IEEE JOURNAL OF

BIOMEDICAL AND HEALTH INFORMATICS

J-BHI Special Issue on “Deep Learning in Intrusion Detection of Cyberattacks for E-Health Applications”

The e-health industry continues to grow and there are no signs that it is slowing down. As such, the industry’s projected revenue of $3.5 billion by 2022 remains right on track. Thus, indicating that every major healthcare network will eventually offer some type of telehealth service to its patients. While e-health offers numerous benefits, it is vulnerable to cyber threats like any other information technology service.

Deep learning is one of the exciting techniques which recently been vastly employed by the IDS or intrusion detection systems to increase their performance in securing the computer networks and hosts. An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues an alert when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management system. Security information and management system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

The report looked at 1 million organizations, including more than 30,000 in the healthcare industry, from September 2019 to April 2020 to assess cybersecurity risk. In a bright spot, despite pivoting in huge numbers to digital healthcare delivery and facing immense challenges. The 30% increase in overall cybersecurity findings includes a range of different attack methods, including a 65% increase in patching cadence findings, one of the primary security policies to protect data and a 56% increase in endpoint security findings. Hackers exploit vulnerabilities in endpoint security to steal data. Implementing cybersecurity tools is the first step in securing patient data and the second step is reviewing security programs. E-health providers need to review their third-party provider contracts and discuss the strategies for responding to any intelligence threat that may arise. In addition, ask how to identify malicious emails and suspicious links so as to avoid cybersecurity threats. Another vital aspect of securing telehealth data includes remaining abreast of any current cybersecurity threats. Finding out up-to-date information related to e-health and cybersecurity.

This special issue will focus on cutting-edge research from both academia and industry and aims to solicit original research papers with a particular emphasis on the challenges and future trends in cyberattacks for e-health applications with deep learning.

.

Topics of interest include, but are not limited to, the following:

- Deep learning in an intrusion detection system for real-time health care cyberattack detection
- Deep learning-based intrusion detection methods for the internet of medical things for e-health applications
- Deep learning in cyberattack detection systems improves threat reaction in e-health
- Deep learning in intrusion detection systems for fog and cloud computing e-health applications
- Deep learning in risk assessment-based security evaluation model for e-health applications
- Deep learning in intrusion detection of security challenges in body area networks for e-health applications
- Deep learning in an intelligent behavioural trust-based intrusion detection system for the smart healthcare system
- Deep learning cyberattacks detection system to improve threat reaction in e-Health
- Deep learning in intrusion detection for hybrid framework healthcare systems
- Deep learning in cybersecurity of multi-cloud healthcare systems
- Deep learning in data augmentation for attack detection on IoT e-health systems
- Deep learning in intrusion detection for cyber-attack detection and mitigation

Guest Editors

Gitanjali Jayaraman, VIT University, gitanjalij@ieee.org
Cristiano André da Costa, Universidade do Vale do Rio dos Sinos, cac@unisinos.br
S. Manimurugan, University of Tabuk, mmurugan@ut.edu.sa
Emmanuel Gbenga Dada, University of Maiduguri, gbengadada@unimaid.edu.ng
George Drosatos, Athena Research Centre, gdrosato@athenarc.gr

Key Dates

Deadline for Submission:	25 Sep, 2023
First Reviews Due:	01 Nov, 2023
Revised Manuscript Due:	15 Dec, 2023
Final Decision:	15 Jan, 2024