E-Disha (Electronic Data Integrity and Security in Health Activities)

Prof. S. M. Shelke[1], Ajit Kumthe[2], Samartha Nagale[3], Gaurav Waware[4], Sanket Shitole[5]
[1,2,3,4,5]*Computer Engineering, SAE, Kondhwa*

***Abstract*: Data integrity is still a major issue in the modern healthcare industry. It makes sure the data is accurate and hasn't even been tampered with in any way. Inaccurate data may pose serious risks to patients' health and place a heavy burden on physicians, leading to issues including fraud, misbehaviour, insufficient care, and data theft. Managing medical data becomes extremely challenging in situations like these dangerous ones. This study aims to characterize the threat landscape of data integrity in the healthcare industry by utilizing a variety of attack statistics from both Saudi Arabia and the rest of the globe, as well as highlighting the significance of the situation there. The intended systematic literature review goal is stated through a literature review using descriptive analysis, unit analysis, and rating analysis.**

***Keywords:* Healthcare; security; electronic health records; storage; integrity; HIPPA.**

I. INTRODUCTION

Electronic data is essential to maintaining patient information, optimizing clinical workflows, and enhancing the quality of care in the modern healthcare era. Ensuring the integrity and security of electronic health data becomes crucial as healthcare institutions adopt digital technology and move away from paper-based records to electronic health records (EHRs).[1],[2]. The demand for effective patient care, data-driven decision-making, and increased accessibility to health information has led to a considerable digital change in the healthcare sector. Modern healthcare now includes electronic health records, telemedicine, wearable technology, and integrated healthcare systems.

The stability, consistency, and accuracy of data across the course of its lifecycle are referred to as data integrity. Upholding data integrity is essential in the healthcare industry to guarantee patient safety and treatment effectiveness. Misdiagnosis, inappropriate treatment, and impaired patient care can result from errors or inconsistencies in electronic health information. Health information is extremely valuable and delicate. Maintaining patient privacy and confidentiality is necessary to adhere to legal and ethical requirements, such as those outlined in the United States' Health Insurance Portability and Accountability Act (HIPAA). [3]

Furthermore, a report states that preserving data integrity is a more serious issue than other cyberthreats in the Kingdom of Saudi Arabia. Any patient could endanger their life if their medical records or information are tampered with. Our study aims to explore the various data sources.

An electronic health record comprises all the essential administrative and clinical data related to the care provided to a patient by a specific provider, including demographics, progress reports, problems, medications, vital signs, medical history, immunization records, laboratory data, and radiology reports. An electronic health record is defined as an electronic version of a patient's medical history kept by the health care provider for a certain period of time. The majority of healthcare institutions and organizations have a substantial paper trail as a result of using paper to record health data, and most of these organizations are interested in switching to electronic health records from paper-based ones.

II. LITERATURE REVIEW

In the investigation conducted by P. Vimalachandran1 and H. Wang, the emphasis was placed on ensuring data integrity in Electronic Health Records (EHR) and its consequential implications for quality health care. The research delved into the influence of data integrity on the utilization of EHR systems and addressed associated issues. The study identified and scrutinized three stages of an EHR system's data integrity. Ultimately, a viable technique for preserving the integrity of EHR systems was proposed. The analysis specifically scrutinized one of the primary clinical systems in Australia, shedding light on its impact on patient care quality and safety.[1]

Ismail Keshta and Ammar Odeh conducted a review focusing on the security and privacy concerns surrounding Electronic Health Records (EHR). The primary objective of this paper was to illuminate the privacy and security challenges faced by health organizations while exploring potential solutions. The review provided insights into incidents related to IT security within healthcare environments. The intention was to facilitate researchers' understanding of these security and privacy issues and to familiarize them with the available remedies.[2]

Mohammad Zarour and Mamdouh Alenezi addressed the persistent challenge of maintaining the accuracy of medical data in the digital health era. The significance of data integrity in the modern healthcare industry remains paramount, ensuring that information is accurate and free from tampering. The repercussions of inaccurate data are substantial, posing serious health risks for patients and imposing significant responsibilities on medical professionals. Moreover, inaccurate data can lead to issues such as fraud, misbehaviour, insufficient care, and data theft. The complexity of managing healthcare data becomes particularly pronounced in precarious situations like these. The study utilizes global attack statistics to characterize the threat landscape associated with data integrity in the healthcare industry.[3]

Jayneel Vora and Parth Devmurari introduced a secured E-Healthcare System based on blind signatures with the aim of enhancing efficiency and reducing costs. The paper addresses a critical concern associated with cloud-based paradigms, specifically the preservation of patient identification and health record privacy. The fear of compromising privacy acts as a significant impediment to fully exploring the potential applications of cloud technology in healthcare, as patients may be hesitant to disclose personal information due to mistrust. The study proposes a method that addresses these concerns by maintaining identification securely. Moreover, the suggested technique upholds patient privacy through the implementation of an authentication scheme that not only meets anonymity requirements but also adopts a flexible and adaptive approach within the cloud computing paradigm.[4]

Nikita R. Nikam and Priyanka R. Patil focused on providing an overview of data integrity, a crucial element highlighted in the US published 21 CFR Part 11, essential for regulatory enforcement. Given the increasing number of warning letters on data integrity issued by inspectors globally, the Food and Drug Administration (FDA) aimed to ensure the collection of reliable data throughout the drug production lifecycle and marketing. The FDA emphasizes electronic data standards with the acronym ALCOA, standing for Original, Attributable, Legible, Contemporary, and Correct. The paper comprehensively covers the concepts, applicability, advantages, disadvantages, legal requirements, and forms of data integrity. Furthermore, it delves into the risks to data privacy and proposes various strategies to mitigate these risks. The paper is deemed valuable for the industry in maintaining the security and accuracy of all data.[5]

