INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1537-1543
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

SECURITY AND PRIVACY CONCERNS IN CLOUD-BASED HEALTHCARE DATA REPOSITORIES: A COMPREHENSIVE STUDY

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, Nigeria

[3]Department of Electrical Engineering, Kebbi State Polytechnic Dakingari, Kebbi State, Nigeria

Corresponding author's email address: aapoju1@gmail.com

DOI: https://www.doi.org/10.58257/IJPREMS39941

ABSTRACT

Although cloud-based healthcare data repositories increase cost-effectiveness and accessibility, there is a significant danger of security and privacy breaches. This study offers a thorough analysis of the body of research, highlighting important topics like data breaches, data sovereignty and unauthorised third-party access. The term "centralisation" describes the concentration of smaller, independent operations in one location where higher security can be used, like scalable storage. However, this has drawbacks, as cross-jurisdictional data storage makes it more difficult to comply with regulations and cloud storage is more susceptible to cyberattacks. Furthermore, one of the main reasons for stringent controls and audits is the possibility of unauthorised access. This study has ethical and legal ramifications, including the need for informed patient permission and adherence to changing data protection regulations. To reduce these dangers, it suggests robust encryption, more comprehensive data governance and continuous enhancement of cybersecurity. To create standardised best practices, regulators, IT firms and healthcare providers should collaborate.

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

1. INTRODUCTION

The data management integration in cloud computing healthcare has not only transformed the infrastructure for data storage but also made it easier and more convenient to retrieve patient records. It is a technological development that makes data-driven decision-making and collaborative care possible. However, there are more security and privacy risks associated with moving sensitive health data to cloud platforms, so we must handle this securely and carefully in accordance with regulatory standards to maintain patient trust.

Healthcare data repositories are cloud based that help healthcare providers store and retrieve an enormous patient information credibly. Regardless of its application, the functionality of these systems supports health information exchange (HIE), electronic health records (EHRs), telemedicine and the quality and continuity of care. Health care entitles can utilize cloud services to balance the growth of loads with relatively low investments in physical infrastructure. In addition, cloud platforms enable the sharing of real time data between the professionals authorised to participate in the collaborative treatment.

Due to these reasons, the transition to the cloud-based systems becomes a critical issue concerning security and privacy. The healthcare data itself is very sensitive, comprising of personal identifiers, medical histories, diagnostic results and treatment plans. Unauthorized access, data breaches and cyberattacks could compromise patient confidentiality and create identity theft and financial fraud, eroding public's trust in the healthcare institutions. For instance, concerts within virtual healthcare services pose a major data security risk; the data breach at Confidant Health involved exposure of extensive health information and personal details for thousands of patients [1].

In this regard, the Healthcare Data has also gained special importance due to the dynamic legislative environment. In respect to accessing personal health information, there are legislations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe that have strict laws that oversee how such information is handled. This will result in huge fine, penalties and legal ground for non-compliance. Currently it is this ongoing tension between allowing the data to be accessible to security personnel (regardless of its locality) and the need to maintain individual privacy that has resulted from recent demands from the UK government to technology companies to make encrypted user data available to the government.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
www.ijprems.com
editor@ijprems.com
Vol. 05, Issue 04, April 2025, pp : 1537-1543
e-ISSN : 2583-1062
Impact Factor : 7.001

2. OBJECTIVES OF THE STUDY

This study aims to thoroughly examine the security and privacy issues raised by cloud-based healthcare data repositories. The objectives are threefold:

1. The primary security and privacy risks occurring within cloud-based healthcare data storage and transmission.
2. Estimate the efficacy of current security strategies and devices in counterbalancing the risks listed out.
3. Proposal of recommendations for maintaining patient data security in cloud environments.

The study intends to help develop more secure and privacy preserving cloud-based healthcare system. The considered objectives will create a viable solution in which the benefits of cloud computing can be realized without compromising patient trust and compliance with regulatory requirements.

