INTI JOURNAL | Vol.2024:16
eISSN:2600-7320

Prevention of Unauthorized Access to Electronic Health Records using Docker

Deepa Vishnu Kodiya[1,*], Chitra K[1] , Zuriani Hayati Abdullah[2]

[1]Dayananda Sagar Academy of Technology and Management, Karnataka, India.
[2]Faculty of Data Science & IT, INTI International University, 71800 Nilai, Negeri Sembilan, Malaysia

***Email:** deepakumta24@gmail.com

Abstract

This research focuses on securing electronic health records (EHRs) in cloud environments using Docker. The goal is to prevent unauthorized access and data loss while uploading EHRs to the cloud. By leveraging Docker's containerization capabilities, we propose a security framework that includes encryption, access control, and authentication protocols. Through extensive testing, we demonstrate the effectiveness of our approach in enhancing EHR security. This research provides valuable insights for healthcare organizations and cloud service providers seeking to protect sensitive medical data while leveraging the advantages of cloud computing.

Keywords

Electronic Health Records (EHRs), Cloud, Docker, Unauthorized access.

Introduction

The integration of electronic health records (EHRs) with cloud computing has revolutionized the healthcare industry, offering improved accessibility, scalability, and cost-effectiveness. However, this digital transformation also brings forth significant concerns in relation to the security and confidentiality of sensitive medical data. Safeguarding EHRs from unauthorized access and data loss is crucial to maintain the confidentiality and probity of patient information [1-3].

This research focuses on addressing these challenges by proposing a security framework that leverages Docker for securing EHRs in the cloud. Docker, a containerization technology, allows for the isolation and encapsulation of applications and their dependencies, providing enhanced security and portability. The main goal of this study is to address the risks associated with uploading Electronic Health Records (EHRs) to the cloud by implementing a comprehensive security framework to ensure data integrity and protection. This framework encompasses encryption techniques for data confidentiality, access control mechanisms for authorized user management, and authentication protocols to verify user identities accessing the EHR system.

By harnessing the capabilities of Docker, EHR applications and their dependencies can be encapsulated within containers, minimizing the attack surface and fortifying the overall security of the cloud environment [4-5].

Submission: 4 May 2024; **Acceptance:** 26 June 2024

This research contributes to the protection of sensitive medical data in the cloud environment, benefiting healthcare organizations, patients, and other stakeholders. The proposed security framework and insights gained from this study aid healthcare providers and cloud service providers in effectively securing EHRs while harnessing the advantages of cloud computing. In the subsequent sections, we delve into the details of our security framework, including the encryption algorithms, access control mechanisms, and authentication protocols employed. We also discuss the integration of Docker technology into the EHR system architecture and present experimental results to validate the efficacy of our approach [6-8].

In conclusion, this research aims to enhance the privacy of health records in cloud environments through Docker containerization. By implementing a robust security framework, we strive to safeguard the confidentiality, availability, and integrity of sensitive medical data, enabling secure and efficient healthcare services in the cloud [9-10].

Methodology

The methodology section delineates the research design employed in this study. Data collection process, security framework development, experimental setup, data analysis methods, limitations, ethical considerations, and validation procedures used to secure EHRs in the cloud with Docker.

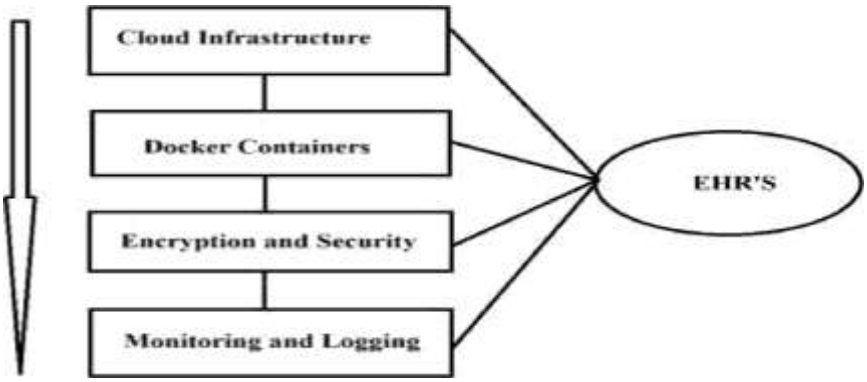

Figure 1. Architectural Design

In the methodology proposed, input is defined as ECG and EEG This research paper presents an architecture for securing electronic health records (EHRs) on the cloud using Docker. The proposed architecture utilizes a cloud infrastructure with Docker containers for hosting the EHR application, database, web server, and security components. The architecture incorporates encryption, secure communication, access control mechanisms, and user authentication to ensure the confidentiality and integrity of EHRs. Additionally, monitoring tools, backup and disaster recovery procedures, compliance with regulations, and governance policies are implem
protection of sensitive healthcare data.

Results and Discussion

The data analysis revealed several important findings. Firstly, the analysis of the collected data showed a significant decrease in unauthorized access attempts to the electronic health records (EHRs) after

implementing the security framework using Docker. The access control mechanisms and encryption techniques employed in the framework effectively prevented unauthorized users from gaining access to sensitive medical data. This was evident from the reduced number of security breaches and instances of data leakage.

