Chapter 7
Explainable Learning Machines for Securing the IoMT Networks

Izhar Ahmed Khan
Nanjing University of Aeronautics and Astronautics, China

Dechang Pi
Nanjing University of Aeronautics and Astronautics, China

ABSTRACT

The necessity to improve modern medical networks such as internet of medical things (IoMT) to monitor patients and their health condition has raised due to the effects of population ageing, increasing number of patients, deficiency of treatment facilities, and spread of widespread diseases. However, resisting cyber-attacks is a challenging concern for researchers. This chapter proposes an explainable learning machines-based security framework for detecting cyber-attacks against IoMT networks in real-time. The proposed model is based on the phenomenon of extreme learning machines to detect multiple kinds of cyber-space attacks carried against IoMT systems. The authors also explain the detection decisions to expand trust management in the employed machine learning algorithm and facilitate security professionals to comprehend the undiscovered data evidence and causal inference. Experiments show the effectiveness of the proposed approach signifying its utility as a workable security framework in contemporary networks of IoMT-based healthcare systems.

INTRODUCTION

The speedy development in communication technologies and sensing tools make the Internet of Things (IoT) networks capable to link numerous physical entities (Idrees, Alhussaini, and Salman, 2020). This progression led to the origination of various applications of IoT, such as intelligent transportation systems, smart homes, ambient assisted living, remote healthcare monitoring, etc. (Idrees and Al-Qurabat, 2021). The medical field has progressed so much by applying IoT tools and applications to design a bright term named the Internet of Medical Things (IoMT) (Khan et al., 2022). According to a report (Salman et al., 2020), the IoT sector will be instituting of more than 5.8 billion items by the end of year 2021, out of

DOI: 10.4018/978-1-6684-3533-5.ch007

which the 40% of the devices will be related to IoMT. More significantly, this report also mentioned that the IoMT industry is projected to become $136.8 billion industry worth, thus concluding that the reliance of medical field on IoMT-based devices can save up to $300 billion.

The progression of IoMT networks motivated by the enlarged amount of connected medical devices that are capable to produce, gather, evaluate, fuse, and transmit the sensed healthcare data to Cloud or any receiver. The IoMT networks are composed of data collected from several biosensor and healthcare devices and applications (Nehra et al., 2021). These IoMT devices are employed to gather clinical data, monitor the real-time health of the patient, and communicate it to health professionals through the remote data centers. Which is why the core objective of IoMT is to enhance the quality of treatment and connected medical systems. Because such medical systems and healthcare applications necessitate speedy response and decision system to support the emergency cases, through the usage of high bandwidth IoMT network for transferring the sensed data. These requirements signify great challenges in the implementation process of an IoMT network. However, a key problem is to defend these networks against evolving cyber-attacks. The healthcare data from these networks needs to be kept safe at various levels (creation, collection, communication, and storing levels) to protect the privacy and security of both data and patients. According to the writers of (CyberMDX, 2020), nearly 50% of the IoMT-centric healthcare devices and tools are exposed to cyber-attacks and exploits. Since the IoMT networks involves identities of patients, the healthcare data costs on average 50 times more as related to other categories of data, subsequently making it enormously treasured on the dark-web and black-market (Maddox, 2019).

Despite the fact that linked IoMT devices bring numerous benefits, they also increase the issues like security against cyber-attacks since these systems process sensitive and life-critical data (CyberMDX, 2020). The attacks against IoMT systems could have substantial physical and lethal harm to patients. E.g., an attack on connected insulin healthcare pump or pacemaker device could actually lead to patients' death if the levels of insulin or pacemaker device are manipulated. Several researchers have pointed out that attacks like eavesdropping, DoS, identity theft, false data injection etc., can actually disturb the security parameters thus threatening the availability of these life-critical devices in IoMT networks (Yaqoob, Abbas, & Atiquzzaman, 2019), or in worst cases it can push the IoMT ecosystem into a complete chaos (CyberMDX, 2020).

Currently, one of the foremost challenges confronted by the effective engagement of IoMT systems in healthcare networks is security against cyber-attacks. The basic security mechanisms required by these networks are described by the authors of (Academy, 2022) as CIANA (confidentiality, integrity, authentication, non-repudiation, and availability). Although the existing security designs are capable to achieve these requirements, but they are unable to provide a comprehensive security model due to the boundaries of connected healthcare devices, for example, these devices have limited storage availability and restricted power requirements. In addition, the tools for IoMT networks and connected healthcare devices are not precisely premeditated to have ingrained security designs.

Recent studies in IoMT networks security domain have mostly hired security models based on trust, encryption, and authentication models to keep the wearables and connected healthcare devices against cyber-attacks. Likewise, the present security models are computationally costly and also hard to deploy on connected healthcare devices because of their resource limited nature. Further, the present researches mostly address the issues related to the IoMT networks' security. For instance, the authors of (Yaacoub et al., 2020) developed a classification approach using cryptographic technique in IoMT system and wireless body area networks. The writers classify their technique in numerous kinds i.e., authorization, intrusion detection system (IDS), availability, and awareness. Similarly, the writers of (Sisinni et al.,