ABSTRACT

The increasing dependence on modern digital healthcare systems and the widespread adoption of healthcare digital records (HDR) and telemedicine, emphasize the critical importance of security of medical image transmission. Protecting patients' sensitive medical images, such as X-rays, CT scans, Ultrasounds, MRIs, PET, and more, is essential to ensure confidentiality, data integrity, and correct treatments. Recent healthcare data breaches (HDB) report by Health Insurance Portability and Accountability Act (HIPAA) journal and cyberattacks targeting medical images and electronic medical records (EMR) have exposed vulnerabilities, emphasizing the need to safeguard patient privacy and prevent potential misdiagnoses or data tampering. This research aims to address these critical challenges in transmission and storage security, bolstering trust in healthcare systems and enhancing healthcare quality by ensuring the security and reliability of medical image data, ultimately promoting patient well-being, trust, and safety.

The security of medical image transmission (SoMIT) is a pivotal component of modern healthcare systems, ensuring the privacy, confidentiality, and integrity of patient data. This research involves a comprehensive investigation into enhancing SoMIT through the development and application of a novel methodology, which combines the Fuzzy-Analytical Hierarchy Process (Fuzzy-AHP) with extended fuzzy synthetic analysis, and degree of possibilities, and introduces the SoMIT metrics using MATLAB tools. The primary objective of this research is to provide healthcare organizations with an effective and adaptable approach to assess and enhance SoMIT, thus contributing to the overall improvement of healthcare data security.

The hybrid Fuzzy-AHP serves as the foundational SoMIT framework for decision-making in the evaluation of security factors and sub-factors. It allows for the integration of expert opinions and addresses the inherent uncertainty in decision-making processes. The extension of Fuzzy-AHP manages imprecise and incomplete information, crucial in the context of transmission security of medical images where data may not always be precise or complete. Degree of Possibilities (DP) accommodates the probabilistic nature of certain security aspects, enhancing the methodology's capacity to address and mitigate risks effectively. The SoMIT metrics specifically designed for this research serve as a

comprehensive set of metrics for quantifying security outcomes. The methodology also involves correlation and regression analysis to examine the relationships between SoMIT factors and security outcomes using MINITAB tools. SoMIT factors are Integrity [MS1], Authentication [MS2], Confidentiality [MS3], Access Control [MS4], and Availability [MS5].

The prioritization of these security factors and sub-factors reveals that integrity is the most critical component. This insight informs healthcare organizations on where to allocate resources and efforts in their security strategies. It emphasizes the significance of maintaining the accuracy and consistency of medical images, which is vital not only for patient privacy but also for the reliability of diagnoses, treatment, and patient trust.

The application of the developed methodology to real-world cases reveals that the overall security assessment, conducted through fuzzy scaling, results in a high-security level of 0.80754. A conducted correlation and regression analyses on 23 organizations to uncover intricate interrelationships between various factors and quantify security outcomes. The results provide essential insights into the factors that significantly impact SoMIT. This substantial score attests to the efficacy of the Hybrid Fuzzy-AHP approach and SoMIT metrics in significantly enhancing SoMIT. Healthcare organizations can use this level as a benchmark to gauge the effectiveness of their security measures and make informed decisions regarding resource allocation and risk mitigation strategies.

Furthermore, a comprehensive comparative analysis by evaluating the performance of the Hybrid Fuzzy-AHP methodology against other prevalent Multi-Criteria Decision Making (MCDM) techniques. The results demonstrate the superior performance of the proposed approach in enhancing SoMIT. This comparative analysis confirms the practical significance and efficiency of the developed methodology in addressing the unique security challenges posed by medical image transmission.

A comprehensive SoMIT framework for enhancing the security of medical image transmission in the healthcare sector. The prioritization of security factors, particularly Integrity, offers valuable guidance for healthcare organizations in their efforts to strengthen medical data security. The high-security level, as determined using the hybrid Fuzzy-AHP approach and SoMIT metrics, serves as a robust measure of security effectiveness and provides a benchmark for healthcare organizations to evaluate their security practices. The

interrelationship of factors and security aids in quantifying the strength of security and determining the direction of the relationship between two continuous parameters. Additionally, the validated results from statistical analysis, which include a case study illustrating the effectiveness and acceptability of the developed model and recommendations, undergo hypothesis testing. The null hypothesis is strongly rejected at the alpha level of significance in the two-tailed test. Consequently, the alternative hypotheses are accepted at a notably significant level, underscoring the vital need for improvements in the security of medical image transmission.

The comparative analysis highlights the superiority of the hybrid Fuzzy-AHP methodology over alternative MCDM techniques, reinforcing its practical significance in healthcare data security. Ultimately, this research advances the protection of sensitive patient data, strengthens trust in digital healthcare systems, and contributes to the broader field of information security.