Chapter 2
Machine Learning-Based Cyber Intrusion Detection System for Internet of Medical Things Attacks in Healthcare Environments

Bhawnesh Kumar
Graphic Era University (Deemed), India

Ashwani Kumar
Shri Ram Group of Colleges, India

Harendra Singh Negi
Graphic Era University (Deemed), India

Javed Alam
Quantlase Lab, Abu Dhabi, UAE

ABSTRACT

In this chapter, the authors calculate the accuracy value of machine learning models for combined, network, bio-medical data. The result shows that random forest has the highest accuracy value 94.17% for combined and 93.19% bio-medical data. For network data, decision tree classifier provides the highest accuracy value which is 94.07% whereas decision tree regression gives the highest accuracy value: 94.62% for combined, 92.11% for bio-medical, and 94.09% for network data.

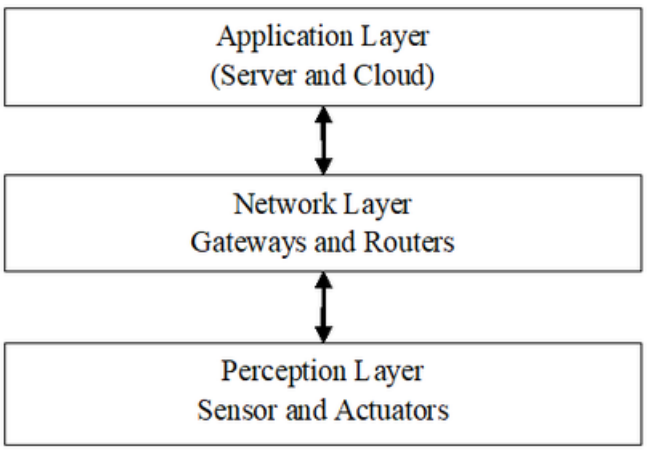
DOI: 10.4018/978-1-6684-6646-9.ch002

INTRODUCTION AND BACKGROUNDS

Sensors, the cloud, and many more advanced technologies give a new aspect to the healthcare system. Advancements in the area of wireless data collection through sensors, data storage, internet, and communication link patients who are far from healthcare professionals. Remote monitoring systems enabled the communication link between doctors and patients using various types of gadgets such as smart watches, smartphones, laptops, and many more devices. These devices are known as the internet of things (IoT). If these devices are integrated for medical purposes, then it becomes the internet of medical things (IoMT) (Razdan & Sharma, 2021). IoMT reduces the visit of the patient and medical professionals can collect the data of patients through the internet. Patient details are represented as a medical record in a digital format than paper which also knows as electronic health records (Dimitrov, 2016) (EHR). Wireless communication is used between the patient and server repository to locate the EHR details. EHR data should be secured from intruders and attacks while transmitted over communication channels through the internet. As IoMT architecture (Toghuj & Turab, 2022) shown in Fig 1 where three layers named application, network, and perception, represent the flow of data from sensors/actuators to cloud/server. These layers performed the following operations on medical data: processed, analyzed, and stored.

To do the computational statistical analysis, machine learning (ML) helped to predict intrusion detection for cyber security (Davenport & Kalakota, 2019a). The most promising technique is to manage issues of security in healthcare systems for attacks (Abouelmehdi et al., 2018). L comprises the rules and methods that can

Figure 1. IoMT architecture



A Surveillance and Spatiotemporal Visualization Model for Infectious Diseases Using Social Network

Younsi Fatima-Zohra, Hamdadou Djamilaand Boussaid Omar (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1027-1046).*

www.irma-international.org/chapter/a-surveillance-and-spatiotemporal-visualization-model-for-infectious-diseases-using-social-network/213842