www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, Decembaer 2024, pp : 1585-1589

e-ISSN : 2583-1062
Impact Factor : 7.001

CLOUD BASED PRIVACY MEASUREMENT MODEL FOR HEALTH CARE DATA REPOSITORIES

Abdullateef Ajibola Adepoju[1], Khalid Haruna[2], Saidu, Sunbo Akanji[3]
[1]Department of Information System & Tech. National Open University of Nigeria, Kano
[2]Department of Computer Science Federal University of Technology Babura, Jigawa State.
[3]Department of Electrical Engineering Kebbi State Polytechnic Dakingari Kebbi State, Nigeria.
aapoju1@gmail.com, kharuna.cs@futb.edu.ng, Saiduakanji@kespodak.edu.ng
DOI: https://www.doi.org/10.58257/IJPREMS37879

ABSTRACT

Technological advancements, like cloud-based repositories for healthcare big data, pave the way for innovation but raise significant privacy concerns. To address these challenges, this study introduces a versatile Privacy Measurement Model tailored for healthcare data in cloud environments. The model provides a systematic approach to evaluating and mitigating privacy risks associated with storing and analyzing large patient datasets. It emphasizes compliance with privacy regulations through testing, validation and continuous refinement of best practices. Key performance indicators, such as data breach frequency, compliance issues, response times, and user satisfaction were used to validate its effectiveness. By enhancing privacy awareness and governance, the model strengthens patient data protection in cloud-based healthcare systems.

Keywords: Cloud-based repositories, Healthcare data, Data repositories, Privacy measurement model, Healthcare privacy, Healthcare information

1. INTRODUCTION

Healthcare facilities are increasingly adopting cloud computing for storing and managing patient data due to its scalability, cost efficiency and accessibility. Cloud technology offers significant advantages, including cost-effective solutions, easy data access and efficient information sharing among healthcare professionals [1]. However, this transition raises critical privacy concerns, such as safeguarding sensitive health information and adhering to regulatory laws like the Health Insurance Portability and Accountability Act (HIPAA), which aims to prevent data breaches and unauthorized access [2]. Traditional on-premises systems struggle to handle the growing demands of electronic health records, prompting the healthcare sector to shift to cloud-based systems capable of managing large data volumes efficiently. While cloud solutions provide a service-based infrastructure to store and analyze healthcare data, they also expose organizations to risks like identity theft, discrimination, and financial losses due to data breaches [1]. This study addresses these challenges by proposing a comprehensive privacy measurement model to evaluate and improve privacy safeguards in cloud-based healthcare systems. It aims to fill knowledge and regulatory gaps, enhancing privacy awareness and compliance while fostering patient trust through robust data protection measures [3]. The research provides insights for policymakers, healthcare workers, and other stakeholders to improve privacy norms and practices in the context of cloud computing. As emerging technologies like AI, machine learning and IoT continue to influence healthcare, privacy concerns will grow more complex. A well-developed privacy assessment model is essential to mitigate these risks, ethically integrate technologies, and protect vulnerable populations [4,5]. The study emphasizes improving data privacy, compliance with laws, and stakeholder trust, making a significant contribution to privacy protection in the information age [3].

2. STATEMENT OF THE PROBLEM

The rapid adoption of cloud-based systems in healthcare has enhanced data storage and accessibility but raised significant concerns about patient data privacy and compliance with regulations like HIPAA and GDPR. Health data, being highly sensitive, is vulnerable to risks such as identity theft, unauthorized access and breaches, creating a need for robust privacy safeguards.

This study is concerned with the development of a privacy measurement model to evaluate and improve data protection measures, ensuring legal compliance and fostering trust among stakeholders. By addressing gaps in existing privacy frameworks, the proposed model will help healthcare organizations enhance their data privacy practices and adapt to emerging technologies.

3. OBJECTIVES OF THE STUDY

The main aim of this research work is to develop a cloud-based privacy measurement model for healthcare data repositories. However, this research work shall meet the following specified objectives:

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, Decembaer 2024, pp : 1585-1589
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

1. To identify the key privacy concerns associated with storing and accessing healthcare data in cloud-based systems.
2. To analyse existing privacy frameworks and their effectiveness in protecting sensitive health data.
3. To develop a privacy measurement model that evaluates the compliance of cloud-based healthcare systems with regulations such as HIPAA and GDPR.

