10.48047/jocaaa.2024.33.02.33

Securing PHI in Cloud-Based Healthcare Systems: Challenges, Frameworks, and Future Directions

Ankit Srivastava
MS Analytics (Harrisburg University)
Email – ankit1985sri@gmail.com

Introduction

The adoption of cloud computing in the medical field has made way for a revolution in the management and processing of Protected Health Information. The technological capabilities offered by technology, such as the ability to be scalable, interoperable, and provide analytic solutions, has far-reaching implications in patient care and other related medical studies. However, there are numerous issues arising from the adoption and use of technology in ensuring the confidentiality, integrity, and available access to the PHI. The technology environment, unlike the on-premise system technology, has complex characteristics in terms of the type and technology it uses, and the properties and systems they entail, namely distributed, dynamic, and multi-tenant systems.

This paper aims to explore the issues concerning the security of PHI in the cloud, examine the frameworks and best practices available in the industry, and offer future directions concerning the ethics and viability of running health care in the cloud. Through an understanding of threats and risks in the management and implementation in the health industry, the innovative solutions presented in the form of federated learning, quantum-secure encryption, and transparency offered through the application use of the blockchain, the paper hopes to make people aware of the knowledge present concerning health care issues in the use of the cloud.

Abstract

In this paper, the issues involved in protecting PHI in the cloud environment in the health industry are discussed. Furthermore, the paper evaluates the types of cloud models in relation to protecting the confidentiality of PHI. The paper discusses the different types of cloud models, such as public, private, and hybrid models. Through the evaluation of various variables, including the levels of data encryption in the different models, the paper aims at developing important insights on the type of model that provides adequate protection.

Data Breach Risks in Multi-Tenant Cloud Environments

There has been significant integration of cloud computing capabilities within the healthcare industry, with transformative potential for effective data management, joint research, and improved patient care [1]. Nevertheless, the paradigm shift entails multidimensional risks, primarily stemming from stringent security & confidentiality requirements for the storage of Protected Health Information. By its very nature, the PHI calls for the implementation of advanced measures to prevent illegal access & breaches, and misuse, especially in the context of cloud storage networks [2]. Generally speaking, the storage of PHI within the local database poses risks due to the absence of effective cybersecurity & data protection measures, which expose the data to illegal attacks & lack scalability for larger volumes of data [3].

10.48047/jocaaa.2024.33.02.33

Due to the dynamic nature of cloud resource sharing, continuous monitoring and audits must be conducted to ensure that allocated resources comply with governing cloud security policies. Any violation or compromise of data confidentiality through the use of cloud resources could substantially erode public confidence in enterprises' businesses. To address the aforementioned issues with access control in the cloud EHR system, advanced access control concepts such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are needed [6]. Despite the importance of access control in cloud EHR solutions for securing data confidentiality by managing access according to prescribed roles and attributes, cloud-based EHR systems pose different challenges compared to traditional EHR solutions, which maintain confidentiality through standard methods [6].

Balancing Accessibility and Security in Cloud-Based Electronic Health Records (EHRs)

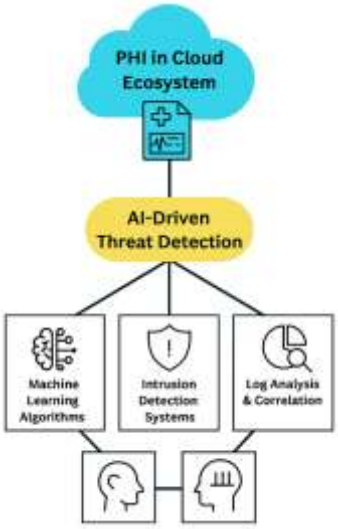
Cloud-based electronic health record systems often have vulnerabilities to breaches, such as hacking and data leaks, which in turn pose risks to the confidentiality, integrity, and availability of health data [7]. This calls for an integrated approach to securing PHR data in the cloud, addressing effective cryptographic methods and access controls [8] [9]. Thus, selecting effective encryption algorithms and key management processes is pivotal for the secure storage of PHI in the cloud [1]. This requires considering effective storage technologies for both symmetric and asymmetric encryption algorithms [10] [11]. Moreover, multi-tenancy, one of the inherent cloud characteristics, also introduces complexities due to the strict access controls required to prevent unauthorized access to data by other tenants who may also be using the same infrastructure [4].

