

Estimating the Impact of Blockchain Models for Securing Electronic Healthcare Records: Super Speciality Hospital Perspective

Thesis submitted in fulfillment of the requirements for
the Degree of

DOCTOR OF PHILOSOPHY

in

INFORMATION TECHNOLOGY



Submitted by

AMAL KRISHNA SARKAR

Supervised by

PROF. RAEES AHMAD KHAN

Department of Information Technology
Babasaheb Bhimrao Ambedkar University, Lucknow

Co-Supervised by

PROF. C. M. PANDEY

Department of Biostatistics & Health Informatics
Sanjay Gandhi Postgraduate Institute of Medical
Sciences, Lucknow

Submitted to

**Babasaheb Bhimrao Ambedkar University,
Lucknow, Uttar Pradesh, India**

MARCH-2021

ABSTRACT

Electronic health system has a numerous advantages but one cannot ignore the challenges that prevent the system from being utilized properly. Security and privacy challenges of the Hospital Information System (HIS) or Electronic Health Record System (EHR System) need to be understood properly and should be resolved. The purpose is to explore and analyze the present state of electronic health systems privacy and security of patient's health records. The focus is on security at the level of healthcare organization policy in order to protect and secure electronic patient records. Increasing security risk and financial consequences of breached patient data emphasized the fact that the security of electronic patient records in health information exchanges in an organization's imperative. For a patient care organization in a healthcare information exchange, only the security events with the loss reaching some critical importance and organizations would only spend a small portion on protection measures.

Sometimes movement of data from a single source or multiple sources to a new target source is needed data migration specifically in super speciality hospital setup data migration The Internet of Medical Things, Smart Devices, Information Systems, and Cloud Services have led to digital transformation in the healthcare industry. Digital healthcare services have paved the way for easier and accessible treatment, thus making our lives far more comfortable. However, the present day healthcare industry has also become the main victim of external as well as internal attacks. Data breaches are not just a concern and complication for security experts but they also affect clients, stakeholders, organizations, and businesses as well. Though the data breaches are of different types, their impact is almost the same.

This study provides insights into the categories and kinds of data breaches faced by different organizations. Furthermore, the main objective of this study is to do an in-depth analysis of healthcare data breaches and draw inferences from them, thereby using these findings to improve healthcare data confidentiality. The study found that hacking/IT incidents are the most prevalent attacks behind healthcare data breaches, followed by unauthorized internal disclosures. Frequency of healthcare data breaches, magnitude of exposed records, and huge financial losses due to breached records are increasing rapidly. Data from the healthcare industry is regarded as the most valuable and expensive. This has become a major lure factor for the misappropriation and pilferage of healthcare data. Addressing this anomaly, the present study employed the simple moving average method and the simple exponential smoothing method of time series analysis to comprehend the trend of healthcare data breaches and their cost. The simple moving average method provided more reliable forecasting results, as compared to the simple exponential smoothing method.

Blockchain technology is among the most significant developments and revolutionary innovations of the Information Technology industry. It corners a crucial space in the present digital era and has already made significant differences in human life. Moreover, it is anticipated that the Blockchain technology will improvise the existing IT facilities in the next several years in many domains. Recent technological developments are allowing for a major advancement in Healthcare sectors. Information security and accessibility are critical considerations for the integration and communication with Electronic Healthcare Record (EHR) systems when sharing private medical information. In this context, selecting the most effective blockchain model for secure and trustworthy EHRs in the healthcare sector requires an accurate mechanism for evaluating the impact of different available blockchain models for its features. The present study uses a scientifically proven approach for evaluating the impact of blockchain technology and provides a novel idea and path to the future researchers. This research analysis garnered the feedback of 56 domain

experts in the healthcare management for assessing the impact of different blockchain models.

To eliminate the ambiguities that arose due to multiple opinions of these experts and for the externalization and organization of information about the selection context of the blockchain model, the study used a decision model. Fuzzy Analytic Analytical Network Process (F-ANP) method was used to calculate the weights of the criteria as well as the Fuzzy-Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) technique was used to evaluate the effect of alternative solutions. Further, the results obtained through this empirical investigation will be an instrumental reference for choosing the most appropriate Blockchain model for maintaining breach-free EHRs.

Data migration is the movement of data from a single source or multiple sources to a new target database. It may be driven by a range of initiative starting from application up-gradation to replacement. The other areas may be the need to consolidate data within a data warehouse in an organization. The purpose is also to study the challenges in migration of healthcare data. With the goal of providing a comprehensive solution and improve the process of data migration and also meet out the challenges in migrating complex data, a strategy has been made. Considering the fact that a tertiary care super specialty hospital, the work requires in depth understanding of its unique requirements and the complexities involved in healthcare data. Hence it is an essential that the processes are efficient, and suitably enabled by latest technology.

The electronic health system has a numerous benefits but one cannot ignore the challenges that prevent the system from being utilized properly. Security and privacy challenges of the hospital information system (HIS) needs to be understood properly and should be resolved. The main purpose of this study is also to explore and analyze the present state of electronic health systems privacy and security of patient health records. The main focus on

security is at the level of healthcare organization policy in order to protect electronic patient record. Increasing security risks and financial consequences of breached patient data emphasized the fact that the security of electronic patient records in health information exchanges is an organization's imperative. For a patient care organization in a healthcare information exchange, only the security events with the loss reaching some critical importance and organizations would only spend a small portion of the intrinsic security risk on protection measures.