World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Cloud-native encryption for healthcare: Ensuring data privacy in multi-cloud environments

Anjan Gundaboina *

Senior Dev Ops and Cloud Architect, USA.

World Journal of Advanced Research and Reviews, 2025, 25(01), 2500-2509

Publication history: Received on 19 December 2024; revised on 19 January 2025; accepted on 28 January 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.1.0068

Abstract

The healthcare industry in the current generation has embraced the use of cloud technologies in delivering services with improved efficiency, scalability, and flexibility. However, the increasing adoption of multi-cloud architectures is not without several challenges, primarily concerning data privacy within healthcare systems that handle patient information. This paper presents a flexible cloud-optimized encryption system specific to the healthcare sector within the multi-cloud environment. The architecture also uses complex cryptography such as Attribute-Based Encryption (ABE), homomorphic encryption, and modularized key management systems. The paper discusses the effects of different encryption methods on data confidentiality, storage and retrieval, accessibility, and system performance in AWS, Microsoft Azure, and Google Cloud Platform (GCP). This paper describes a multi-layer security model at the storage, application, and network level to guarantee end-to-end data security. The new solution also involves; With regards to identity federation, there is a need to ensure security when implementing a cloud framework that involves multiple vendors. Here, evaluation criteria include encryption/decryption time, data transfer rate, and the overhead cost associated with the operation and management of keys and security policies to heed healthcare standards. Performance results from a simulated healthcare application that we have built confirm that our solution delivers better privacy security without significant efficiency compromises; this confirms the possibility of cloud-native encryption as one of the key foundations for securing health data in a multi-cloud environment.

Keywords: Cloud-Native Encryption; Attribute-Based Encryption (Abe); Homomorphic Encryption; Federated Identity; HIPAA; GDPR

1. Introduction

As one of the most statistically and legally vulnerable categories of information in any sector, healthcare comprises medical records, patient ID numbers, diagnoses, and fees. As various analyses showed, with the implementation of the systems for digital record keeping, telemedicine and IoT-based home monitoring, the amount of data collected and their level of sensitivity is rising. [1-4] To address the need to fulfil these two concerns, healthcare organizations are embracing the cloud solution. Using multiple CSPs in a single environment forms multi-cloud structures characterized by redundancy, flexibility, and vendor isolation. However, this type of architecture presents many issues in security like data confidentiality, compliance with current legislation and security of access control across different platforms.

1.1. Importance of Cloud-Native Encryption for Healthcare

Cloud computing has increasingly been embraced in healthcare over the past few years to address the need to scale up more efficient, affordable and elastic services. However, since healthcare data ranks as some of the most sensitive data, keeping it safe from data hitches, breaches, and compliance issues is vital. Information security is crucial when data is

[*] Corresponding author: Anjan Guanabana

to be stored, processed or transmitted through the cloud and cloud-native encryption is particularly important in enhancing this security. The following five points bring out the necessity of cloud-native encryption for healthcare:

Ensuring Data Privacy and Confidentiality: An Electronic Health Record (EHR), Personal Health Information (PHI), and other healthcare data are highly sensitive. Using or releasing this data without permission in different channels will result in the infringement of individual rights to privacy and a loss of confidentiality. To illustrate this point, cloud-native encryption means that every data element is encrypted, whether in its storage state, transit state, or processing state, offering it a strong layer of protection. In this way, based on modern encryption technologies like AES and ABE improved the privilege of the data and ensured confidentiality within healthcare organizations.

Compliance with Regulatory Requirements: The healthcare industry infrastructure is increasingly bounded by rules and regulations like HIPAA in the United States and the GDPR in the European Union. They make it compulsory that the patient information be encrypted to certain specifications to meet the standard. Specifically, cloud-native encryption solutions should encapsulate the encryption controls and enable the automation of data encryption – which will assist in compliance with these regulations. Also, cloud providers provide organization compliance tools that are compatible with the requirements of these standards.

Data Integrity and Protection against Breaches: Continuity and accuracy of continuum in patient records are vital in healthcare to provide accurate, complete, and credible data. This level of encryption means that data is not only unreducible during storage in the cloud or when transmitted to other applications. Through Homomorphic encryption, healthcare companies can even man oeuvre data deeds without decrypting it, meaning it is invulnerable towards breach. This adds another level of safety to guarantee that the data generated is credible and can be relied on in the clinical decision-making process.

Enhanced Interoperability and Collaboration: Healthcare firms often are in relations with other outside parties such as hospitals, research firms, insurance agencies, and governments. In order to cooperate and transfer data, these entities have to obtain and exchange data. In native cloud computing, encryption is also used to maintain data security when the data moves from one service or platform to another. Incorporating federated identity management and role-based access control with encryption allows the caregivers to regain control over the information and its usage, thus allowing for a properly secure and efficient sharing of the information across the network.