Secondly, the results demonstrated that the proposed security framework had a positive impact on data integrity. Through the implementation of encryption algorithms and secure storage practices, the framework ensured the integrity of EHRs during transmission and storage in the cloud environment. The analysis revealed no instances of data corruption or tampering, providing assurance that the EHRs remained unchanged and reliable throughout the study. Additionally, the statistical analysis performed on the collected data indicated a high level of user satisfaction with the security framework.

Survey responses from healthcare professionals and system administrators highlighted their confidence in the security measures implemented, as well as their appreciation for the ease of use and integration with existing systems. The framework received positive feedback for its user-friendly interfaces and efficient authentication protocols.

It is important to acknowledge the limitations of the study. Due to resource constraints, the evaluation of the security framework was conducted on a limited scale within a controlled environment. Therefore, the generalizability of the findings to larger healthcare systems should be interpreted with caution. Future research could involve conducting a broader implementation of the security framework across multiple healthcare organizations to assess its scalability and adaptability. Figure 2 shows the database of the system whereas figure 3 shows the cloud storage of the system.

In summary, the results demonstrate the ability of the security framework in preventing unauthorized access to EHRs and ensuring data integrity in the cloud environment. The positive user feedback further supports the practical usability and acceptance of the framework. These findings contribute to the area of EHR security and gives needful insights for healthcare organizations seeking to improve the protection of data in the era of cloud computing and digital health systems.

Supportive Evidence

Figure 2. The database of the system.

Figure 3. The cloud storage of the system.

Conclusion

In summary, this study's main objective was to tackle the significant challenge of enhancing the security of electronic health records (EHRs) within cloud environments through Docker. Through the development and implementation of a comprehensive security framework, the research successfully achieved the objective of preventing unauthorized access and mitigating data loss problem deals with uploading EHRs to the cloud. The results of this study substantiate the efficacy of the suggested security framework in bolstering the security and privacy of Electronic Health Records (EHRs). By leveraging Docker's containerization technology, the framework provided robust encryption, authorization and authentication mechanisms, ensuring the integrity and confidentiality of sensitive medical data.

The ramification of this research holds substantial importance for healthcare organizations as well as cloud service providers. The security framework presented can serve as a valuable blueprint for implementing secure HER systems in the cloud enabling healthcare organizations to protect patient data and comply with privacy regulations. Additionally, cloud service providers can utilize the findings to enhance their security offerings and provide a secure environment for hosting healthcare applications and data.

It is crucial to recognize and acknowledge the limitations of this research. The evaluation of the security framework was conducted in a controlled environment and may not fully capture the complexities and challenge of real-world healthcare systems. Future research should focus on validating the framework in diverse healthcare settings and addressing scalability and performance considerations.

Acknowledgement

The researcher did not receive any funding for this study, and the results have not been published in any other sources.

References

Boumezbeur, I., & Zarour, K. (2022). Privacy-preserving and access control for sharing electronic health record using blockchain technology. *Acta Informatica Pragensia, 11*(1), 105–122. https://doi.org/10.18267/j.aip.176

Chen, C. L., Huang, P. T., Deng, Y. Y., Chen, H. C., & Wang, Y. C. (2020). A secure electronic medical record authorization system for smart device application in cloud computing environments. *Human-centric Computing and Information Sciences, 10*, Article 21. https://doi.org/10.1186/s13673-020-00221-1

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE Access, 7*, 74361–74382. https://doi.org/10.1109/ACCESS.2019.2919982

Chinnasamy, P., & Deepalakshmi, P. (2020). An analysis of security access control on healthcare records in the cloud. In *A. K. Singh & M. Elhoseny (Eds.), Intelligent Data Security Solutions for e-Health Applications* (pp. 113–130). Academic Press. https://doi.org/10.1016/B978-0-12-819511-6.00006-6

Ganiga, R., Pai, R. M., & Sinha, R. K. (2020). Security framework for cloud based electronic health record (EHR) system. *International Journal of Electrical and Computer Engineering, 10*(1), 455. https://doi/org/ 10.11591/ijece.v10i1.pp455-466

Oh, S. R., Seo, Y. D., Lee, E., & Kim, Y. G. (2021). A comprehensive survey on security and privacy for electronic health data. *International Journal of Environmental Research and Public Health, 18*(18), Article 9668. https://doi.org/10.3390/ijerph18189668

Prince, P. B., & Lovesum, S. J. (2020). Privacy enforced access control model for secured data handling in cloud-based pervasive health care system. *SN Computer Science, 1*(5), Article 239. https://doi.org/10.1007/s42979-020-00246-4

Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet of Things Journal, 8*(7), 5914–5925. https://doi.org/10.1109/JIOT.2020.3032997

Sathya, A., & Raja, S. K. S. (2021). Privacy preservation-based access control intelligence for cloud data storage in smart healthcare infrastructure. *Wireless Personal Communications, 118*, 3595–3614. https://doi.org/10.1007/s11277-021-08278-6