Healthcare Analytics xxx (xxxx) xxx

Contents lists available at ScienceDirect

Healthcare Analytics

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

Autonomic and adaptive cyber-defense algorithms for healthcare applications

The field of cybersecurity is constantly changing, with cyberattacks taking many forms, from sophisticated SQL injection methods to the use of botnets. As a result, cybersecurity experts must continuously adapt and innovate to keep one step ahead of these dangers. Conventional defensive methods frequently fail to achieve the necessary balance between security and performance. Recent large-scale breaches in the healthcare industry starkly remind us of the potential repercussions of such failures. A new generation of cyber-defense algorithms that can dynamically identify, prevent, and mitigate assaults in real time is needed in light of these difficulties. Given the complexity of today's cyber threats, these algorithms must function holistically and cooperatively. We introduce autonomic and adaptive cyber-defense systems, a potentially exciting area of cybersecurity research. These systems are made to adapt to new threats and changing attack vectors, imitating biological organisms' self-regulating and self-healing properties.

The healthcare sector is one where the value of solid cybersecurity is most apparent. Due to the sensitive patient data they are entrusted with, hospitals, physician offices, and other healthcare institutions are often the targets of cyberattacks. To ensure patient privacy and organizational integrity, executives and operational leaders in the healthcare industry must prioritize maintaining the confidentiality, availability, and integrity of electronically protected health information (ePHI). Healthcare-specific cyber defense systems (CDS) are built on the foundation of autonomous and adaptive cyber-protection algorithms. However, there are particular difficulties in successfully putting these algorithms into practice. Robust and adaptable cybersecurity methods are necessary due to the ever-changing regulatory landscape and the dynamic nature of healthcare facilities. Adherence to rules like HIPAA introduces an extra degree of complexity, calling for customized cybersecurity strategies.

In today's healthcare systems, protecting patient data is critical when the stakes are high, and a breach might have dire repercussions. Hospitals face technological difficulties, from safeguarding network infrastructure to avoiding sophisticated cyberattacks. To reduce the danger of insider threats and human mistakes, they must address human issues, such as staff awareness and training. In this situation, cyber-defense systems must be autonomous and adaptable to function well in dynamic, constantly evolving operational contexts. In this sense, algorithms are essential because they offer the computational intelligence required to recognize dangers, detect abnormalities, and take immediate action. The correct and dependable use of these algorithms, which necessitates careful consideration of contextual elements and operational limits, will ultimately determine their efficacy.

In conclusion, the necessity for sophisticated cyber-defense measures is highlighted by the changing threat landscape and the vital significance of protecting sensitive data in the healthcare sector. To counter new cyber dangers, autonomous and adaptive systems present a possible approach by utilizing the concepts of self-regulation and adaptation. A highly confidential and secure environment in a healthcare system requires the development of robust security techniques. However, to fully utilize these technologies, one must overcome technological obstacles and navigate legislative hurdles, highlighting the necessity of a multifaceted approach to cybersecurity in the healthcare industry.

In this special Issue, we have successfully published 12 articles. In the first article, the authors proposed two non-competitive and competitive methods to establish a connection between general and community hospitals. The authors claim that the proposed model improves the system's utility. The conclusion demonstrates that system utility may be increased by lowering the unit personnel's service cost. In community hospitals, introducing competition can reduce the referral rate and encourage initial consultations.

The authors proposed a hybrid logistic DNA-based encryption system in the second article to secure patient monitoring using the Internet of Things. This research uses discrete Fourier tests, run length tests, and frequency monobit tests to secure data transmission. The proposed technique has outperformed the previous encryption techniques and provides high-level security for medical data transmission.

In the third article, the authors have developed an adaptive cyber defense strategy for making prototyping and distributing cutting-edge software and services more accessible for healthcare systems. This research discusses future challenges and concerns regarding IoT-enabled healthcare systems. These designs provide fresh approaches to managing smart devices and applications or tackle persistent problems in a particular field, such as security, privacy, or compatibility. Conventional IoT networks must be integrated with peripheral processing units To achieve the highest efficiency level.

The fourth article presents the deployment of two retrieval-based and generative-based chatbots using Deep Learning and Machine Learning to improve mental health. The proposed model achieves an accuracy of 94.45%. The primary significance of the research claimed by authors lies in using generative and retrieval-based chatbots together, where one can generate new text and the other restricts only to best outputs. The authors point out that the lack of a robust control group raises the possibility of placebo effects and that more research with more sophisticated designs may be necessary to find "hidden" cases of depression that the chatbot was unable to identify accurately.