Md. Shohidul Islam, Mohamed Ariff Bin Ameedeen. discussed a contains sensitive information and a vast number of individual health records. The necessity for accurate and secure storage of health data is highlighted in the virtual era of big data, considering the increasing diversity of health informatization. However, traditional health data exchanges pose challenges in terms of privacy breaches. Additionally, newly approved blockchain applications often face issues related to privacy and performance. In response to these concerns, the study proposes a blockchain-based system tailored for public health facilities. This system aims to ensure the safe and secure exchange and storage of information. The solution emphasizes security for sharing and storing health data within the blockchain by incorporating a hash-256-based access controller and transaction signature with a consensus policy. Through this method, the blockchain platform seeks to address privacy issues and enhance the overall security of health data transactions.[6]

III. SYSTEM ARCHIETECTURE

System Architecture for e-DISHA

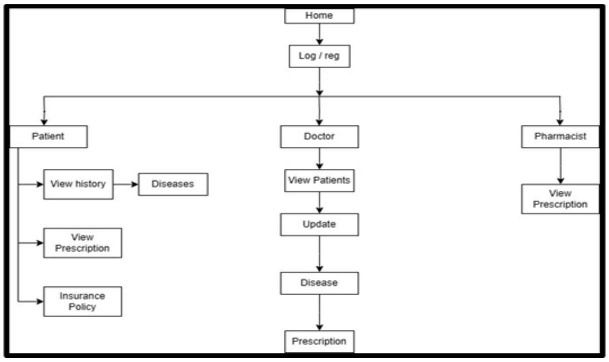

Figure 1: SYSTEM ARCHITECTURE DIAGRAM

VI. METHODOLOGY

The article's research discussed data integrity as a security problem in the healthcare industry and provided some numerical solutions. SLR contains articles that approach the issue of healthcare reputation from a particular angle. The different search numbers have been obtained from different digital archives in order to properly understand the search process. Through a thorough examination, the researchers want to uncover the current data integrity techniques employed by healthcare organizations and highlight the importance of healthcare data integrity challenges. This was achieved by compiling information on various breach statistics.

Data Security: Implement robust security measures to protect patient data, including encryption, access controls, and auditing. Compliance with regulations like HIPAA is crucial.

- Data Storage Technologies: Choose appropriate storage technologies such as relational databases, NoSQL databases, or specialized healthcare data warehouses, based on your data types and requirements.
- Scalability: Ensure the storage solution can scale to accommodate growing volumes of healthcare data over time.
- Data Redundancy: Implement data redundancy and backup strategies to ensure data availability and integrity.
- Data Retrieval: Create efficient mechanisms for retrieving and querying data, which may involve structured query languages (SQL) or specialized healthcare data query languages.
- Data Integration: Consider how data from various sources (e.g., EHRs, IoT devices) will be integrated and stored in a cohesive manner.[4]
- Data Lifecycle Management: Define data retention and archiving policies to manage data over time, considering legal and regulatory requirements.
- Data Privacy and Consent: Implement mechanisms for obtaining patient consent for data storage and sharing, and allow patients to control their data.
- Interoperability: Ensure your data storage methodology allows for interoperability with other healthcare systems and applications.
- Data Analytics: Plan for data analytics and reporting capabilities, which can help in clinical decision support and research.
- Compliance and Regulation: Stay up-to-date with healthcare data storage regulations and standards, and ensure your methodology complies with them.
- Disaster Recovery: Develop a disaster recovery plan to ensure data availability in case of emergencies.
- Monitoring and Maintenance: Regularly monitor the performance and health of your data storage system, and perform routine maintenance and updates.

  Training and Documentation: Train personnel on data handling best practices and maintain comprehensive documentation for data storage procedures.

V. CONCLUSION

The article's research discussed data integrity as a security problem in the healthcare industry and provided some numerical solutions. eDISHA contains articles that approach the healthcare issue from a particular angle. The researchers aim to emphasize the significance of healthcare data integrity concerns and identify the existing data integrity strategies used by healthcare organizations through a detailed analysis. This was accomplished by gathering data on different breach statistics. Thus, the issue of security and maintained EHR is solved. Retrieving is made easy.

REFERENCE

[1] P. Vimalachandran1, H. Wang, “Ensuring Data Integrity in Electronic Health Records: A Quality Health Care Implication”, See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/322929722

[2] Ismail Keshta a, ⇑, Ammar Odeh, “Security and privacy of electronic health records: Concerns and challenges”, https://doi.org/10.1016/j.eij.2020.07.003 1110-8665/ 2021

[3] Mohammad Zarour, Mamdouh Alenezi, “Ensuring data integrity of healthcare information in the era of digital health”, DOI: 10.1049/htl2.12008

[4] Jayneel Vora ∗, Parth Devmurari †, “Blind Signatures Based Secured E-Healthcare System”,

Conference Paper August 2018 DOI: 10.1109/CITS.2018.8440164

[5] Nikita R. Nikam1*, Priyanka R. Patil, "DATA INTEGRITY: AN OVERVIEW", International Journal of Recent Scientific Research Vol. 11, Issue, 06 (A), pp. 38762-38767, June, 2020

[6] Md. Shohidul Islam, Mohamed Ariff Bin Ameedeen, "Blockchain-enabled Secure Privacy-preserving System for Public Health-center".

[7] ABHISHEK KUMAR PANDEY1 , ASIF IRSHAD KHAN2, "Key Issues in Healthcare Data Integrity".