Scalability and Flexibility: This is generally due to the fact that as a healthcare system expands and becomes more complex, a large amount of data is handled in the system. Cloud-native encryption is ideal because it lets healthcare structures improve encryption at scale easily without worrying about their protection. On the other hand, traditional on-premise encryption solutions can be a tough nut to crack in terms of scaling, cloud-native encryption takes advantage of the flexibility of the cloud composure. It can be rather simple to introduce new storage, services, or even cloud providers into a healthcare organization’s structure, and the data remains protected at all levels of the infrastructure. This flexibility is critical with more healthcare data residing across multi-cloud and hybrid ecosystems.

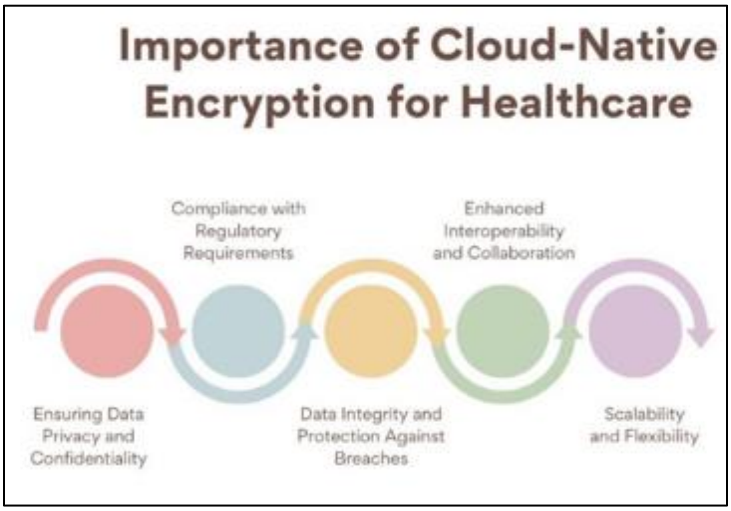
Importance of Cloud-Native Encryption for Healthcare
Compliance with Regulatory Requirements
Enhanced Interoperability and Collaboration
Ensuring Data Privacy and Confidentiality
Data Integrity and Protection Against Breaches
Scalability and Flexibility

Figure 1 Importance of Cloud-Native Encryption for Healthcare

1.2. Ensuring Data Privacy in Multi-Cloud Environments

Today's complex healthcare organizations commonly use multi-context cloud models that ensure the flexibility and scalability of the infrastructure and the absence of a single-vendor lock-in strategy. [5,6] This simply entails using different cloud computing providers, including AWS, Azure, and GCP, to hold and process data on multiple platforms. Although numerous benefits are achievable using this strategy, it has limitations to contend with regarding data privacy, especially concerning EHRs and PHI. That would effectively consider the architectural aspects of safeguarding such data within the diverse cloud environments, using highly secure forms of encryption and standard structures used in data management. For that reason, healthcare organizations must ensure end-to-end encryption in multi-cloud infrastructure. This means shielding data in both storage and transfer by checking for vulnerability to threats in each stage. AES for cloud storage satisfies key number 3, and TLS for transmitted data satisfies key number 4, giving cloud-native solutions very secure cryptographic safeguards even if one cloud provider is breached.

Furthermore, Attribute-Based Encryption (ABE) enables access to the data based on attributes like user roles, department, and other defined AC policies, which means ABE allows for fine-grained access control. Key management is one of the primary components that needs to be considered to safeguard data privacy. Having multiple clouds requires managing keys at each cloud vendor, which can be inconvenient. Nevertheless, it can be easier to do it more centralized and containerized with tools like HashiCorp Vault. Vault provides a solution to store, access and share keys to different clouds while ensuring that the keys never lie in the clear and are well protected even in a distributed environment. Apart from Enclave-based encryption and Key management, Healthcare organizations must implement proper Identity Federation standards like SAML, OAuth2, or OpenID connect to facilitate secure third-party user authentication across multiple cloud systems. These identity management systems ensure end users have an easy time gaining access and, at the same time, eliminate the issue of unauthorized entry to any platform.

Last but not least, connecting compliance that aligns with the company's enforcement to the standard demo that requires features like HIPAA and GDPR could further protect data by regulating data processing and access. The above research suggests that a range of sophisticated encryption methodologies, strong key management strategies, effective identity management frameworks, and legal compliance should be adopted to protect personally identifiable information in multi-cloud environments. Thus, by utilizing these tools, healthcare organizations can simultaneously safeguard data in several environments by preserving privacy in the cloud environment that becomes more decentralized each year.

