Chapter 6
A Machine Learning-Based Framework for Intrusion Detection Systems in Healthcare Systems

Janmejay Pant
Graphic Era Hill University, India

Rakesh Kumar Sharma
Pal College of Technology and Management, Haldwani, India

Himanshu Pant
Graphic Era Hill University, India

Devendra Singh
Graphic Era Hill University, India

Durgesh Pant
Uttarakhand Open University, Haldwani, India

ABSTRACT

A reliable intrusion detection system is an important key component of healthcare-based systems. Intrusion detection systems are crucial in e-healthcare because patient medical records must be maintained accurately, safely, and secretly. Errors in diagnosis and therapy might result from changing the actual patient data. It is not possible to handle complex data using traditional techniques. Current network requirements cannot be met by diversified intrusion techniques. In addition to the rise in data, attacks are also escalating rapidly. The area of network security is trending when it comes to machine learning techniques. This study aims to develop a novel machine learning framework for detecting attacks.

DOI: 10.4018/978-1-6684-6646-9.ch006

Copyright © 2023, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

In recent years, there has been a growing need for applications and domains to use the Internet, resulting in more data being moved and more workload on the network. Even though there are several security mechanisms in place, such as the firewall system, an excellent mitigation and protection system is in place. Firewall systems prevent illegal access to systems after transferring information but cannot track surveillance. If a threat is attempted to penetrate it, it will not be able to detect it. For the network to be controlled, intrusion detection systems (Pande, S. et al., 2021) must be deployed. The intrusion was described as posing a threat to resource availability, confidentiality, and integrity that was either brought on by authorized system operators misusing their authority or by unauthorized system operators taking advantage of particular permissions gaps (Kumaar, M. A. et al., 2001). An intrusion detection system has been the subject of many studies in recent years. The Internet has become one of the best tools for gathering information about the modern world. One of the critical elements of education and business and health purposes can be regarded as the Internet. As a result, Internet data transfers need to be safe. One of the main issues in today's world is internet security. It is crucial to develop a system to safeguard the consumers who utilize the data and the data itself because the Internet is constantly under assault. The intrusion detection system (IDS) was created to meet that need. Network administrators modify intrusion detection systems to thwart malicious attempts. To effectively manage security, intrusion detection systems become crucial. The intrusion detection system discovers and reports any infiltration or network abuse attempts. IDS can perform thorough security analysis, detect, and thwart harmful attacks on the network, and maintain normal functioning throughout any hostile outbreak. Due to the need to maintain the accuracy, confidentiality, and high level of security of patient medical records, intrusion systems are essential in e-healthcare. Any modification to the original patient data has the potential to result in inaccuracies in the diagnosis and treatment process. For intrusion detection, the bulk of artificial intelligence-based systems currently in use were trained on outdated repositories, which may result in more false positives and need for a full algorithm retraining to handle new threats. Since intrusion detection systems are frequently out of date as a result of these behaviours, it is particularly difficult to protect patient records in medical systems. Attacks against organizations mostly aim to take private user information. These signs draw attention to a background that is essential for modern cyberattack detection and prevention.

With the increasing demand for healthcare services, hospitals are adopting e-healthcare systems to promptly meet patient needs. These systems allow for the efficient management of Electronic Health Records (EHR) and Patient Records,

9 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/a-machine-learning-based-framework-for-intrusion-detection-systems-in-healthcare-systems/328126

Related Content

Real-Name Registration Regulation in China: An Examination of Chinese Netizens' Discussions About Censorship, Privacy, and Political Freedom
Kenneth C. C. Yangand Yowei Kang (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1098-1124).*
www.irma-international.org/chapter/real-name-registration-regulation-in-china/213846

Should We Publish That?: Managing Conflicting Stakeholder Expectations in the Publishing Industry
Loren Falkenbergand Oleksiy Osiyevskyy (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1657-1684).*
www.irma-international.org/chapter/should-we-publish-that/213876

Secure Data Sharing Using Revocable-Storage Identity-Based Encryption
Muthumanikandan Vanamoorthy (2023). *Cyber Trafficking, Threat Behavior, and Malicious Activity Monitoring for Healthcare Organizations (pp. 72-84).*
www.irma-international.org/chapter/secure-data-sharing-using-revocable-storage-identity-based-encryption/328125

Who Watches?
(2022). *Modern Day Surveillance Ecosystem and Impacts on Privacy (pp. 41-63).*
www.irma-international.org/chapter/who-watches/287143

The World is Polluted With Leaked Cyber Data
Ivan D. Burkeand Renier P. van Heerden (2019). *National Security: Breakthroughs in Research and Practice (pp. 497-513).*
www.irma-international.org/chapter/the-world-is-polluted-with-leaked-cyber-data/220897