INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 16, Issue 5, (2026) E-ISSN: 2222-6990

Encryption Performance and Resilience in Privacy Preserving Cloud Data Processing

Qing Guan[1,2], Mobd Nurul Hafiz Ibrahim[3]

[1,3]FOIT, City University, Malaysia, [2]FOIT, Gan nan University of Science and Technology, China

Email: guanqing29@gmail.com

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v16-i5/28313

Published Date: 16 May 2026

Abstract

Cloud computing has become the backbone of digital infrastructure, but protecting sensitive data while enabling efficient processing remains a major challenge. This paper benchmarks advanced encryption techniques—AES-256, RSA-2048, Homomorphic Encryption, Format-Preserving Encryption (FPE), and ChaCha20—across structured, semi-structured, and unstructured healthcare datasets in cloud environments. Using MIMIC-IV data and simulated attack scenarios, we evaluate encryption performance (speed, CPU/memory use) and resilience (brute force, side-channel, and MITM resistance). Results show AES-256 offers high throughput with low resource cost, RSA-2048 ensures secure key exchange, Homomorphic Encryption provides strong privacy at high computational expense, and FPE maintains legacy compatibility. ChaCha20 delivers both speed and consistency, making it a lightweight option. While compliance frameworks such as GDPR, HIPAA, and CCPA motivate the adoption of strong encryption, our findings confirm that no single method satisfies all cloud requirements. A hybrid, use-case-specific encryption strategy is essential for privacy-preserving healthcare cloud adoption.

Keywords: Cloud Security, Homomorphic Encryption, GDPR Compliance, Healthcare Data, Privacy-Preserving Architecture

Introduction

Background

Cloud computing has radically changed the way companies store, process, and manage data making it more scalable, flexible and cost-effective (Javaid et al., 2022). The problem is, as business data processing in the cloud has become so common that privacy concerns are on the rise. Moreover, as external servers start to process sensitive data such as personal or financial information, health records, etc., the associated risk also grows: in these conditions carried data breaches and unauthorized access brick by brick ruin compliance walls. Herewith the necessity of privacy-preserving architectures for cloud data processing activities became one of the vital concerns for researchers, developers and regulatory bodies.

In cloud data processing privacy-preserving architectures, an example is encryption. It works through encryption i.e by transforming valuable data into a coded language then it will be readable to those people who have the key or code to decrypt that encoded language. Cloud systems also utilize advanced encryption techniques that process the data in encrypted form using homomorphic and multi-party computation encryption, which prevent unauthorized access to user information even when data is being processed (Qureshi et al., 2022). Specifically, homomorphic encryption allows for computations on encrypted data — meaning it secures user privacy across the entire data lifecycle. This method is advantageous because it removes the necessity of data exposure to cloud service providers in which the owner of the data cannot be entirely trusted. In addition, you can use encryption along with methods such as tokenization and data masking that ensure that sensitive data is substituted with surrogate values or abstracted in manners which retain its referential integrity while restricting its utility.

Motivation and Problem Statement

The research literature often depicts encryption as a solution distinct from other security controls with emphasis on its ability to thwart access control and data breach related problems. But this ignores that encryption by itself is not sufficient to comply with all the wide-ranging legal obligations imposed around privacy, retention, access control and audit. While encryption techniques are a key element to keep data safe, compliance mechanisms play an equally important role in proving that enterprises comply with regulatory stipulations (Mohammad, 2022). This is especially critical in a multicloud, international environment where data moves between jurisdictions hosted by different cloud service providers who have their own practices and standards. And without a holistic solution that lays compliance on top of cutting-edge data encryption, firms either fulfil the threat protection or are still found wanting when it comes to privacy regulations. This missing component to the link in the chain a privacy-preserving, advanced-encryption-based security architecture combined with strategies for addressing compliance will require new approaches to both architectures and means of ensuring that data is always secure and protected from legal exposure throughout its life.