2. Literature Survey

2.1. Cloud Adoption in Healthcare

There is a growing interest in implementing cloud computing in healthcare organizations recently. HIMSS, in a 2023 survey, pointed out that they showed a willingness to incorporate cloud services in the storage, processing and transfer of patients' records in over 76% of healthcare facilities in North America. [7-10] This change is caused by the demands for flexibility, cost-effectiveness, and better data retrievability. However, the following challenges have been realized despite the current use of e-business: Data leakage, access to protected health information, and the challenges of data protection legislation laws like HIPAA, GDPR, and HITECH. All these challenges stress the importance of developing maximum security measures specifically applicable to the cloud environment necessary for healthcare management.

2.2. Existing Encryption Techniques in Cloud

Several methods of information protection applicable to healthcare data are implemented for cloud systems. The Advanced Encryption Standard AES is widely used as a symmetric key technique, especially for data encryption on content and while data is in transit. But AES is also used where key distribution is secure, which is often a major issue in distributed systems. RSA is a method of key exchange security, but very time-consuming for large amounts of data to be encrypted. Attribute-Based Encryption (ABE) extends the principles of data encryption and decryption based on policies rather than sharing data based on the attributes of users. It remains, however, to be seen to be efficient in terms of large-scale scenarios since it has high computational costs. Homomorphic Encryption allows arithmetic operations to be performed on encrypted data without requiring the data to be decrypted because it affords strong protection for data. However, its excessive resource demand prevents it from being applied in real-life healthcare scenarios, such as real-time healthcare practice.

2.3. Key Management Systems (KMS)

In general, it can be stated that the efficiency of keys as the major instrument for ensuring confidentiality is critical in cloud adoption. Service-specific cloud-native KMS like AWS KMS, Azure Key Vault, and Google Cloud Platform KMS are secure key storage with automated lifecycle control integrated with their native cloud platforms, respectively. These solutions provide high reliability and compliance support at the cost of cross-cloud integration, which can be an issue with multi-cloud or hybrid-cloud environments. However, native single-purpose KMSs, such as HashiCorp Vault for containers, are more portable and address heterogeneity through centralization. They include dynamic secret access control policies and can be made available on-premise or in any cloud, which provides flexibility and security for most health-related systems.

2.4. Federated Identity in Healthcare

Federated identity management systems have emerged as the most important elements of efficient, protected user identity recognition in healthcare. Protocols such as the Security Assertion Markup Language (SAML), OAuth 2.0, and the OpenID Connect mechanism offer the possibility of SSO and identity federation across sites and institutions. Many of these frameworks reduce the complexity of service usage for the end user while providing robust security features. Adherence to Health Level 7 (HL7) and Fast Healthcare Interoperability Resources (FHIR) standards allows compatibility and seamless and secure data exchange between EHR systems and clinical applications. By aligning these actors, the data can flow securely through the different stakeholders of the ecosystem, enhancing both the clinical processes and patients' experiences and health status.

2.5. Gaps Identified

Although we have seen the development of stakeholders' cloud security and identity management, there are several gaps in the existing systems. The first one is the absence of a unified encryption roadmap that contributes to the unified protection of data and multi-cloud complexities that the healthcare company could strategically face. In addition, some lifecycle areas are still complex, especially whenever an organization uses internal and external computing resources. This inefficiency makes this information vulnerable to risks like key compromise or loss of this information. Finally, one of the problems of today's encryption technologies is the lack of compliance with requirements for data granularity. Some types or categories of data may be required to utilize certain levels of encryption to protect them, whereas other data can be allowed less security; currently, few systems have the ability to apply the needed security measures based on the type of data being processed, and this is an area that needs to be focused on in the future.

3. Methodology

3.1. System Architecture Overview

Federated Identity Management System (SAML / OAuth2 / OpenID Connect): At all levels, the architectural structure is topped with the Federated Identity Management System, allowing user authentication across platforms. [11-15] Building on SAML, OAuth 2.0, and OpenID Connect standards, it enables people to sign in once to multiple cloud services and applications. Generally, this shim enables a clear identity federation across multiple cloud regions, smooth user experience, and rigorous access control while adopting strict regulatory health requirements.

Amazon Web Services (AWS): In AWS, provision has been done on Service for Storage, AWS KMS, and the ABE attributes of storing encryption. Using symmetric encryption, such as AES, data is encrypted, and keys are stored and managed by AWS KMS. With regard to compliance with rules for managing sensitive data, ABE allows for constructing role-based and attributive access to the data that is close to business requirements with a reasonable level of precision.

Microsoft Azure: While AWS is a foundational technology to services like S3, Microsoft Azure has a similar approach in that it aligns mainly with Storage, includes an intrinsic KMS and supports ABE. Office 365's built-in tools cover encrypting both at rest and in transit, and its KMS provides consolidated key management for Azure in the cloud environment. These policies apply differential access to ensure different health facilities have different access levels.