3. METHODOLOGY

The present study follows a descriptive and exploratory research design, relying solely on secondary data sources to investigate the security and privacy concerns in cloud-based healthcare data repositories. This approach is suitable for synthesizing existing knowledge, identifying research gaps and gaining a comprehensive understanding of the field without the need for primary data collection techniques such as interviews or surveys [3,4]. The study adopts a systematic process of reviewing relevant literature and analyzing real-world case studies to provide both theoretical and practical perspectives on the subject matter. Data collection was carried out through a systematic review of scholarly literature and detailed analysis of case studies, focusing on the time span between 2010 and 2025 to capture both foundational developments and recent advancements. Relevant keywords, including "cloud computing," "healthcare data," "security," "privacy," and "data breach," were used to search across academic databases such as PubMed, ScienceDirect, IEEE Xplore, and ACM Digital Library [6]. The inclusion criteria were strictly limited to peer-reviewed articles written in English and directly related to cloud-based healthcare data security and privacy. From an initial pool of 1,245 retrieved articles, a rigorous screening process resulted in the selection of 87 articles that met the criteria for final analysis [7,8]. To complement the literature review, a detailed examination of real-world case studies was conducted to understand how theoretical security models and policies translate into practice. Particular attention was given to incidents involving actual breaches in healthcare organizations that utilized cloud repositories. This included high-profile events such as the 2024 data breach of Confidant Health, where an unsecured cloud database led to the exposure of protected patient information, emphasizing the importance of robust security frameworks [11]. Another significant case analyzed involved a major healthcare provider that became the target of a ransomware attack, resulting in disruption of medical services and violation of patient privacy [12].

The selection of these case studies was based on their relevance and authenticity, with sources including industry reports, cybersecurity whitepapers, and credible news articles [9,10]. These examples provided concrete illustrations of how inadequate security practices can lead to severe consequences, while also offering lessons on mitigation strategies and the evolution of security policies in healthcare environments.

Through the integration of a systematic literature review and real-world case analysis, this methodology offers a comprehensive approach that bridges academic research with applied healthcare data security concerns. The combination enables a deeper understanding of both the current landscape and the persistent challenges in ensuring the privacy and integrity of cloud-based healthcare data systems.

Procedure for Data Analysis

The analysis of qualitative data through thematic breakdown from literature review and case studies described security and privacy issues in cloud-based healthcare data repositories according to [13]. The research analysis method used coding tools to sort data into four core segments consisting of data breaches, privacy violations, compliance difficulties and security protection techniques. The method enabled security professionals to discover major threats along with assessing present security protocols' operational effectiveness [14].

4. RESULTS

The following section presents the outcomes from numerous sources alongside case-specific data related to security and privacy threats affecting health data storage in cloud databases. The result was presented under the following relevant sub-headings:

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
www.ijprems.com
editor@ijprems.com
Vol. 05, Issue 04, April 2025, pp : 1537-1543
e-ISSN : 2583-1062
Impact Factor : 7.001

A. Systematic Literature Review Findings

Various persistent security and privacy problems related to cloud-based healthcare systems emerged through the reviewed literature analysis.

1) Data Breaches and Unauthorized Access

Many research reports established that unauthorized access to private patient data stored in cloud platforms has caused numerous breaches throughout healthcare systems. Studies showed that weak access controls combined with insufficient authentication methods were commonly listed among the contributing elements. Mehraeen et al. demonstrated that cloud-based EHRs need secure authentication and authorization solutions to stay protected [18].

2) Compliance with Regulatory Standards

Healthcare organizations must focus on HIPAA adherence among other regulatory standards because this was determined to be a major challenge. According to studies cloud service providers require implementing thorough security protocols to fulfill regulatory standards and safeguard patient confidentiality information [19].

3) Data Integrity and Availability

The protection and easy access to healthcare information stored in cloud systems demonstrated itself as a major problem. Research suggest data corruption, loss and availability problems will produce severe negative effects on patient treatment. The authors suggested using redundancy systems and regular backup protocols to deal with these security risks [7].

4) Insider Threats

The examination of literature showed insider threats pose a threat because authorized personnel misuse their access to breach patient information. User activities should be monitored as well as strict access controls to serve as effective countermeasures according to the recommendation research [20].

B. Identified Security Challenges

Various security challenges in cloud-based healthcare data repositories emerged during the review of literature as identified in multiple studies.