This motivates our research to bridge this gap and offer a comprehensive methodology for secure data management in cloud environment (Alghamdi et al., 2021). This paper is an attempt to investigate the well-understood intersection in between encryption and compliance and provide guidance for a stronger and legally-enforced cloud data processing architecture.

Objectives and Contributions

The main objective of this paper is to develop a privacy-preserving cloud architecture that integrates advanced encryption techniques with compliance mechanisms such as GDPR and HIPAA. It contributes by proposing a hybrid framework combining Homomorphic Encryption and Multi-Party Computation with automated auditing and access control, ensuring data security, legal compliance, and efficient cloud performance.

Literature Review

Overview of Cloud Security Mechanisms

Cloud computing has revolutionized the approach of organizations towards the storage, processing, and management of data but it also bring enormous challenges for the data security and privacy (Latifian, 2022). Over the years, numerous security measures were innovated to counteract the risks accompanying the utilization of cloud environments. Of those, encryption and compliance are two major pillars to secure sensitive information. For the most part, cloud security mechanisms can be broadly categorized into mechanisms that provide data confidentiality, integrity and availability thereby addressing the threats (data loss, unauthorized access, data breach, service disruptions etc.) to the data. Encryption in this case becomes a fundamental technology for data security at rest and in transit, complemented by compliance mechanisms that keep the organizations of businesses operating within the boundaries set by legal and regulatory frameworks, all meant to safeguard an individual's privacy while preserving data management integrity (Joseph, 2023).

Table 1

Cloud Security Mechanism

Cloud Security Mechanism	Description	Strengths	Weaknesses
Encryption	Transforms data into an unreadable format accessible only by authorized users, using methods like symmetric and asymmetric encryption.	Ensures data confidentiality; protects data at rest and in transit.	Vulnerable to decryption if weak keys are used; requires key management.
Advanced Encryption (Homomorphic & MPC)	Homomorphic encryption allows data processing without decryption; Multi-Party Computation (MPC) enables secure computation across multiple parties.	Provides strong privacy for sensitive data in multi-tenant environments.	High computational cost and complexity; still emerging in cloud implementation.
Compliance Mechanisms	Ensures data management adheres to regulations like GDPR, HIPAA, and CCPA, addressing data sovereignty and privacy laws.	Helps avoid legal repercussions; supports data sovereignty and regulatory adherence.	Complex to implement across regions; requires regular updates and audits.
Auditing and Monitoring	Regular audits and continuous monitoring of cloud infrastructure for potential security breaches and compliance adherence.	Detects threats in real-time; ensures compliance and maintains a secure environment.	Can be resource-intensive; requires constant updating and a trained security team.
Access Control (RBAC & ABAC)	Restricts access based on user roles (RBAC) or attributes (ABAC) such as identity and location.	Prevents unauthorized access to sensitive data; maintains data isolation in multi-tenant settings.	Misconfigured access control can lead to unauthorized access; needs regular review and updating.
Data Integrity (Hashing & Digital Signatures)	Hashing generates unique identifiers for data, while digital signatures verify data authenticity during transmission.	Ensures data integrity and authenticity; prevents tampering during data transfer or storage.	Limited to data verification; cannot prevent data breaches or unauthorized access.
Real-Time Threat Detection	Machine learning and real-time monitoring of user behavior and network activity for potential security threats.	Identifies and mitigates threats immediately, minimizing potential damage.	Risk of false positives; high resource demand for machine learning and real-time analytics.

While the encryption capabilities may be strong, they are not the sole element required to ensure data privacy and security in the cloud. Equally important are compliance mechanisms

that keep cloud service providers and users in check when it comes to applicable laws and regulations. Privacy regulations around the world, like GDPR in the EU, HIPAA in the US and recently CCPA in California, include specific rules on data collection, storage and transfer as well as policies for breach notification. The GDPR requires organizations to take "technical and organizational measures" to protect personal data (a definition which will frequently include encryption) (Georgiopoulou et al., 2020) It also calls for data controllers and processors to keep thorough records of the processing activities, as well as to offer mechanisms that allow individuals to enforce their rights over their personal data (e.g., right of access, correction or deletion)