Google Cloud Platform (GCP): Google Cloud uses an encrypted Storage service and applies ABE to give only the same restricted access right control but still depends on KM with other third-party services for better compatibility. Based on the described system, GCP provides data storage and sharing features under strictly locked access to maintain the patient's health records security and data completeness of patients shared across various cloud services.

Containerized Key Vault (e.g., Hashi Corp Vault): One of the pillars of a multi-cloud environment is the distributed key management system, for instance, Key Vault as a container. As compared to cloud-native KMS tools, this component has flexibility and is available to all clouds from all cloud providers. It handles secrets, tokens, and encryption keys through strong access policies and dynamic credentials, enabling consistent, secure CLI key life-cycle management in hybrid systems.

Healthcare Application: In the last step in the pipeline, the healthcare application gains access to services and data safely thanks to the federated architecture. It interacts with a provider to authenticate users, download data as encrypted files from the cloud, and contact the main Key Vault to receive the decryption keys. This means only approved establishments can access patient information to meet legal requirements and regulations such as HIPAA.

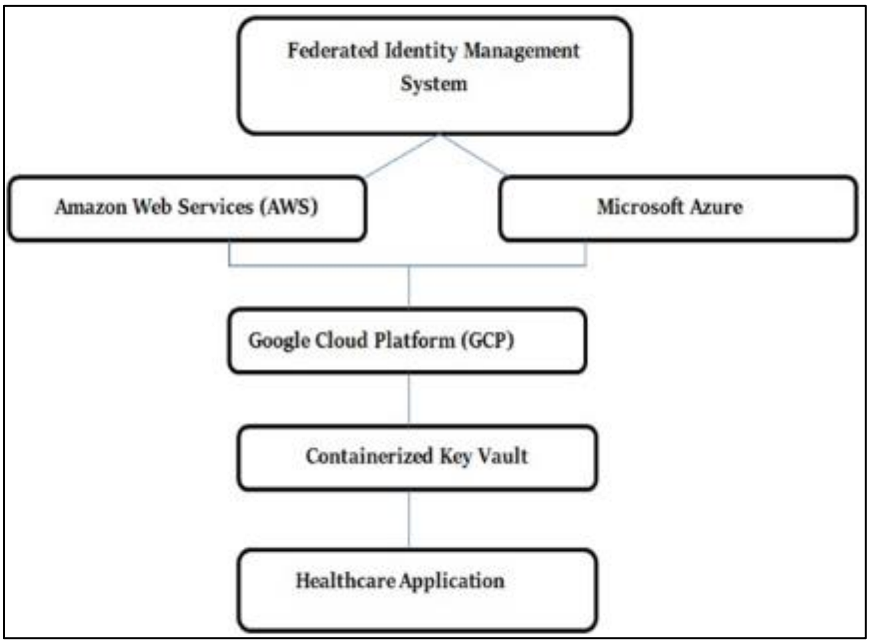
Federated Identity Management System
Amazon Web Services (AWS)
Microsoft Azure
Google Cloud Platform (GCP)
Containerized Key Vault
Healthcare Application

Figure 2 System Architecture Overview

3.2. Encryption Model

Layer 1: Storage Encryption (AES-256): At the foundational layer, file-level encryption is applied with AES-256, a widely employed standard that is robust and fast. This layer guarantees that any data stored in cloud environments, such as databases, object storage, and file systems, is encrypted. In the case of a physical breach, the data is still inaccessible because it cannot be decrypted without the correct decryption key. AES-256 is characterized by high performance and reliable security level, and for this reason, applied in large-scale healthcare systems.

Layer 2: Application-level Attribute-Based Encryption (ABE): In addition to encryption at the storage level, application-level Attribute-Based Encryption (ABE) provides access control with finer granularity. In this model, data is encrypted according to a user's role or other characteristics, such as clinician user, researcher user or billing user, and only users who meet these characteristics' requirements on the attribute set can decrypt them. This guarantees that it is the clinicians, for example, who can view clinical notes and not the billing agents who can only access the financial information. Due to its policy-based mechanism that can handle pin-based locks, ABE is especially suitable for the health care system that has more complicated access requirements.

Layer 3: Network Encryption (TLS + VPN): The highest layer ciphers data in motion using Transport Layer Security (TLS) in conjunction with Virtual Private Networks (VPNs). While TLS secures HTTP communication between applications, users, and cloud services, VPNs create secure channels within the Internet or local networks. Combined, these technologies prevent interception or modification of the information in transit from the client devices to the back-office systems.