- Data breaches constitute a substantial security challenge because they permit unapproved users to access private patient records. The compromise of Confidant Health exposed patient therapy sessions alongside their personal details which affected thousands of patients because the database remained unsecured [21].
- Weak access control functions enable unauthorized users to gain entry to health data which should remain confidential. Access control measures need to be implemented robustly for organizations to reduce this risk because they must include multi-factor authentication and role-based access control [19].
- Data Loss and Recovery requires effective solutions because medical systems can fail because of system breakdowns and cyber-attacks. The data recovery features of cloud computing after natural disasters create extra layers of protection for data security as well as privacy [7].
- Maintaining data security through HIPAA healthcare regulations alongside other health policies demands absolute compliance from healthcare providers. Organizations facing non-compliance issues will face legal penalties as well as patient trust breakdowns [7].

C. Privacy Concerns

Roeltgen M. P. (2020) conducted a study that revealed major privacy issues related to healthcare data storage systems based in the cloud:

- Patient concerns: Managing patient consent operations for data storage and sharing tasks proves complicated in cloud-based systems. Healthcare operators must establish policies with proper procedures to protect patient self-determination and build trust [22].
- Data Anonymization: Patient identity protection through anonymization techniques remains vulnerable to re-identification attempts because insufficient anonymization behaves as a security threat. Protection of patient privacy requires the deployment of effective strong anonymization systems [23].

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
www.ijprems.com
editor@ijprems.com
Vol. 05, Issue 04, April 2025, pp : 1537-1543
e-ISSN : 2583-1062
Impact Factor : 7.001

D. Mitigation Strategies

Multiple solutions exist according to literature to solve the problems security and privacy present in cloud environments.

- Encyption: Every healthcare organization must follow encryption practices to secure data during resting periods and transit phases since these measures protect against unauthorized access attempts. Cloud-based healthcare systems benefit from state-of-the-art encryption techniques which elevate their data security level [24].
- Regular Audits: The practice of conducting frequent audits through security inspections supports both compliance checks and new vulnerability detection for protecting data against unauthorized access. Healthcare data integrity needs proactive measures because this is essential for its continued maintenance [18].
- Access control: The proper execution of access controls by adopting multi-factor authentication and role-based access control allows authorized healthcare personnel to access medical data securely [25].

E. Case Study Insights

The examination of genuine healthcare data repository incidents in the cloud offered concrete evidence about security failures that led to data breaches:

Sensitive patient information became accessible because Confidant Health operated an insecure database which revealed therapeutic sessions and patient details. The occurrence demonstrates why cloud-based healthcare systems absolutely need strong data protection measures [7].

A data breach occurred at Confidant Health during August 2024 because an insecure cloud database exposed more than 5.3 terabytes of protected patient information along with therapy session recordings and medical history files. The incident demonstrated the fundamental need to secure cloud storage configurations because they prevent unauthorized access [18].

F. Ransomware Attack on Healthcare Provider

Ransomware hackers attacked a big health organization which caused them to lock patient information while interrupting clinical treatment operations. Such vulnerabilities existed within the provider's cloud infrastructure because their security measures were insufficient and thus resulted in this attack which required urgent vulnerability assessments to prevent similar threats [25].

5. DISCUSSION

This research reveals multiple security and privacy challenges which affect data repositories that use cloud-based health systems. Security challenges in healthcare data repositories that require attention consist of data breaches and regulatory compliance as well as data integrity and insider threats. These security problems require organizations to enact broad protection plans which combine multiple security elements such as strong authorization systems and systematic data backup protocols along with constant system supervision and regulatory protocols compliance. Healthcare organizations gain significant benefits by integrating cloud computing since it provides both increased accessibility of data combined with expanded scalability and reduced costs. The migration process brings important security together with privacy difficulties which healthcare institutions need to handle thoroughly to safeguard delicate patient information. The main threat people face with the cloud is exposure to data breaches. Cloud storage's centralized configuration attracts cyber criminals because it provides them easy targets. Strong security measures for cloud configuration systems are essential due to the 2024 security breach at Confidant Health which revealed more than 5 terabytes of health data stored in an insecure database [18]. Data sovereignty presents another challenge. The data storage operations of cloud service providers typically span several jurisdictions that maintain different sets of data protection rules. Healthcare organizations face difficulties in data compliance because various legal frameworks overlap with one another thus requiring them to guarantee patient data protection [26]. The possibility of third-party unauthorized access to patient data ends up threatening patient privacy in substantial ways. The health data accessible through cloud service personnel and external entities creates stronger possibilities for unauthorized disclosure of personal healthcare information. Healthcare organizations need to establish strong access restrictions alongside extensive review procedures for third-party interaction to manage this potential risk [26]. New health care regulations create more obstacles for organizations to use cloud-based solutions in healthcare. New York legislators have proposed the Health Information Privacy Act to protect patient data through restrictions on health application data sharing unless users explicitly provide their consent [27]. The aim of these safety regulations is to protect privacy but healthcare providers together with technology companies face increased compliance requirements as a result. Ethical