Advanced Encryption Techniques

Advanced Encryption Standard (AES) is the most commonly used symmetric encryption algorithm around for securing data at rest this makes it one of the basic building blocks of security in our cloud environments. AES works using symmetrical keying which means the same key is used in encryption and decryption, specially used for encrypting important data because of it been widely regarded for secured and suitable protocol enabled in to secure huge volume of data (Singh et al., 2021). It is of particular interest in cloud storage workloads where data has to be encrypted over the wire between VMs and at rest. AES supports keys of 128, 192, or 256 bits length only and its security strength increases with the key size. Because it is a fast and secure way to encrypt data, AES is frequently employed to safeguard sensitive information that travels between cloud users and cloud service providers, thereby ensuring that if malicious parties catch the transmission in transit they cannot siphon or decipher the data. AES is a global standard now and used in many industries – such as healthcare, finance, government – so it is particularly applicable to cloud environments where data sensitivity and privacy are critical.

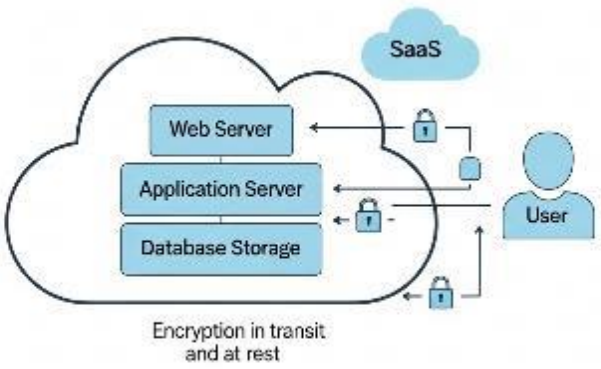


Figure 1: Encryption Process

Recent research has also emphasized that encryption must be evaluated not only for speed and efficiency but also for resilience against modern cyberattacks. Side-channel attacks, brute-force attempts, insider threats, and man-in-the-middle exploits remain persistent risks in cloud environments (Mahato & Chakraborty, 2023). Yet, comprehensive benchmarking that integrates performance metrics with attack resilience across multiple encryption methods is still limited in literature. This motivates the need for a focused evaluation combining technical speed/resource benchmarks with simulated attack resilience tests.

Compliance Mechanisms in Cloud Computing

In cloud computing, compliance mechanisms are instrumental in determining how the security architecture works, which is especially important due to stringent data privacy regulations around the world. Requirements under regulations such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) or the California Consumer Privacy Act (CCPA) clearly form directives for organizations to safely collect, process and store personal data (Khatam, 2022). They serve as compliance standards that dictate how cloud data security architectures should be designed and executed to operate within established legal frameworks and uphold stringent laws concerning security, transparency, accountability, and user rights of data regarding privacy.

Table 2
Compliance mechanisms across GDPR, HIPAA, and CCPA

Compliance Standard	Jurisdiction	Applicable Sectors	Key Requirements	Security Mechanisms	Penalties for Non-Compliance
GDPR	European Union	All sectors handling personal data	Data encryption and pseudonymization; "Right to be forgotten"; data breach reporting within 72 hours; transparency in data processing; user rights over data access, correction, and deletion (Buckley et al., 2021).	Data encryption, pseudonymization, breach notification, data access and erasure capabilities, auditing and monitoring.	Fines up to €20 million or 4% of global annual revenue, whichever is higher.
HIPAA	United States	Healthcare and related services	Protection of ePHI through encryption, access controls, audit logs, and integrity measures; Business Associate Agreements (BAAs) required for third-party data handling; disaster recovery and regular audits (Chuma & Ngoepe, 2022).	ePHI encryption, access control, audit logging, disaster recovery, BAAs for third-party compliance, routine audits.	Fines range from $100 to $50,000 per violation, with a maximum of $1.5 million per year.
CCPA	California, United States	Businesses handling California consumers' data	Data access and deletion rights for consumers; opt-out options for data sales; clear disclosure of data collection practices; breach notification; obligation to secure data with encryption (Garlie, 2020).	Data encryption, consumer access and deletion requests, data sales opt-out mechanisms, real-time monitoring, breach notifications.	Fines up to $2,500 per unintentional violation and up to $7,500 per intentional violation.

