



Chapter 5

Malware Detection in Industrial Scenarios Using Machine Learning and Deep Learning Techniques

Ángel Luis Perales Gómez
University of Murcia, Spain

Lorenzo Fernández Maimó
 <https://orcid.org/0000-0003-2027-4239>
University of Murcia, Spain

Alberto Huertas Celdrán
University of Zurich, Switzerland

Félix Jesús García Clemente
 <https://orcid.org/0000-0001-6181-5033>
University of Murcia, Spain

ABSTRACT

In the last decades, factories have suffered a significant change in automation, evolving from isolated towards interconnected systems. However, the adoption of open standards and the opening to the internet have caused an increment in the number of attacks. In addition, traditional intrusion detection systems relying on a signature database, where malware patterns are stored, are failing due to the high specialization of industrial cyberattacks. For this reason, the research community is moving towards the anomaly detection paradigm. This paradigm is showing great results when it is implemented using machine learning and deep learning techniques. This chapter surveys several incidents caused by cyberattacks targeting industrial scenarios. Next, to understand the current status of anomaly detection solutions, it analyses the current industrial datasets and anomaly detection systems in the industrial field. In addition, the chapter shows an example of malware attacking a manufacturing plant, resulting in a safety threat. Finally, cybersecurity and safety solutions are reviewed.

DOI: 10.4018/978-1-7998-7789-9.ch005

INTRODUCTION

Nowadays, industry plays a fundamental role in our society since an essential part of the economy is based on this sector. Therefore, any advance that involves a significant increase in the industrial production of factories is associated with an improvement in the economy and, consequently, with the growth of countries. In this context, industrial processes automation has been the way followed by factories to increase production without increasing cost.

Decades ago, automation in factories consisted of small isolated elements capable of making measurements and, based on these measurements, performing certain types of actions. However, new technologies are being introduced progressively in the industrial ecosystem, facilitating the automation of processes. In recent years, new terms, such as Industry 4.0 (Lasi et al., 2014), Industrial Internet of Things (IIoT) (Boyes et al., 2018), and recently, Industry 5.0 and Society 5.0 (Perakovic et al., 2020), have emerged strongly. In general, these terms are related to each other and refer to introducing new smart devices in industrial factories. These devices use typical technologies of communication networks, such as Ethernet or WiFi, to exchange information between them. In addition, more and more factories are being connected to the Internet (Mirian et al., 2016) to provide new functions such as remote control or information sharing between factories in different geographical areas. In addition, and based on the Industry 5.0 paradigm, Artificial Intelligence (AI) techniques are being introduced in industrial scenarios (Skovelev et al., 2017).

Although Industry 4.0/5.0 comprises many different elements and the identification of its parameters is crucial (Perakovic et al., 2020), the core part of the factory automation are the Industrial Control Systems (ICS) that encompass a large number of heterogeneous devices whose goal is to control and supervise industrial processes. To achieve this goal, ICS comprise devices that operate in both the logical and physical layers of industrial processes. This is the reason why ICS are also known as Cyber-Physical Systems (CPS). Devices in the logical layer govern the system behavior, while devices in the physical layer, such as controllers and sensors, interact with the physical world.

ICS control and supervise the industrial processes from manufacturing industries to critical infrastructures such as power-grids or gas pipelines. They are placed from the second level to below in the automation pyramid, as shown in Figure 1. In the zero level of the pyramid, we found low-level devices nearest to the controlled process; in other words, the physical layer. Among these devices, actuators and sensors are responsible for getting information from the environment and making actions over the physical world. In the upper level, the Programmable Logic Controllers (PLC) are located. PLC serve as intermediaries between the lower level (sensors and actuators) and the next upper level. To be specific, PLC receive commands from the upper level that are transmitted to actuators/sensors. Sensors and actuators execute the commands received and send back the result to the PLC, which transmits it to the upper level. In the second level of the automation pyramid, we find the Supervisory Control And Data Acquisition (SCADA) systems (Boyer, 2019). These systems are responsible for monitoring and controlling all the devices in the ICS. At this level, we see devices and software closer to traditional networks than control networks are. For example, devices that incorporate web, database, and historian servers are located at this level. SCADA collect the information from different PLC and store it in databases. Most SCADA can manage alarms and display trend graphics and other useful information shown in Human-Machine Interface (HMI) devices. Operators use these devices to monitor the correct operation of the processes. If a process malfunction is detected, operators can interact with the process through the HMI. The last two levels of the automation pyramid are more related to business tasks than

18 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/malware-detection-in-industrial-scenarios-using-machine-learning-and-deep-learning-techniques/292232

Related Content

Exploring Barriers Affecting the Acceptance of Mobile Commerce

Priyanka Gupta (2016). *Securing Transactions and Payment Systems for M-Commerce* (pp. 234-250).
www.irma-international.org/chapter/exploring-barriers-affecting-the-acceptance-of-mobile-commerce/150078

Optimized Deep Neuro Fuzzy Network for Cyber Forensic Investigation in Big Data-Based IoT Infrastructures

Suman Thapaliya and Pawan Kumar Sharma (2023). *International Journal of Information Security and Privacy* (pp. 1-22).
www.irma-international.org/article/optimized-deep-neuro-fuzzy-network-for-cyber-forensic-investigation-in-big-data-based-iot-infrastructures/315819

Access Management as a Security Critical Factor: A Portuguese Telecommunications Company Case Study

Pedro Fernandes Anunciação and Eliana Nunes (2021). *International Journal of Risk and Contingency Management* (pp. 12-25).
www.irma-international.org/article/access-management-as-a-security-critical-factor/284441

Data Security and Chase

Zbigniew W. Ras and Seunghyun Im (2007). *Encyclopedia of Information Ethics and Security* (pp. 114-120).
www.irma-international.org/chapter/data-security-chase/13461

Current Network Security Systems

Göran Pulkkis, Kaj Grahnan and Peik Astrom (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 1339-1348).
www.irma-international.org/chapter/current-network-security-systems/23161