factors serve as a primary essential component. Patients need to receive information about the complete procedures involved in data collection and storage as well as usage of their information. The integrity of healthcare relationships depends substantially on clear explanations between doctors and patients as well as obtaining patient agreement. The matter of monetizing health data by turning it into anonymized information continues to generate debates between medical research enhancement and patient privacy protection as discussed by political figures like Tony Blair and William Hague [28]. Healthcare organizations need to put in place complete data encryption procedures which protect resting and moving data against unauthorized access. System vulnerabilities and weaknesses in the system become detectable through regular security audits and vulnerability assessments [26]. Businesses need complete guidelines for data governance to operate successfully. The security frameworks need to clearly establish who owns the data alongside access control policies as well as responsibility systems to define each stakeholder responsibility in protecting data security [26]. The establishment of ongoing cybersecurity practice advancement requires complete organizational commitment. Security threats develop with new patterns that require corresponding security strategies to counteract these developments. The organization must monitor emerging cybersecurity trends while modifying its procedures and policies [26].

6. SUMMARY OF KEY FINDINGS

The deployment of healthcare data systems in cloud environments provides organizations with benefits which include flexible growth capabilities combined with financial savings and enhanced data availability. These operational benefits come with major security challenges that create both vulnerabilities and requirements to follow healthcare privacy regulations such as HIPAA and GDPR [3,4].

1) Research findings show that security threats at the organization mainly stem from data breaches combined with ransomware attacks together with insider threats [9]. The Poor security measures at Confidant Health in 2024 demonstrated how vulnerable patient data becomes when an unsecured database leads to a data breach [10]. The number of ransomware attacks against healthcare organizations has increased to the point where they disrupt medical operations while endangering patient privacy [12].
2) The threats in healthcare data security have met several proposed responses which combine advanced encryption strategies with multi-factor authentication methods alongside continuous system monitoring capabilities according to [8,7]. Strategic implementation of these security measures becomes possible by following regulatory compliance guidelines while implementing extensive employee education that reduces human mistakes which trigger most security incidents [11,12].
3) Healthcare institutions need to establish defense layers from both technical and administrative approaches with physical protection strategies to deliver stronger data protection systems. Healthcare organizations need to spend in modern cybersecurity technologies which combine artificial intelligence to detect potential security breaches [29].
4) Following the principles of HIPAA and GDPR should be a top priority because they ensure patient privacy protection and maintain data integrity [30]. Strengthened data governance frameworks alongside scheduled security audits help organizations demonstrate accountability and maintain legal compliance [6].

7. CONCLUSION

A broad examination of security and privacy risks linked to cloud-based healthcare information storage units was achieved through both systematic review of research literature and assessment of actual healthcare scenarios. The results indicate healthcare organizations must implement thorough security protections to defend private medical records because cloud computing has become essential in modern healthcare systems.

8. References

[1] Wired. Therapy Sessions Exposed by Mental Health Care Firm's Unsecured Database. Available from: https://www.wired.com/story/confidant-health therapy-records-database-exposure

[2] The Guardian. UK demands ability to access Apple users' encrypted data. Available from: https://www.theguardian.com/technology/2025/feb/07/uk-confronts-apple-with-demand-for-cloud-backdoor-to-users-encrypted-data

[3] Alzubi JA, Singh A, Aloudat A. A survey of cloud computing security challenges and solutions. Computers in Human Behavior. 2022;125:106906.