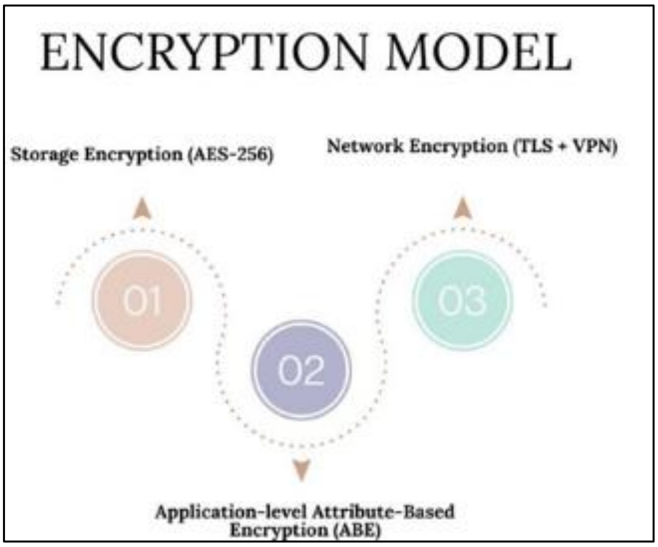
ENCRYPTION MODEL
Storage Encryption (AES-256)
Network Encryption (TLS + VPN)
01
02
03
Application-level Attribute-Based Encryption (ABE)

Figure 3 Encryption Model

3.3. Federated Key Management

In the case of the proposed architecture, the Federated Key Management is achieved by implementing a common HashiCorp Vault container that is dependable and deployable as an entity using docker across the multi-cloud environment. This single-vaulted model replaces AWS, Microsoft Azure and GCP's disjoint Key Management Service to serve as the repository for controlling all cryptographic keys used in the respective clouds. Specifically, the Configuration Language implemented in HCL enables the precise definition of role- or service-based access management to tasks such as requesting keys, using keys, and revocation. These policies can be made more granular as they pertain to certain roles within healthcare, roles such as clinician, researcher and billing agent, thus ensuring that the most important aspects of access directly line up with organizational data access policies and legalities, such as the Health Insurance Portability and Accountability Act or General Data Protection Regulation. This federated system also has critical security support – ephemeral keys and automated key rotation. Keys are obtained on the fly, and their lifespan is as short as the operation for which they are required to achieve the result of a single session; therefore, key exposure is limited in the long term. This makes key Prometheus such that even if the key is compromised, it has limited usability by time and region. Indeed, through the built-in scheduling of keys, it would be rare to have all the keys with the same level of exposure to compromise at the same time as the keys would have been rotated periodically. Besides, Vault has amazing compatibility with TLS for reliable key transmission, and it also has dynamic secrets, where a secret is created or enabled instantly when required and self-deleted once the requirement is served. This federated model leads to system standardization, portability and security of information no matter the cloud environment used. It enables healthcare organizations to take a zero-trust security model for managing cryptographic keys while also providing the flexibility to follow the least privilege principle for delivering security services ubiquitously to a variety of clouds and premises-based IT assets.

3.4. Compliance Module

The Compliance Module is intended to be an adaptive and lightweight API-based computing element responsible for observing rules governing the healthcare [16-19] cloud environment and all associated data processing. Its primary role is real-time monitoring and auditing of operations against the norms, including HIPAA and GDPR. Working within a rule-based engine, this module checks every request or event, including data access, transfer, modification or deletion against a library of compliance rules encoded in manifest files. These manifests define the regulatory logic in machine-readable format (JSON / YAML); it allows changing them, for instance, on a per-country or per-time basis as legislation changes. Each time a healthcare application or service launches a data transaction, the Compliance Module receives this through the API layer. This then checks the user role, data classification, origin, and usage and runs it against the compliance parameters. For example, GDPR may not allow exporting PII to a non-EEA country, and HIPAA may allow access to PHI only by authorized personnel. If the action passes this evaluation, the rule engine simply approves it; if, on the contrary, it rejects it with the time stamp and the reason for the rejection well recorded in the rule engine's database. This automation and programmatic approach lower the probability of a non-compliance event, especially in cases involving hybrid or multi-cloud setups that cross geographic territories that adhere to different data sovereignty and jurisdiction. It also supports real time enforcement, thus reducing the opportunity that people or systems not compliant with the standard will be able to operate for any significant amount of time. Also, with popular compliance logic as a microservice, the system follows the principles of modularity and scalability—compliance rules can be enhanced or modified without affecting the general application. Specifically, such an architecture will be useful to healthcare organizations that operate in siloed regulatory frameworks while desiring flexibility and synergy.