Insider Threats and Human Error in Cloud Healthcare Systems

Despite the importance of technological measures for securing cloud-based systems in the healthcare industry, human error and malicious behavior by cloud system insiders also pose considerable risks to the confidentiality of protected health-related data. Thus, to ensure the safety of crucial medical data from cloud system threats, comprehensive staff training on cloud security measures is essential. Additionally, the aspect of secure access controls in cloud systems also poses considerable risks to the confidentiality of crucial medical data. Thus, implementing comprehensive access controls in cloud system infrastructure through the utilization of advanced identity-and-access-management solutions that employ multi-factor authentication is vital [12]. Furthermore, the implementation of advanced cloud system analytics and machine-learning solutions also offers considerable potential to improve cloud system access controls by enabling the detection of internal threats through pattern analysis of cloud system usage [13]. Finally, despite technological measures in place to ensure cloud system data confidentiality in the healthcare industry, the lack of transparency in cloud system data usage also poses considerable threats to the confidentiality of crucial medical data in cloud-based infrastructure [14]. Additionally, cloud system data usage also poses threats to the confidentiality of crucial medical data in cloud-based infrastructure. Thus, the importance of cloud system data usage policies that ensure the confidentiality of cloud system data is vital [14]. Thus, because of the various considerable risks posed by cloud-based system threats despite the implementation of advanced cloud system technological measures for the confidentiality of crucial medical data in the healthcare industry, the implementation of comprehensive cloud system measures for cloud system threats is imperative [15]

10.48047/jocaaa.2024.33.02.33

AI-Driven Threat Detection for PHI in Cloud Ecosystems



Applying concepts from artificial intelligence and machine learning presents interesting opportunities to improve automated detection capabilities for advanced cyber threats targeting Protected Health Information in cloud infrastructure. This also includes the ability to apply AI in real-time anomaly detection for various cloud infrastructures. Other aspects include the use of predictive analytics to protect against threats, leveraging the strengths inherent in intelligent automation for quick responses to various cyber threats [18] [19] [20]. Applying AI concepts would provide an interesting augmentation to conventional methods for detecting threats in cloud infrastructure by analysing subtle patterns, causal to insider threats or system-level vulnerabilities that might otherwise go unnoticed [21]. Additionally, the system necessitates the consistent application of ethical guidelines for cloud infrastructure.

Securing PHI data in the cloud

Securing Protected Health Information (PHI) in AWS and Snowflake cloud environments requires a layered approach that combines regulatory compliance, technical safeguards, and governance controls. In AWS, organizations should leverage native services such as AWS Key Management Service (KMS) for data-at-rest and data-in-transit encryption, Identity and Access Management (IAM) for fine-grained role-based access, and CloudTrail/Config for continuous monitoring and auditing of PHI-related activities. Snowflake complements this by providing end-to-end encryption, role-based access control (RBAC), and dynamic data masking to protect sensitive data while enabling analytics. Both platforms support HIPAA-eligible services, meaning PHI can be securely processed under a Business Associate Agreement (BAA). To strengthen privacy-preserving analytics, organizations should implement least-privilege access policies, enforce multi-factor authentication (MFA), and integrate data loss prevention (DLP) tools. Finally, continuous compliance monitoring, combined with frameworks like the NIST Cybersecurity Framework and Zero Trust Architecture, ensures PHI remains secure while enabling scalable healthcare research and reporting.