[4] Kaur H, Sood SK. Analyzing security attacks in cloud computing: A systematic review. Journal of Network and Computer Applications. 2021;178:102996.

[5] Moher D, Liberati A, Tetzlaff J, Altman DG. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Med. 2009;6(7):e1000097

[6] Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A, Khan SU. The rise of "big data" on cloud computing: Review and open research issues. Information Systems. 2015;47:98-115.

[7] Mehraeen E, Ghazisaeedi M, Farzi J, Mirshekari S. Security challenges in healthcare cloud computing: A systematic review. Global Journal of Health Science. 2017;9(3):157

[8] Zhang R, Liu L. Security models and requirements for healthcare application clouds. IEEE Cloud Computing. 2019;6(2):64-71.

[9] Chinthakindi S, Dantu R, Wijesekera D. Security and privacy issues in cloud computing: A survey. Journal of Computer Security. 2023;31(1):49-82.

[10] Scher K. Therapy sessions exposed by mental health care firm's unsecured database. Wired. 2024. Available from: https://www.wired.com/story/confidant-health-therapy-records-database-exposure

[11] Zimba A, Wang Z, Chen H. A survey of cybersecurity attack detection in cloud computing. Journal of Cloud Computing. 2021;10(1):1-32.

[12] O'Dowd E. Ransomware attack cripples US healthcare system, exposing data and disrupting care. HealthITSecurity. 2024. Available from: https://healthitsecurity.com

[13] Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006;3(2):77-101.

[14] Nowell LS, Norris JM, White DE, Moules NJ. Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods. 2017;16(1):1-13

[15] Resnik DB. What is ethics in research & why is it important? National Institute of Environmental Health Sciences. 2020.

[16] Heale R, Forbes D. Understanding triangulation in research. Evidence-Based Nursing. 2013;16(4):98

[17] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ. 2021;372:n71

[18] Therapy Sessions Exposed by Mental Health Care Firm's Unsecured Database. Wired. 2024. Available from: https://www.wired.com/story/confidant-health-therapy-records-database-exposure

[19] Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. Computers. 2024;13(2):41. Available from: https://www.mdpi.com/2073-431X/13/2/41

[20] Security and Privacy Concerns in Cloud-based Scientific and Business Workflows: A Systematic Review. arXiv preprint arXiv:2210.02161. 2022. Available from: https://arxiv.org/abs/2210.02161

[21] A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses. arXiv preprint arXiv:2005.07359. 2020. Available from: https://arxiv.org/abs/2005.07359

[22] Soveizi N, Turkmen F, Karastoyanova D. Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. arXiv preprint arXiv:2210.02161. 2022.

[23] Bose S, Marijan D. A survey on privacy of health data lifecycle: A taxonomy, review, and future directions. arXiv preprint arXiv:2311.05404. 2023.

[24] Newaz AI, Sikder AK, Rahman MA, Uluagac AS. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. arXiv preprint arXiv:2005.07359. 2020.

[25] Security challenges in healthcare cloud computing: A systematic review. Global Journal of Health Science. 2017;9(3):157.

[26] Privacy Concerns in Cloud-Based Healthcare Systems. DEV Community. Available from: https://dev.to/iskender83/privacy-concerns-in-cloud-based-healthcare-systems-3agg

[27] New Yorkers' health data faces tighter protection under new bill. Times Union. 2025. Available from: https://www.timesunion.com/capitol/article/new-yorkers-health-data-face-stricter-protection-20163245.php

[28] Tony Blair and William Hague: Sell NHS data to fund medical advances. The Times. 2024. Available from: https://www.thetimes.co.uk/article/tony-blair-and-william-hague-sell-nhs-data-to-fund-medical-advances-fz27bmb98

[29] Ahmad RW, Gani A, Hamid SHA, Shiraz M, Yousafzai A. A survey on mobile edge computing: The future of cloud computing. Journal of Network and Computer Applications. 2020;153:102682.

[30] Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences. 2015;305:357-83.

[31] Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information Sciences. 2017;460-461:198-213.

[32] Gentry C. Fully homomorphic encryption using ideal lattices. Proceedings of the 41st annual ACM symposium on Theory of computing. 2009;169-78.