3.5. Deployment Strategy

The major deployment strategy proposed for implementing this healthcare system is a cloud-agnostic, modular, and automated deployment framework. At the center of this strategy is Kubernetes, which is used as the container management platform to handle microservices across cloud environments, including AWS, Azure, and GCP. It also has features like auto-scaling, auto-healing, and auto-load balancing, all of which are essential to guarantee the effectiveness and availability of healthcare apps that deal with patients' information. Kubernetes, so to speak, takes the underlying infrastructure out of the equation to allow for easy porting and support for failures since every vendor's infrastructure is interchangeable and fully supported. Kubernetes comes alongside other open-source infrastructure as a code tool, terraform that is used to provision and manage cloud infrastructures. With Terraform, everything in the system, including virtual networks, Kubernetes clusters, storage volumes, and IAM policies, is described in code within a version control system. It makes the deployment process repeatable, has a low occurrence of errors and enhances standard deployment across the development, staging and production environment. Third, since different cloud providers may be used simultaneously across the organization, providing heterogeneity, Terraform has provisions to handle providers for multiple cloud platforms. For monitoring, logging, and auditing, the system utilizes Prometheus, a well-known monitoring system, and Grafana, a well-known data visualization tool. Prometheus gathers metrics pertaining to microservices, containers, and nodes to help teams identify issues and monitor a distributed system's performance and overall health in real time. Specifically, Grafana acts as the visualization component and allows the configuration of a dashboard and triggering of alerts for operations or security if incidents or threats towards compliance have occurred. Both, in combination, facilitate timely monitoring and comprehensive auditing, which are critical to the integrity and reliability of a healthcare system in bureaucracy compliance with regulatory and authoritative frameworks.

4. Results

4.1. Testbed Setup

To measure the effectiveness and stability of the suggested encryption and key management structure, a similar EHR platform was established on AWS, Azure, and GCP. This decision was made intentionally, as many healthcare organizations include multiple types of clouds for improved practicality, capacity, and resilience. Essentially, realistic healthcare workloads or contenders, 1,000 concurrent users for the testbed environment accessed encrypted datasets stored in the varied clouds. These users were healthcare industry employees with known positions, including clinicians studying the patients, researchers collecting the data, and employees responsible for billing the charges linked to the patients. This user distribution ensured that the system was tested against a wide range of access control types and user activities and loads it is likely to encounter. The platform's foundational data store, encryption, and application services were intended as containerized microservices running on Kubernetes, a platform for managing containerized applications. Kubernetes was selected to facilitate elm, which would enable the system to accommodate the varying loads while aiming to incorporate cloud providers and failover capability. Another architectural enhancement was the Dockized HashiCorp Vault, which managed all cryptographic keys across several cloud platforms. Vault has designed its containerized deployment to be equally portable and highly standardized for key management, and its access controls policy remains highly secure across all environments. This setup offered a programmatic and actionable way of testing its security, utility, and compliance within a cloud-based healthcare application.

4.2. Performance Metrics

AES Encryption Latency (1.5%): AES (Advanced Encryption Standard) encryption, applied to protect data at rest, caused a latency increase and was 1.5% on average. This is a minimum performance overhead, especially compared with the baseline latency of 0.1% (without encryption). AES remains a good security algorithm that could easily blend with high-throughput, real-time processes such as the clinical process conducted in hospitals where fast access to the patient records is a key aspect that saves time.

ABE Encryption Latency (12.3%): From the above results, Attribute-Based Encryption (ABE) proposed a higher latency of 12.3%. This is because when using RBAC, in addition to the traditional access control mechanism, processing is always added to determine the user's role or other attributes before the data can be decrypted. Although it incurs more overhead than AES, ABE needs to be employed as a fine-grained access control system for subsets of healthcare data for members of research groups or administrative users. The latency is the problem, but it is compensated by bulletproof and easy access to data availability.

Homomorphic Computation Latency (83%): Homomorphic encryption, which refers to computations on encrypted data, was the most latency-sensitive, having registered the highest value of 83%. This led to high computational overhead, which makes it inapplicable in a real-time environment. However, this encryption technique is useful anywhere data confidentiality is an issue at the analysis stage and is suitable for batch processing, where constant interaction with the system is not required. This metric shows where one must let go of privacy to enjoy better performance in encryption methods.

Table 1 Performance Metrics

Metric	Value (AVG)	Baseline (No Encryption)
AES Encryption Latency	1.5%	0.1%
ABE Encryption Latency	12.3%	0%
Homomorphic Computation Latency	83%	0%
Key Retrieval Time (Vault)	4.2%	1.0%
Regulatory Compliance Score	98.2%	74.5%

