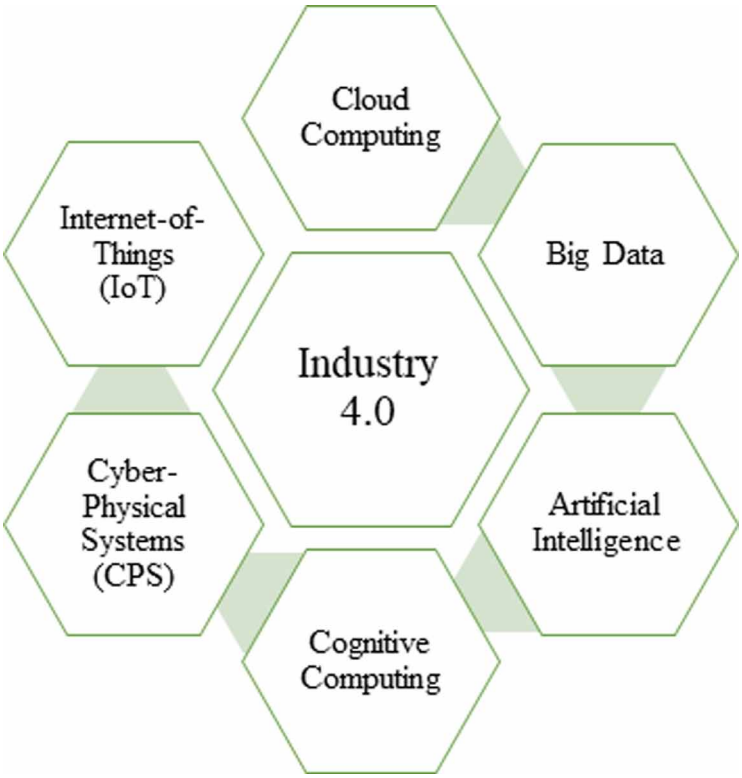
The convergence of information technology (IT) and operational technology (OT) and the associated paradigm shift toward fourth industrial revolution (aka Industry 4.0) in companies has brought tremendous changes in technology vision with innovative technologies such as robotics, big data, cloud computing, online monitoring, internet of things (IoT), cyber-physical systems (CPS), cognitive computing, and artificial intelligence (AI). However, this transition towards the fourth industrial revolution has many benefits in productivity, efficiency, revenues, customer experience, and profitability, but also imposes many challenges. One of the challenges is to manage and secure large amount of data generated from internet of things (IoT) devices that provide many entry points for hackers in the form of a threat to exploit new and existing vulnerabilities within the network. This chapter investigates various cybersecurity issues and challenges in Industry 4.0 with more focus on three industrial case studies.

INTRODUCTION

The evolution from Industry 1.0 as steam-powered machines towards Industry 4.0 as cyber physical systems (CPS) has brought many benefits in productivity, efficiency, revenues, customer experience, and profitability, but also imposes many challenges as managing human factors, often a critical element in several domains (Fontaine et al, 2016). One of the challenges is to manage and secure large amount of data generated from Internet-of-Things (IoT) devices that provide many entry points for an intruder (a person who attempts to gain unauthorized access to a system in order to compromise system availability, data Integrity or data Confidentiality) in the form of a threat to exploit new and existing vulnerabilities within the IoT network. Today, more and more organizations and businesses understand that an efficient flow of secured information creates major benefits, both economically and with greater customer satisfaction. To remain proficient and responsive, business processes must permanently transform themselves in this technological world of Industry 4.0 (Figure 1).

DOI: 10.4018/978-1-7998-8548-1.ch093

Figure 1. Industry 4.0



Industry 4.0 is a national strategic initiative from the German government where numerous elements comprising industrial systems are being interfaced with internet communication technologies to form the smart factories and manufacturing organizations of the future (Thames and Schaefer, 2017). The IoT connected devices itself is a superb innovation, but it also presents numerous points of entry for malicious activities. Figure 2 shows the number of connected IoT devices from year 2012 to 2025.

Figure 2. Number of connected IoT devices from year 2012 to 2025 (Columbus, 2016)