Deep Learning for Cyber Security Risk Assessment in IIoT Systems

Mirjana D. Stojanović
https://orcid.org/0000-0003-1073-5804
University of Belgrade, Serbia

Jasna D. Marković-Petrović
Public Enterprise Electric Power Industry of Serbia, Serbia

BACKGROUND

This section briefly reviews the theoretical background for cyber security risk assessment in the industrial IoT environment. Since identification of risks, threats and attacks precedes risk assessment process, the first part is dedicated to classification of cyber security risks, threats and attacks that are specific for IIoT systems. The second part surveys cyber security risk assessment of industrial systems in terms of actual standards, security principles and priorities, as well as classification of risk assessment methods. The final part discusses general use of machine learning for security and engineering risk assessment.

IIoT Cyber Security Risks, Threats and Attacks

In addition to performance degradation, successful cyber attacks on IIoT system may have permanent or temporary impact on human health and lives, the environment and assets. The main security risks include the lack of authentication and security in sensors and other cyber-physical devices; insecure gateways through which data is transmitted to the cloud; cloud security issues and insecure communication protocols. Successful attacks may cause a number of operational issues such as equipment damage, unforeseen operational concerns, endangered personal safety and regulatory issues (Stojanović & Boštjančič Rakas, 2020).

Several recent studies have provided classification and description of the cyber security threats and attacks against IIoT systems. Sajid, Abbas, and Saleem (2016) identify the most specific threats to supervisory control and data acquisition (SCADA) systems in IoT-cloud environments as follows: advanced persistent threats (APT), lack of data integrity protection, man-in-the-middle (MITM) attacks, identity theft, eavesdropping, replay attacks, as well as different forms of denial of service (DoS) attacks. Leander, Čaušević, and Hansson (2019) apply a threat model based on the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) method, which was originally introduced by Microsoft. They demonstrate the model on three typical scenarios related to the flow-control loop from the perspective of an industrial automation and control system (IACS). Tsiknas, Taketzis, Demertzis, and Skianis (2021) classify the IIoT threats in five generic categories: phishing attacks, ransomware, protocol, supply chain, and system attacks. Such a classification enables understanding of the security risks and the associated countermeasures in the IIoT environment.

Berger, Burger, and Roglinger (2020) propose three-layer taxonomy of attacks on the IIoT, where each layer is associated with appropriate dimensions and characteristics. Thus, the method of operation layer

DOI: 10.4018/978-1-7998-9220-5.ch127

identifies the entry points and methods used to perform an attack. This layer classifies attacks according to the technique, mechanism, executability and focus. The target layer classifies attacks according to the vulnerability and IIoT level. Finally, the impact layer characterizes effects of the successful attack in the sense of consequence and scope. Table 1 briefly summarizes previously described approaches.

Table 1. Taxonomies of IIoT cyber security risks, threats and attacks

Source	Category	Taxonomy	Main characteristics
Stojanović and Boštjančič Rakas (2020)	Cyber security risks	• Lack of authentication and security in cyber-physical devices • Insecure gateways • Cloud security issues • Insecure communication protocols	General classification that facilitates identification of IIoT operational issues in the case of successful attacks
Sajid et al. (2016)	Cyber security threats	• APT • Lack of data integrity protection • MITM attacks • Identity theft • Eavesdropping • Replay attacks • Different forms of DoS	Intended for IoT-based SCADA systems
Leander et al. (2019)	Cyber security threats	• STRIDE model	Intended for IACS
Tsiknas et al. (2021)	Cyber security threats	Five-category model: • Phishing attacks • Ransomware • Protocol • Supply chain • System attacks	Generic model suitable for definition of countermeasures
Berger et al. (2020)	Cyber security attacks	Three-layer model: • Method of operation layer • Target layer • Impact layer	Multi-layer taxonomy that facilitates identification of similarities and differences between attacks on the IIoT

Cyber Security Risk Assessment of Industrial Control Systems

According to the International Organization for Standardization (ISO) standard 31000:2018, risk assessment is considered as a core element of the risk management process, and includes risk identification, risk analysis, and risk evaluation (ISO, 2018). This assumes the following steps: (1) identification of the sources of risks and possible consequences, (2) analysis of the likelihood and impact of risks, and (3) evaluation of risks to assess the need for subsequent actions. In addition, the International Electrotechnical Commission (IEC) has published the IEC 31010:2019 (as a double logo standard with ISO), which provides guidance on the selection and application of techniques for assessing risk in a wide range of situations (IEC, 2019). Similarly, the International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) defines risk management and risk profile guidelines for telecommunication organizations in its recommendation X.1055 (ITU-T, 2008).

In the context of ICS security, the U.S. National Institute of Standards and Technology (NIST) defines risk assessment as ‘’the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact’’ (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015, p. 6-7). The Industrial Internet Consortium (IIC) addresses risk assessment in the view of overall security measures and highlights the