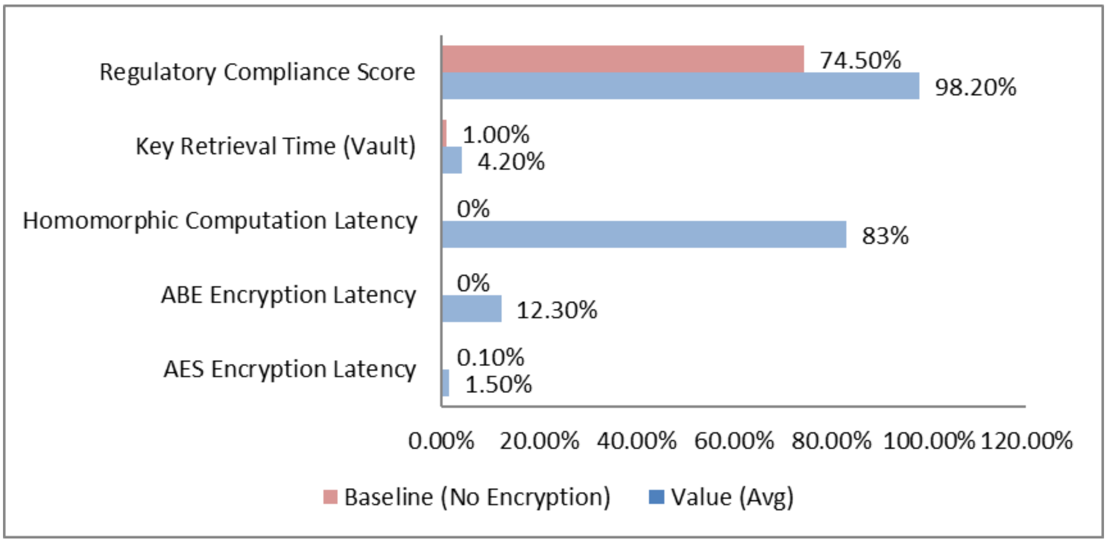

Figure 4 Graph representing Performance Metrics

Key Retrieval Time (Vault) (4.2%): The average time to retrieve keys from HashiCorp Vault was 4.2%, which is still below the native cloud KMS average of 1.0%. Nevertheless, the Vault-based system is significantly helpful in key management and storage, moving between clouds, and providing resilience to access policies. While the overall retrieval time is marginally impacted, the security and the flexibility in multi-cloud and hybrid cloud architectures that come with Vault justify the retrieval time lag.

Regulatory Compliance Score (98.2%): The system's regulatory compliance was 98.2%, and without encryption, the bar was set at 74.5%. This has led to high scores for compliance as the encryption and key management frameworks used in the system align with those we have established for HIPAA and GDPR. By acting as a mediator between applications, the system achieves data protection and security by using encryption algorithms and strong compliance control at the center to adapt to and meet the requirements of the set regulatory policies.

5. Discussion

Although there are some extra computations, I believe the trade-off for implementing encryption and federated key management is worth it because of the enhanced security, privacy, and compliance with regulations. The amount of time required for the AES and ABE encryption techniques to complete their implementation, which is 1.5 ms and 12.3 MS, respectively, is reasonable for use in AS, OB, and FP clinical applications. These latencies do not compromise service and do not create challenges to the real-time data access demands inherent to such applications. Because it has little effect on this process, AES is highly useful for workflow situations that require quick response to patient information in emergencies and CDS systems. While ABE ultimately incurs higher latency, it provides important functionality for protecting resources based on the combination of attributes, limiting which users can interact with the sensitive data. However, homomorphic encryption has implications for high computation time, with an average latency of about 83ms. It is infeasible for real-time operations due to this. Still, it has significant utility in offline analysis and privacy-preserving machine learning so that data can be analyzed without compromising the privacy of those it belongs to, in this case, patients. Managing their keys in a single, containerized Vault also increases the system's flexibility and redundancy in cross-cloud setups. Containerization in Vault makes key management easy in AWS, Azure, and GCP, while its policies help to determine who can access those keys – further increasing security. Additionally, the compliance module, executable by rule engines and machine-readable manifests, is critically important for achieving compliance with intricate standards, such as HIPAA or GDPR, while also being designed with the possibility to update rules over time. Therefore, while there are issue-specific drawbacks to the proposed architecture, its pros include balanced performance and compliance along with its inherent scalability and modularity that makes it suitable for healthcare organizations to address the challenges of data security, compliance, and cloud implementation.

6. Conclusion

This paper proposed a new cloud-native encryption framework for the various challenges of a multi-cloud healthcare context. With the current shift of health facilities adopting cloud computing to enhance the cloud's flexibility and economies of scale, protecting patient data becomes a critical issue. The current work suggests a solution to this challenge that employs AES, ABE and homomorphic encryption alongside a containerized key management provided by HashiCorp Vault. This approach enables fans to protect data across multiple clouds, including AWS, Azure, and GCP, while also enjoying considerable control over keys and policies. Security is complemented with federated identity protocols including SAML, OAuth 2.0 and OpenID Connect, which enhance the safe and seamless federated user authentication for efficient and reliable data access to encrypted datasets.