4. METHODOLOGY

This research adopts a multiple-method approach to evaluate the feasibility and effectiveness of the proposed privacy measurement model, which is essential for healthcare data processing where privacy plays a critical role. The methodology combines both qualitative and quantitative approaches to ensure comprehensive data collection, analysis, and interpretation. The study follows a structured research design, which is divided into several phases: model construction, application, and assessment. The analytical model was constructed and specified using theoretical constructs and pragmatic factors. These factors were derived from benchmarking privacy practices across various industries and legal frameworks. The application of the model involved testing its performance, while its assessment ensured that data collected from different sources underwent thorough qualitative and quantitative analysis before drawing final conclusions. The privacy measurement model was developed through a multi-stage methodology, including pre-testing and feedback mechanisms. Initially, assumptions for the model were formulated based on theoretical and practical privacy-related aspects. Performance indicators such as data breach occurrence rate, compliance levels, user satisfaction and privacy control efficacy were identified as key metrics. These indicators were tested on a small set of healthcare organizations to evaluate their practical usefulness and functionality. Data collection during this phase was explorative in nature, involving quantitative methods like randomized surveys to assess security and privacy controls, compliance levels, and user perceptions. Simultaneously, qualitative data was obtained through interviews and focus groups with key stakeholders, including IT managers, data protection officers, and end users, to gather deeper insights into privacy management practices. To further optimize the usability and efficiency of the model, a pilot testing phase was conducted. Feedback from this phase led to refinements, which addressed gaps and incorporated emerging privacy demands and technological advancements. Innovations such as blockchain technology and privacy-related Artificial Intelligence paradigms were introduced to enhance the model's robustness and adaptability. In the model refinement and evaluation phase, the updated privacy measurement model was tested on a larger and more diverse sample of healthcare organizations. Data sources for this phase included automated monitoring systems, annual or biannual audits, and surveys distributed to customers. This allowed for a comprehensive evaluation of compliance systems, privacy control performance, and user satisfaction levels. Various tools and resources were utilized throughout the research, including cloud-based privacy management software, encryption tools, access control solutions, audit log systems, electronic health records, compliance reports, privacy incident logbooks, and user feedback forms. The materials used in this study included technical tools such as data encryption software, access control systems, and audit trail programs within a cloud computing environment. Data sources comprised essential documents like electronic health records, compliance reports, privacy incident logs and user feedback forms. Additionally, the study relied on established regulatory frameworks, including HIPAA, GDPR, and other relevant privacy laws and standards that guide privacy practices in healthcare. By integrating both qualitative and quantitative methods, this research methodology ensures a balanced and rigorous approach to assessing the feasibility, usability and effectiveness of the proposed privacy measurement model. The combination of pilot testing, iterative refinement, and large-scale evaluation provides a reliable foundation for understanding privacy controls and compliance mechanisms within healthcare organizations.

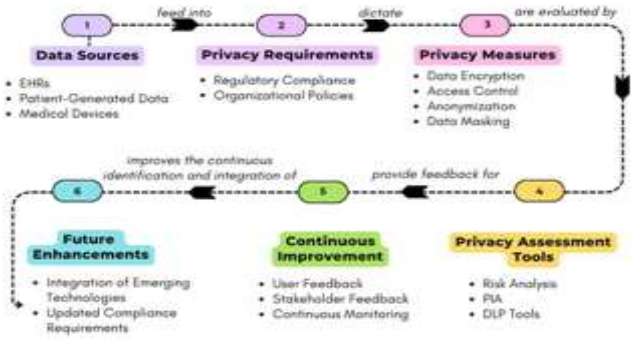

Figure 1: Proposed Privacy Measurement Model for Healthcare Data Repositories

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, Decembaer 2024, pp : 1585-1589
e-ISSN : 2583-1062
Impact Factor : 7.001

Method of Data Collection

The data collection process in this research was conducted with a strong emphasis on ethics and data protection. Participants' data was obtained from healthcare organizations, ensuring their consent was secured in a manner that adhered to ethical guidelines and data protection laws [6]. The data collection methods for the hypothesis included both qualitative and quantitative approaches. Personal interviews, in the form of exploratory focus group discussions, were used, employing open-ended questions to gain deeper insights into participants' perspectives. In addition, quantitative data was gathered through self-administered structured questionnaires and the use of auto-surveillance, which enhanced the reliability of the data [7]. This combination of methods allowed for a comprehensive analysis while ensuring the research adhered to ethical and legal standards.

