Applied Soft Computing 140 (2023) 110227

Contents lists available at ScienceDirect

Applied Soft Computing

journal homepage: www.elsevier.com/locate/asoc

Review article

Survey of Machine Learning based intrusion detection methods for Internet of Medical Things

Ayoub Si-Ahmed [a,d,*], Mohammed Ali Al-Garadi [b], Narhimene Boustia [c]

[a] Blida 1 University, LRDSI Laboratory, Blida, B.P 270, Algeria
[b] Emory University, School of Medicine, Department of Biomedical Informatics, Atlanta, GA 30322, USA
[c] Blida 1 University, SIIR/LRDSI (Blida1) & RCR/RIIMA (USTHB) Laboratory, Blida, B.P 270, Algeria
[d] PROXYLAN SPA/Subsidiary of CERIST, Algeria, 16028, Algeria

ARTICLE INFO

Article history:
Received 24 September 2022
Received in revised form 9 February 2023
Accepted 13 March 2023
Available online 22 March 2023

Keywords:
Internet of Medical Things
Intrusion Detection System
Machine Learning
Privacy
Security

ABSTRACT

The Internet of Medical Things (IoMT) has revolutionized the healthcare industry by enabling physiological data collection using sensors, which are transmitted to remote servers for continuous analysis by physicians and healthcare professionals. This technology offers numerous benefits, including early disease detection and automatic medication for patients with chronic illnesses. However, IoMT technology also presents significant security risks, such as violating patient privacy or exposing sensitive data to interception attacks due to wireless communication, which could be fatal for the patient. Additionally, traditional security measures, such as cryptography, are challenging to implement in medical equipment due to the heterogeneous communication and their limited computation, storage, and energy capacity. These protection methods are also ineffective against new and zero-day attacks. It is essential to adopt robust security measures to ensure data integrity, confidentiality, and availability during data collection, transmission, storage, and processing. In this context, using Intrusion Detection Systems (IDS) based on Machine Learning (ML) can bring a complementary security solution adapted to the unique characteristics of IoMT systems. Therefore, this paper investigates how IDS based on ML can address security and privacy issues in IoMT systems. First, the generic three-layer architecture of IoMT is provided, and the security requirements of IoMT systems are outlined. Then, the various threats that can affect IoMT security are identified, and the advantages, disadvantages, methods, and datasets used in each solution based on ML at the three layers that make up IoMT are presented. Finally, the paper discusses the challenges and limitations of applying IDS based on ML at each layer of IoMT, which can serve as a future research direction.

Contents

* Corresponding author at: Blida 1 University, LRDSI Laboratory, Blida, B.P 270, Algeria.
E-mail addresses: si_ahmed.ayoub@etu.univ-blida.dz, ayoub.siahmed@proxylan.dz (A. Si-Ahmed), m.a.al-garadi@emory.edu (M.A. Al-Garadi), nboustia@univ-blida.dz (N. Boustia).

https://doi.org/10.1016/j.asoc.2023.110227
1568-4946/