Chapter 3

Cybersecurity of Industrial Internet of Things

Gordana Gardašević
Faculty of Electrical Engineering, University of Banja Luka, Bosnia and Herzegovina

Lazar Berbakov
https://orcid.org/0000-0002-9628-2967
Mihailo Pupin Institute, University of Belgrade, Serbia

Aleksandar Mastilović
https://orcid.org/0000-0002-9130-619X
Communications Regulatory Agency BH, Bosnia and Herzegovina

ABSTRACT

The Internet of Things (IoT) is an emerging and even revolutionary technology with an immense impact on our everyday life. The Industrial Internet of Things (IIoT) is a fast-growing technology that increases productivity and efficiency by combining the IoT platform with an existing industrial environment. IIoT networks are one of the main pillars for the success of the future Industry 4.0 and Cyber-Physical System (CPS) paradigm. The IIoT ecosystem represents a network of connected industrial devices that exchange and analyze collected data to enable new insights into industrial processes. Recently, intensive research activities have focused on cybersecurity issues for the IIoT. This chapter addresses the critical components of the IIoT security framework by analyzing the relevant aspects and providing an overview of state-of-the-art activities in this field. This chapter also discusses the IIoT architectural structure, applications, and underlying networking technologies, with a particular focus on security challenges and standardization activities.

DOI: 10.4018/978-1-7998-2910-2.ch003
INTRODUCTION

The Internet of Things (IoT) refers to a global phenomenon that provides technology to support emerging applications in every single part of the worldwide society. Approaching the 21st century, many accessible technology buzzwords, besides the IoT, find a way to create their own space in the engineering community, such as Big Data, Artificial Intelligence (AI), Machine Learning (ML), Smart Industry 4.0, etc. (Institute of Electrical and Electronics Engineers [IEEE], 2017). Humanity has decided to collect data on everything, to correlate them, thus achieving in-depth and hidden knowledge on every parameter, process, or behavior. The Deep Knowledge unlocks possibilities to analyze, predict, and optimize processes and services at homes, cities, in an industrial environment, etc. It creates artificial smartness in the ambiance of conventional decision makings and non-optimized resource usage. Not only are all these technologies and solutions related to the IoT, but also many aspects of modern lifestyles and regular services (e.g., smart cities and local urban services). These opportunities enable the Digitalization and even more extensive – Digital Transformation, which affects not only the engineering aspect but also the social aspect of everyday life. These cumulative results of existing modern solutions create the new industrial and business environment. The 4th industrial revolution or Industry 4.0 launches the transition from automated manufacturing toward an intelligent manufacturing concept (Hermann, Pentek, & Otto, 2015). The Industry 4.0 concept envisions that Industries of the Future will rely on a network of connecting factories, machines, and other parts of the value chain. Such a network is used to effectively exchange information among different parts of the system, which results in improved industrial processes and reduced waste. Nowadays, assembled products enhanced with, e.g., Radio-Frequency Identification (RFID) tags, provide additional functionalities so that they can easily be identified and localized across the manufacturing line. In this way, an original product forwards information to the production line and to different parts of the production processes depending on their current status. This approach is particularly suitable for Small and Medium-sized Enterprises (SMEs), thus providing increased flexibility and the capability to produce smaller batches that adhere to the customer’s preferences.

For practical applications and scenarios, the IoT architecture enables massive sensors deployment within the measurement and detection network, which can sense the environment (Gardašević et al., 2017). From that perspective, the next step is an ability to create a proper mechanism for an automated reaction for predefined and learned triggers that mimics the reflex response of a living being. Systems with these abilities are named “responsive” and represent an advanced level of “smart” systems. From the telecommunications’ perspective and depending on the type of application and its technical requirements, two types of sensors deployment may be distinguished: Massive Machine-to-Machine (mM2M) communications and Critical Machine-to-Machine communications (cM2M). The most promising applications and scenarios for the IoT are in the industrial and finance sectors. In these sectors, there is a strong need for optimization and high investment prospect for advanced research and new applications.

The Industrial Internet of Things (IIoT) is a fast-growing technology that increases productivity and efficiency by combining the IoT platform with an existing industrial environment. IIoT networks are one of the main pillars for the success of the future Industry 4.0 and Cyber-Physical System (CPS) paradigm. The IIoT ecosystem represents a network of connected industrial devices that exchange and analyze collected data to enable new insights into industrial processes. As a result, it provides significant cuts in operational costs, reduces waste, improves quality, and increase the overall safety of industrial systems. Also, predictive maintenance, on its own, can bring significant benefits in terms of reduction of operation costs while also ensuring smooth and uninterrupted operation of critical infrastructure.
Related Content

**Light-Weight Content-Based Search for File Sharing Systems**
[www.igi-global.com/chapter/light-weight-content-based-search/16865?camid=4v1a](www.igi-global.com/chapter/light-weight-content-based-search/16865?camid=4v1a)

**The Open Source Community Choice: Automate or Die!**
[www.igi-global.com/chapter/the-open-source-community-choice/214438?camid=4v1a](www.igi-global.com/chapter/the-open-source-community-choice/214438?camid=4v1a)

**Modeling Data-Intensive Web Sites for Personalization, Integrity and Performance**
[www.igi-global.com/chapter/modeling-data-intensive-web-sites/22976?camid=4v1a](www.igi-global.com/chapter/modeling-data-intensive-web-sites/22976?camid=4v1a)

**An Approach to Faulty Reader Detection in RFID Reader Network**
Hairulnizam Mahdin and Jemal H. Abawajy (2012). *Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications* (pp. 70-84).
[www.igi-global.com/chapter/approach-faulty-reader-detection-rfid/63546?camid=4v1a](www.igi-global.com/chapter/approach-faulty-reader-detection-rfid/63546?camid=4v1a)