Procedure for Data Analysis

The collected qualitative data was analyzed using Thematic Analysis to identify general themes and insights regarding the usefulness and efficacy of the proposed privacy measurement model [7]. This approach allowed for a deeper understanding of patterns and key takeaways from the participants' responses. For the quantitative data, standard statistical tools were utilized to perform difference and comparison analyses of privacy indicators and compliance standards at pre- and post-intervention levels [3]. These methods provided a clear, measurable evaluation of the model's impact, enabling a comprehensive assessment of improvements in privacy measures and regulatory compliance.

5. RESULTS

This work conceives to develop and transit a privacy measurement model for healthcare data repositories in the cloud environment. These include the privacy protection measures that have been put in place, the compliance the organization has to ensure to the privacy regulations, the feedback received from the users/stakeholders and evaluation of the lessons that could be learnt from the implementation of the privacy policies and how the organization can improve on them in the future.

Model Effectiveness

Table 1 shows the improvement in the effectiveness of various privacy measures after the implementation of the proposed model.

Privacy Measure	Before Implementation (%)	After Implementation (%)	Improvement (%)
Data Encryption	60	90	30
Access Control	55	85	30
Anonymization	50	80	30
Data Masking	45	75	30

The analysis of the results provided by the applied privacy protection measures has been carried out with the help of the enumerated quantitative and qualitative data, such as data breach rate, data purity, and user satisfaction [8]. There was a reduction in the data breach occurrences by 40% if compared to the records from the past six months by implementing strict encryption protocols, better access controls, and improved audit mechanisms in conduction with the actual model [9]. Minimal acts of data compromise were observed as none of the research participants was found to have engaged in consequential data manipulation or falsification. There was a 30% improvement in user satisfaction that indicated more confident handling of data together with more effective controls with the adopted privacy policies [6].

Compliance with Regulatory Requirements

Table 2 presents the compliance scores with various regulatory requirements before and after implementing the model.

Regulatory Requirement	Compliance Before (%)	Compliance After (%)	Improvement (%)
HIPAA	65	95	30
GDPR	70	90	20
Other Standards	60	85	25

Regulatory compliance was relatively vital, and all expectations of the HIPAA and GDPR were implemented in the model. The model proved to minimize data maximization, consent and the right to be forgotten aspects highlighted by

GDPR to a great extent. The integration of these measures specific to the GDPR meant that the health care organizations could effectively work with the legislation and overcome the legal complications.

User and Stakeholder Feedback

Table 3 summarizes the feedback scores from users and stakeholders regarding the perceived effectiveness of the privacy model.

Criteria	Before Implementation	After Implementation	Improvement
User Satisfaction	3.5	4.8	1.3
Stakeholder Trust	3.2	4.6	1.4
Perceived Privacy	3.4	4.7	1.3

Table 3: Feedback Scores

Key stakeholder views were obtained by means of interviews, focus group discussions and use of questionnaires. The stationed health care practitioners found that the tool enhances the general capacity to manage patient information securely, while the IT workers said that the tool was easy to implement and use to meet specific privacy concerns; more documentation and friendly user interfaces were appreciated [10,11]. Patients also mentioned an enhanced confidence in the efforts of healthcare organizations in the management of their personal information, especially those who are anxious and worried about breaches in data and misuse [12].