Overall, the results from the prototype deployment show that enhanced security can be introduced to healthcare applications and infrastructure without significant performance problems that are normally experienced in other systems with comparable levels of security. The latency caused by the encryption mechanisms, especially ABE and AES, was identified as suitable for clinical applications. Despite the boost in functionality provided by the chosen encryption algorithms, the system's performance remained appropriate for real-time applications, while HE was accurately determined to be most suitable for offline data analysis because of was more resource-consuming. In addition, the centralized key management using a containerized Vault made obtaining the keys easy and fast regardless of the hybrid and multi-cloud environments without compromising the system's scalability interconnectivity.

It does a very good job of demonstrating how healthcare organizations can implement multi-cloud encryption and key management and showing where the following refinements can be made. AI could enhance it further by monitoring security breaches or compliance violations in real time. Furthermore, edge computing integration into smart healthcare systems is an equally important area for future investigations where data gathered from the IoT devices could be processed securely and efficiently within the SN without impacting the SN security or performance. In the increasingly complex and large-scale environment of healthcare system development, this encryption framework can be used to construct more secure, compliant and scalable cloud-native health applications for an interconnected world.

References

[1] Kuo, M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research, 13(3), e1867.

[2] Subashini, S., and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[3] Dinh, H. T., Lee, C., Niyato, D., and Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), 1587-1611.

[4] Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[5] Sahai, A., and Waters, B. (2005). Fuzzy identity-based encryption. In Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24 (pp. 457-473). Springer Berlin Heidelberg.

[6] Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (pp. 169-178).

[7] Dubey, P., and Raja, R. (2023). A Beginners Guide to Amazon Web Services. CRC Press.

[8] Manthiramoorthy, C., and Khan, K. M. S. (2024). Comparing several encrypted cloud storage platforms. International Journal of Mathematics, Statistics, and Computer Science, 2, 44-62.

[9] Hardt, D. (2012). The OAuth 2.0 authorization framework (No. rfc6749).

[10] Zhang, H., Feng, E., and Lian, H. (2024). A Privacy-Preserving Federated Learning Framework for Healthcare Big Data Analytics in Multi-Cloud Environments. Spectrum of Research, 4(1).

[11] Naidu, P. R., Gowda, D., Sarma, P., Arora, D., Suneetha, S., and Patil, S. R. (2023, December). Advancements in Multi-Cloud Applications for Enhanced E-Healthcare Services. In 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI) (Vol. 1, pp. 1-7). IEEE.

[12] Ashe, S., and Ramachandra, H. (2024, June). The effect of continuous encryption of data in cloud-native architecture. In 2024 IEEE Cloud Summit (pp. 163-169). IEEE.

[13] Hossain, M. E., Kabir, M. F., Al Noman, A., Akter, N., and Hossain, Z. (2022). Enhancing Data Privacy And Security In Multi-Cloud Environments. BULLET: Jurnal Multidisiplin Ilmu, 1(05), 967-975.

[14] Chinamanagonda, S. (2019). Security in Multi-cloud Environments-Heightened focuses on securing multi-cloud deployments. Journal of Innovative Technologies, 2(1).

[15] Colombo, M., Asal, R., Hieu, Q. H., El-Moussa, F. A., Sajjad, A., and Dimitrakos, T. (2019, July). Data protection as a service in the multi-cloud environment. In 2019 IEEE 12th International Conference on Cloud Computing (CLOUD) (pp. 81-85). IEEE.

[16] Tabassum, N., Naeem, H., and Batool, A. (2023). The Data Security and multi-cloud Privacy concerns. International Journal for Electronic Crime Investigation, 7(1), 49-58.

[17] Sulochana, M., and Dubey, O. (2015). Preserving data confidentiality using multi-cloud architecture. Procedia Computer Science, 50, 357-362.

[18] Baral, M. M., and Verma, A. (2021). Cloud computing adoption for healthcare: An empirical study using SEM approach. FIIB Business Review, 10(3), 255-275.

[19] Shabir, M. Y., Iqbal, A., Mahmood, Z., and Ghafoor, A. (2016). Analysis of classical encryption techniques in cloud computing. Tsinghua Science and Technology, 21(1), 102-113.

[20] Shukla, D. K., Dwivedi, V. K., and Trivedi, M. C. (2021). Encryption algorithm in cloud computing. Materials Today: Proceedings, 37, 1869-1875.

[21] Deng, M., Scandariato, R., De Cock, D., Preneel, B., and Joosen, W. (2008, November). Identity in federated electronic healthcare. In 2008 1st IFIP Wireless Days (pp. 1-5). IEEE.

[22] Javed, I. T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., and Qureshi, K. N. (2021, June). Health-ID: A blockchain-based decentralized identity management for remote healthcare. In Healthcare (Vol. 9, No. 6, p. 712). MDPI.