To protect Protected Health Information (PHI) in the AWS and Snowflake cloud infrastructures, one must ensure PHI confidentiality by utilizing PHI best practices. To protect PHI in AWS cloud

10.48047/jocaaa.2024.33.02.33

infrastructure, one must use AWS Key Management Service for data-at-rest and in-transit encryption. However, one must also use Identity & Access Management to implement strict role-based access controls in the AWS cloud infrastructure. To monitor the use of PHI in AWS cloud infrastructure, one must make use of AWS CloudTrail/Config. However, the use of PHI in the Snowflake cloud infrastructure ensures its confidentiality by utilizing end-to-end encryption. Nevertheless, the use of PHI in the Snowflake cloud infrastructure also ensures its confidentiality through the Role-Based Access Controls (RBAC) mechanism. To ensure the confidentiality of PHI across both cloud infrastructures, one must use the Data Masking mechanism. Finally, the use of PHI in cloud infrastructure for healthcare research enables HIPAA-eligible services.

When cloud outages happen, continuity in securing access to Protected Health Information (PHI) is achieved through specific cloud continuity strategies that aim for redundancy, compliance, and the ability to adapt to different scenarios. Cloud continuity strategies for the healthcare industry must use cloud architecture that supports multiple regions for replication and recovery, enabling automated failover to standby regions. Offline access solutions for PHI, such as cached copies within mobile and desktop apps, provide continuity during the outage. However, all of the aforementioned continuity solutions must work in conjunction with compliance-focused strategies in PHI cloud storage. These solutions involve HIPAA-compliant encryption, log generation for audits, and the enforcement of access controls to ensure that continuity processes during cloud outages remain secure.

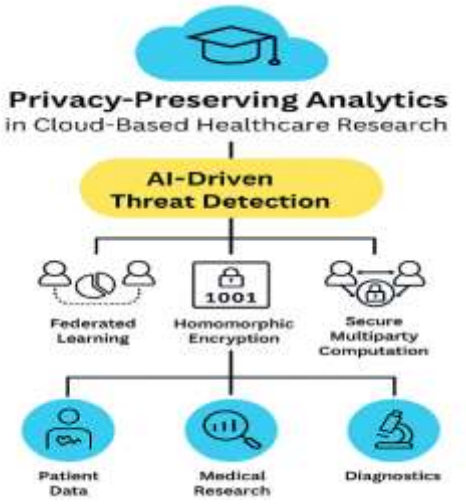
Privacy-Preserving Analytics in Cloud-Based Healthcare Research

- Federated Learning: Enables collaborative model training without sharing raw PHI.
- Data Anonymization: Removes identifiers to protect patient privacy.
- Differential Privacy: Adds statistical noise to prevent re-identification.
- Homomorphic Encryption: Allows computation on encrypted data without decryption.

The importance of privacy-preserving technologies, such as homomorphic encryption and federated learning, in cloud infrastructure cannot be underestimated for enabling the secure analysis of PHI while maintaining its confidentiality. Techniques such as homomorphic encryption enable computations on the data without prior decryption. This serves to protect PHI during the analysis process. Additionally, federated learning brings together multiple organizations to train a single model without requiring access to raw data.

Privacy-Preserving Analytics for IoT in Healthcare

10.48047/jocaaa.2024.33.02.33



At the center is the Healthcare IoT Cloud Platform, surrounded by four key privacy-preserving techniques:

Federated Learning: Keeps patient data on local devices while training shared models.

Differential Privacy: Adds statistical noise to prevent re-identification.

Homomorphic Encryption: Enables computation on encrypted data without decryption.

Secure Edge Computing: Processes data locally on IoT devices to reduce cloud exposure.

Firstly, IoT in the healthcare industry produces immense amounts of personal data. To maintain the confidentiality of sensitive data, effective methods for privacy-preserving analytics must be adopted. This ensures that real-time data from wearables and sensors is amenable to analysis in the cloud. Hence, the adoption of IoT in the industry promotes the field of personalized medicine. This becomes especially important in the wake of the growing use of AI and ML in industry.

Case study

A large U.S. healthcare organization, serving over 750,000 patients annually, initiated a migration of its Electronic Health Record (EHR) analytics workloads to AWS and Snowflake cloud platforms. The goal was to improve scalability, enable advanced analytics, and reduce infrastructure costs, while ensuring strict compliance with HIPAA and HITECH regulations.

Challenges

Multi-Tenant Risks: Shared cloud infrastructure raised concerns about PHI leakage between tenants.

