**INTRODUCTION**

**T**HE rapid evolution of the Internet of Medical Things (IOMT) leads the healthcare ecosystem to a new digital paradigm with valuable services, such as remote monitoring, faster diagnosis, preventive care, and health education. Based on the current situation of the COVID-19 pandemic and future pandemics, this evolution and, in general, the complete digitization of the healthcare cyber–physical infrastructures become more necessary than ever. However, despite the benefits, this new reality raises crucial cyber security and privacy risks due to the sensitive nature of the healthcare data and the vulnerabilities of the involved entities [1]. In particular, the healthcare sector is considered as the most sensitive critical infrastructure (CI) in terms of cyber security due to the vast amount of personal and administrative data aggregated in electronic health record applications. A characteristic healthcare-related cyber security incident was the WannaCry ransom ware, which paralyzed the United Kingdom’s National Health Service in May 2017.

Therefore, based on the aforementioned remarks, the presence of reliable intrusion detection and prevention mechanisms is vital. In this article, we focus our attention on the IEC 60 870-5-104 protocol, which is widely adopted by industrial healthcare systems [2]. IEC 60 870-5-104 is characterized by severe cyber security issues since it does not include adequate authentication and authorization mechanisms. Thus, it allows potential cyber attackers to perform various cyber attacks like Denial of Service (DOS) and unauthorized access. Such cyber attacks against IEC 60 870-5-104 can lead to devastating consequences in the healthcare ecosystem. Moreover, it is noteworthy that IEC 60 870-5-104 is used by other CIs, such as the energy domain. Consequently, possible IEC 60 870-5-104 cyber attacks can lead to cascading effects among different CIs. First, this article investigates the criticality of the IEC 60 870-5-104 cyber attacks by introducing a quantitative threat model, which combines an Attack Defence Tree (ADT) and the Common Vulnerability Scoring System (CVSS) v3.1. Next, we provide an intrusion detection and prevention system (IDPS), which takes advantage of the machine learning (ML) and software defined networking (SDN) technologies. ML is used to detect the IEC 60 870-5-104 cyber attacks, utilizing 1) Transmission Control Protocol (TCP)/Internet Protocol (IP) network flow statistics and 2) IEC 60 870-5-104 payload flow statistics. On the other side, the automated mitigation is transformed into a multi armed bandit (MAB) problem, which is solved through a reinforcement learning (RL) method called Thomson sampling (TS) and SDN. Hence, the contributions of this article are summarized as follows.

1) Providing a quantitative IEC 60 870-5-104 threat model: The proposed threat model determines the severity of the IEC 60 870-5-104 cyberattacks, combining ADT and CVSS v3.1.

2) Detecting IEC 60 870-5-104 cyber attacks :We provide an ML-based IDPS capable of detecting accurately the IEC 60 870-5-104 cyber attacks. Due to the lack of available IEC 60 870-5-104 datasets, a new IEC 60 870-5-104 intrusion detection dataset is implemented and provided in the context of this work.

3) Mitigating automatically IEC 60 870-5-104 cyber attacks: The automatic mitigation is transformed into a MAB problem, which is solved through TS and SDN. TS is responsible for the decision-making process, while SDN

undertakes to apply the mitigation strategy.

The rest of this article is organized as follows. Section II discusses relevant works. Section III presents the quantitative IEC 60 870-5-104 threat model. Section IV describes the architecture of the proposed IDPS, focusing mainly on the detection of the IEC 60 870-5-104 cyberattacks. Section V analyzes the mitigation process. Section VI is devoted to the evaluation results. Finally, Section VII concludes this article.