The fifth article proposes a skin and oral cancer detection model using a convolutional neural network. The model uses medical images and applies resizing and filtering on the input images to improve their quality and reduce noise. The authors analyzed various CNN models, including AlexNet, VGGNet, Inception, ResNet, DenseNet, and Graph

https://doi.org/10.1016/j.health.2024.100345

Available online 31 May 2024

Neural Network. The final results show that the DenseNet model performs better than other models. These findings may significantly impact the advancement of technology for detecting and diagnosing skin cancer.

In the sixth article, the authors suggested a machine-learning model for detecting disease-miRNA connections. The final findings indicate that the proposed model has better accuracy and ROC curve than previous techniques. The proposed method uses network internal topology data to establish the disease-miRNA connection. It is possible to demonstrate that the proposed model can accurately anticipate the relationship between diseases and miRNAs, which will be helpful for further research on the genesis of diseases.

The authors comprehensively reviewed various neural network models for medical image processing in the seventh article. The development, limitations, merits, and future perspectives of different neural network modes for medical image processing have been analyzed. Furthermore, various publicly available data sources have been summarized in the article. The authors concluded that personalized medicine is made possible by deep learning algorithms that assess medical pictures and other clinical data, including genetics or electronic health records. By incorporating patient-specific data, DNNs can help with treatment planning, prognostication, and selecting the best medicines based on image-derived features and patterns.

The eighth article employed an eXtreme Gradient Boosting model to predict the Brain tumor. In the proposed model, the authors have used the Contrast-Limited Adaptive Histogram Equalization method to enhance image contrast. Furthermore, the particle swarm optimization technique has been employed for feature selection. The model is trained and tested on an MRI image dataset. The proposed model performs better for brain tumor detection with an accuracy of 97%. Given the necessity of a timely and accurate diagnosis of brain tumors without any delay, our subsequent research endeavors will concentrate on the creation of powerful hybrid alternatives for the categorization of brain tumors. These tactics will be more straightforward and need less time to implement. Furthermore, MRIs and CT scans can be used with the suggested techniques to help diagnose a range of malignancies.

The ninth article (Shrivastava et al., 2023) proposes a machine learning-based method for predicting systolic and diastolic blood pressure. Clinical characteristics like gender, blood sugar and cholesterol levels, smoking status, age, alcohol usage, weight, and previous heart disease history are considered together to predict blood pressure. Different training, validation, and testing ratios were analyzed using machine learning methods to improve the model accuracy. The random forest model has achieved the best accuracy.

In the tenth article, the authors have suggested a unique digital forensic architecture to improve the credibility of digital evidence. The architecture uses Software Defined Networking and Blockchain technologies to improve the infrastructure of digital forensics. A secure-Ring-Verification Authentication technique ensures security from suspicious accounts, and Harmony Search Optimization is utilized for secret critical production. According to a thorough analysis, the recommended forensic architecture has a positive response, evidence insertion, and verification times.

In the eleventh article, a combination of artificial intelligence and computational intelligence is used to detect breast cancer. The authors use tagged Internet of Things devices in this article to gather data and train a GRU-RNN classifier. The algorithm's accuracy is tested using Wisconsin Diagnostic Breast Cancer (WDBC) data. The findings demonstrate that the suggested Internet of Medical Things (IoMT) retains 95% of the original GRU-RNN while outperforming the existing approaches in recall, accuracy, and precision.

In the twelfth article, the authors use an enhanced augmentation strategy to modify the Convolutional Neural Network (CNN) model as a pre-trained Visual Geometry Group19 (VGG19) to identify lung cancer biopsy pictures. Up to 97.73% accuracy is achieved using the refined VGG19 model and enhanced augmentation method. The suggested technique outperforms the current approaches in the experiment findings. This research aims to quickly and accurately construct models for practical, real-time cancer diagnosis.

Mohammad Shabaz*
Model Institute of Engineering and Technology, Jammu, J&K, India

Ahmed Farouk
Department of Computer Science, Faculty of Computers and Artificial Intelligence, South Valley University, Hurghada, Egypt

Salman Ahmad
University of the West of Scotland, Paisley, Scotland

Shah Nazir
Department of Computer Science, University of Swabi, Swabi, Pakistan

Abolfazl Mehbodniya
Department of Electronics and Communication Engineering, Kuwait College of Science and Technology (KCST), 7th Ring Road, Doha, Kuwait

* Corresponding author.
E-mail address: bhatsab4@gmail.com (M. Shabaz).