Regulatory Compliance: Ensuring HIPAA/HITECH adherence across distributed cloud environments.

Access Control: Balancing clinician accessibility with strict security safeguards.

Incident Response: Preparing for outages or breaches in PHI systems.

Frameworks Adopted

10.48047/jocaaa.2024.33.02.33

The organization implemented a multi-layered security framework:

HIPAA Compliance Programs: Business Associate Agreements (BAAs) with AWS and Snowflake.

NIST Cybersecurity Framework: Identity management, encryption, and continuous monitoring controls.

Zero Trust Architecture: Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and least-privilege policies.

AI-Driven Threat Detection: Machine learning models to detect anomalies in PHI access patterns.

Implementation

Encryption: AWS KMS and Snowflake's native encryption secured PHI at rest and in transit.

Data Masking: Dynamic masking protected sensitive fields while enabling analytics.

Disaster Recovery: Multi-region replication ensured PHI availability during outages.

Audit Trails: AWS CloudTrail and Snowflake Access History provided compliance-ready logs.

Outcomes

Zero major breaches reported in the first 24 months post-migration.

Improved clinician accessibility via secure mobile and web portals.

Enhanced patient trust through transparent communication about PHI safeguards.

Scalable analytics enabled privacy-preserving research across multiple facilities.

Future Directions

The organization is now exploring:

Federated Learning: Collaborative research without centralizing PHI.

Quantum-Resistant Encryption: Preparing for next-generation cyber threats.

Edge Computing: Localized PHI processing to reduce exposure in centralized clouds.

Blockchain Transparency: Immutable audit trails for PHI usage and sharing.

Conclusion

This ability not only enables the secondary use of healthcare data for research & development but also reduces the risks posed by violations of data confidentiality in cloud infrastructure. Future work must explore the use of the aforementioned privacy-preserving methods in conjunction with advanced security orchestration & automated response solutions in order to build an adaptable defense mechanism against dynamic cyber threats. There is also a need for further research on the future equilibrium point for both attackers & defenders in the context of AI-powered cyberattacks to ensure sufficient safety against cyber threats. Finally, the combination of AI & the Blockchain could

10.48047/jocaaa.2024.33.02.33

provide an effective approach to keeping all data access & usage transparent in the cloud environment for the healthcare industry.

References

1. S. M. Gupta, “Cloud Security for Healthcare Services,” Journal of Management and Service Science (JMSS), vol. 3, no. 1, p. 1, Jan. 2023, doi: 10.54060/jmss.v3i1.41.
2. B. Guo, N. S. A. Shukor, and I. S. Ishak, “Enhancing healthcare services through cloud service: a systematic review,” International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering, vol. 14, no. 1. Institute of Advanced Engineering and Science (IAES), p. 1135, Nov. 14, 2023. doi: 10.11591/ijece.v14i1.pp1135-1146.
3. H. Taherdoost, “Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives,” Sci, vol. 5, no. 4, p. 41, Oct. 2023, doi: 10.3390/sci5040041.
4. A. Elgujja, “Impact of Information Technology on Patient Confidentiality Rights,” in Advances in medical technologies and clinical practice book series, IGI Global, 2019, p. 365. doi: 10.4018/978-1-7998-0047-7.ch018.
5. S. Bhutada, “Access Control for Multi-Tenancy in Cloud-Based Health Information Systems,” International Journal for Research in Applied Science and Engineering Technology, vol. 6, no. 4, p. 2647, Apr. 2018, doi: 10.22214/ijraset.2018.4443.
6. T. Kanwal, A. Anjum, and A. Khan, “Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities,” Cluster Computing, vol. 24, no. 1, p. 293, Apr. 2020, doi: 10.1007/s10586-020-03106-1.
7. O. C. Otieno and . H. T. L., “SECURITY AND PRIVACY DETERMINANTS FOR A SECURED CLOUD-BASED ELECTRONIC HEALTH RECORD SYSTEM,” International Journal of Engineering Applied Sciences and Technology, vol. 4, no. 3, p. 35, Jul. 2019, doi: 10.33564/ijeast.2019.v04i03.005.
8. R. Walid, K. P. Joshi, S. G. Choi, and D. Kim, “Cloud-based Encrypted EHR System with Semantically Rich Access Control and Searchable Encryption,” in 2021 IEEE International Conference on Big Data (Big Data), Dec. 2020, p. 4075. doi: 10.1109/bigdata50022.2020.9378002.
9. R. P. Puneeth and G. Parthasarathy, “Survey on Security and Interoperability of Electronic Health Record Sharing Using Blockchain Technology,” Acta Informatica Pragensia, vol. 12, no. 1, p. 160, Sep. 2022, doi: 10.18267/j.aip.187.
10. K. Gariépy-Saper and N. Decarie, “Privacy of electronic health records: a review of the literature,” Journal of the Canadian Health Libraries Association / Journal de l Association de bilbiothèques de la santé du Canada, vol. 42, no. 1. University of Alberta, Apr. 02, 2021. doi: 10.29173/jchla29496.

