IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 9, May 2023

Analysing Health Care Data and Preserving Security using Decoy File and Fog Computing

Prof. Y. R. Chikane[1], Mr. Mahesh Patil[2], Ms. Shrushti Satpute[3], Mr. Suyog Bangar[4], Ms. Snehal Salve[5]

Professor, Department of Information Technology[1]
Student, Department of Information Technology[2,3,4,5]
Amrutvahini College of Engineering, Sangamner, India

Abstract: *Currently, humans face various diseases due to the current environmental condition and their living habits. Early identification and prediction of diseases are crucial to prevent their severity. However, doctors may find it challenging to accurately identify illnesses manually. This project aims to use predictive analysis to identify and predict patients with a higher risk of developing chronic diseases. By utilizing data analysis techniques, including machine learning and data mining, healthcare professionals can get early warnings of potential illnesses and take timely preventive measures, ultimately improving patients' overall health outcomes. Automating the diagnosis process can also help reduce healthcare costs, making healthcare more affordable and accessible. The use of data mining is crucial in predicting diseases, which is a difficult task. The proposed system employs machine learning algorithms such as the convolutional neural network (CNN) to provide a comprehensive disease prognosis based on a patient's symptoms. This system offers an automated feature extraction approach, enabling healthcare professionals to make more informed decisions. Therefore, it can contribute significantly to enhancing disease prediction and providing appropriate treatment. Storage and evaluation of big data is flexible and scalable on the cloud but at the same time there are issues in security such as data theft attacks. The problem of security can be resolved by using the technique called Fog computing. The data can be stored the security by using implementing decoy technique in fog. Decoy file are Honeypots and other false information which is used to secure the original data from an unauthorized user who is trying to access the private data. We are using decoy file to contain fake data which confusing the attacker.*

Keywords: Text detection, Morphological operations, painting, Connected component labelling

REFERENCES

[1]. S. Wang et al, “KRProtector: Detection and Files Protection for IoT Devices on Android Without ROOT Against Ransomware Based on Decoys”, in IEEE Internet of Things Journal, vol. 9, no. 19, pp. 18251-18266, 1 Oct.1, 2022, doi: 10.1109/JIOT.2022.3156571.

[2]. Wang, Senmiao, Sujuan Qin, Nengqiang He, Tengfei Tu, Junjie Hou, Hua Zhang, and Yijie Shi. 2021. “KRRecover: An Autoecovery Tool for Hijacked Devices and Encrypted Files by Ransomwares on Android” Symmetry 13, no. 5: 861. https://doi.org/10.3390/sym13050861

[3]. H. Chen, Y. Gu, P. Wang, J. Dong and Y. Ren, “Research on Privacy Data Protection in Mobile Applications”, 2021 33rd Chinese Control and Decision Conference (CCDC),2021, pp. 4912-4915, doi: 10.1109/CCDC52312.2021.9602169.

[4]. P. Chittora et al., “Prediction of Chronic Kidney Disease - A Machine Learning Perspective”, in IEEE Access, vol. 9, pp. 17312-17334, 2021, doi: 10.1109/ACCESS.2021.3053763.

[5]. D. Chicco, C. A. Lovejoy and L. Oneto, “A Machine Learning Analysis of Health Records of Patients with Chronic Kidney Disease at Risk of Cardiovascular Disease”, in IEEE Access, vol. 9, pp. 165132-165144, 2021,doi:10.1109/ACCESS.2021.3133700

DOI: 10.48175/IJARSCT-10364