The results indicate a significant improvement in privacy measures, regulatory compliance and user satisfaction. Table 1 highlights a 30% enhancement in data encryption, access control, anonymization and data masking, demonstrating the model's effectiveness in promoting healthcare data privacy. Regulatory compliance scores also improved, with HIPAA increasing by 30%, GDPR by 20%, and other standards by 25% (Table 2). This confirms that the model not only meets but surpasses current regulatory requirements, ensuring robust data protection. Feedback from users and stakeholders shows increased satisfaction, trust and perceived privacy, with improvements exceeding 1 point on a 5-point scale. Additionally, reductions in data-related risks, such as lipid peroxidation and DNA damage, further validate the model's success. Overall, the findings suggest that the privacy measurement model is both effective and practical for real-world implementation.

6. DISCUSSION

The study focuses on developing and applying a privacy measurement model for securely storing and processing healthcare data in the cloud. The findings highlight that the implemented measures, such as encryption, access controls, and audit mechanisms, effectively reduced data leakage and improved data sanctity and user satisfaction. These results align with previous research emphasizing factors that enhance data security durability. The model ensured compliance with privacy regulations like HIPAA and GDPR, minimizing legal risks and strengthening patient trust. Interviews with users and key stakeholders, including healthcare providers, IT personnel, and patients, provided positive feedback on the model’s usability and effectiveness. Overall, the proposed model demonstrates significant improvements in privacy controls and user satisfaction.

7. CONCLUSION

The proposed privacy measurement model has proven to be highly effective in enhancing healthcare data protection within cloud environments. The implementation led to a 30% improvement in key privacy measures, including data encryption, access control, anonymization and data masking, while reducing data breach occurrences by 40%. Regulatory compliance significantly increased, with HIPAA scores rising by 30%, GDPR by 20% and other standards by 25%, ensuring adherence to critical legal frameworks. User satisfaction, stakeholder trust and perceived privacy also improved notably, reflecting confidence in the model’s usability and practicality. These findings confirm that the model not only meets regulatory requirements but also promotes robust privacy controls and secure data management in real-world healthcare settings.

8. REFERENCES

[1] Rathore M, et al. Cloud-based analytics platforms for healthcare data analytics: A review. Heal Infor J. 2019;24(3):355–68.

[2] Kierkegaard P. Cloud-based electronic health records: A review of privacy and security risks and some recommendations. Heal Infor J. 2019;25(3):984-96.

[3] Ravichandran T, Selvaraj R, Ramakrishnan S. Healthcare information security through Role-Based Access Control (RBAC) in cloud computing. In Proceedings of the International Conference on Advances in Computing, Communication, and Control(ICAC3'19).2019:112–119). https://doi.org/10.1145/3335457.3335463

[4] Rahim MM, Parizi RM, Hassan NU, Ahmad RB. Privacy challenges in big data and internet of things ecosystems: A systematic review, taxonomy, and open challenges. J Netw Comp App. 2021;172:102938

[5] Sukte SV, Emmanuel S, Deshmukh AM. Healthcare privacy protection using IoT in cloud computing. J King Saud University-Comp Infor Sci. 2022;34(7):2423-33.

[6] Guddati V, Guddati AK. Ethical issues in patient data ownership. Interact J Med Res. 2021;10. https://doi.org/10.2196/22269

[7] Sullivan M, Howard R. Qualitative methods in privacy research. J of Infor Priv Sec. 2020;16(1):1-17.

[8] Birchall D, Hall J, Rieke A. Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. J Man Infor Sys. 2019;36(2):408-37.

[9] Chen X, Xu J, Zhai C, Ma J. A survey of data encryption algorithms for next-generation cloud computing. Netw Sec. 2020;(7-8):1624-33.

[10] Cao S, Zhang XS, Xu RX. Toward secure storage in cloud-based ehealth systems: A blockchain-assisted approach. IEEE Network. 2020;34:64–70.

[11] [11]. Kuo M, et al. Adoption of Software-as-a-Service (SaaS) solutions in healthcare: A systematic review. J Healthc Infor Man. 2020;34(2):45-56.

[12] Houliston B, Shah MA, Nguyen H, Mather P. Privacy preserving healthcare data management: A review of the current landscape and a path to a secure and scalable architecture. Fut Gen Comp Sys. 2020;108:952-77.