10.48047/jocaaa.2024.33.02.33

11. J. J. P. C. Rodrigues, I. de la T. Díez, G. Fernández, and M. López-Coronado, “Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems,” Journal of Medical Internet Research, vol. 15, no. 8, Aug. 2013, doi: 10.2196/jmir.2494.

12. B. Calabrese and M. Cannataro, “Cloud Computing in Healthcare and Biomedicine,” Scalable Computing Practice and Experience, vol. 16, no. 1, Feb. 2015, doi: 10.12694/scpe.v16i1.1057.

13. S. Thavamani and M. Rajakumar, “Privacy Preserving Healthcare Data using Cloud Computing,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, p. 118, Sep. 2019, doi: 10.35940/ijitee.j1022.08810s19.

14. I. Kumar, “A REVIEW OF PRIVACY AND SECURITY ISSUES IN HEALTHCARE SYSTEMS,” NeuroQuantology, vol. 20, no. 3. NeuroQuantology, May 07, 2023. doi: 10.48047/nq.2022.20.3.nq22961.

15. G. Dhanalakshmi and V. S. G. G, “Secure and Privacy-Preserving Storage of E-Healthcare Data in the Cloud: Advanced Data Integrity Measures and Privacy Assurance,” International Journal of Engineering Trends and Technology, vol. 71, no. 10, p. 238, Oct. 2023, doi: 10.14445/22315381/ijett-v71i10p222.

16. M. M. Moncy, S. Afreen, and S. Purkayastha, “Healthcare Security Breaches in the United States: Insights and their Socio-Technical Implications,” arXiv (Cornell University), Nov. 2023, doi: 10.48550/arxiv.2311.03664.

17. E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, “Security Challenges in Healthcare Cloud Computing: A Systematic Review,” Global Journal of Health Science, vol. 9, no. 3. Canadian Center of Science and Education, p. 157, Jul. 12, 2016. doi: 10.5539/gjhs.v9n3p157.

18. K. Singh, “Artificial Intelligence & Cloud in Healthcare: Analyzing Challenges and Solutions Within Regulatory Boundaries,” International Journal of Computer Science and Engineering, vol. 10, no. 9, p. 1, Sep. 2023, doi: 10.14445/23488387/ijcse-v10i9p101.

19. A. J. Samuel, “Cloud security architectures for AI-enabled healthcare diagnostics and personalized treatment plans,” World Journal of Advanced Engineering Technology and Sciences, vol. 11, no. 1, p. 467, Feb. 2024, doi: 10.30574/wjaets.2024.11.1.0036.

20. S. Pawar, “Securing Health Data in Mobile Cloud Computing by a Modular Encryption Approach,” International Journal for Research in Applied Science and Engineering Technology, vol. 11, no. 11, p. 1968, Nov. 2023, doi: 10.22214/ijraset.2023.56900.

21. F. K. Mupila, H. Gupta, and A. Bhardwaj, “Securing the Cloud: An In-depth Exploration of Conceptual Models, Emerging Trends, and Forward-looking Insights,” Research Square (Research Square), Oct. 2023, doi: 10.21203/rs.3.rs-3448528/v1.