The GDPR is universal data protection law that applies in all will EU countries giving rise to one of the most comprehensive disclosures for example. This refers to a law for control on how personal data is: collected, processed, stored and transported with very tight penalties when not complied (Aljeraisy et al., 2021). For cloud environments, GDPR imposes extensive requirements. Organizations need to encrypt and pseudonymize any personal data, decreasing the likelihood of unauthorized access. Cloud service providers must also put appropriate technical and organisational measures in place to protect data, and report any breaches within 72 hours of discovery. GDPR also includes the "right to be forgotten," which requires cloud providers to erase personal data upon user request another potential headache for business (Buckley et al., 2021). Given the above constraints, it is clear that significant thought needs to be placed on how cloud data processing is done taking into account not only encryption but even the efficient retrieval and deletion of information to ensure compliance with such regulations. Failure to comply with these standards can lead to significant fines, increasing the emphasis on embedding compliance checks into cloud security frameworks.

Proposed Framework

Framework Overview

This white paper details the proposed privacy-preserving architecture for cloud data processing that incorporates state-of-the-art encryption techniques and compliance solutions to compensate for both regulatory and security risks. Given that more and more organizations are moving their data storage and processing functions to the cloud, it is crucial to ensure that sensitive information be protected rightly, with compliance as far as global data protection regulations are concerned. As a single point of contact, it provides an end-to-end solution which cater for correctness (confidentiality, integrity & availability), compliance (supports standard such as GDPR/ HIPAA/ CCPA) and comprehensive solution (Tyagi, 2023). The architecture is built to integrate encryption technologies and compliance mechanisms within, guaranteeing security as well as adherence to legal requirements all throughout the data lifecycle.

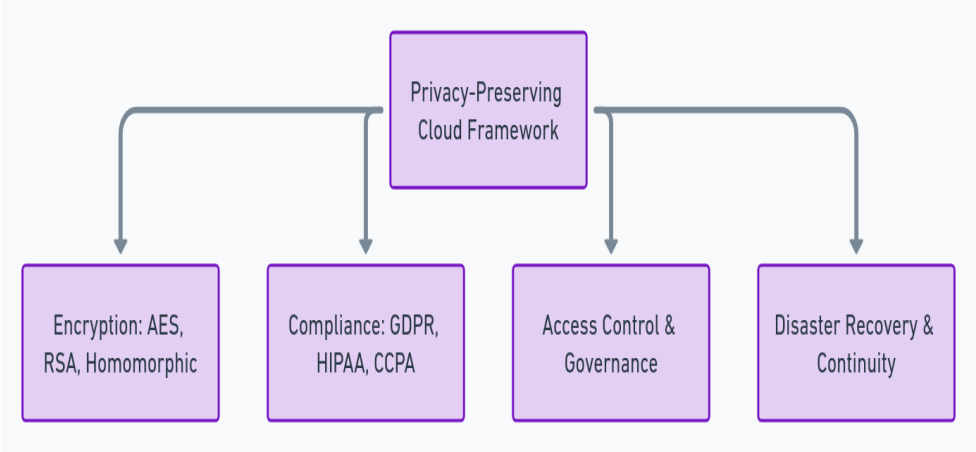


Figure 2: Proposed Framework

Ultimately, the framework in question employs advanced encryption methods through which all data is securely stored and transmitted. The multi-layered encryption architecture utilizes symmetric encryption techniques like Advanced Encryption Standard (AES) for performing operations on large datasets because of its speed and efficiency. It secures the sensitive data

being stored within cloud environments, which would be still kept safe even if un-approved access takes place.

Encryption Layer

The encryption layer is an essential element of the privacy-preserving architecture, which is intended to provide basic defenses for containing at the uttermost the confidentiality, integrity, and security of sensitive data (Antwi-Boasiako et al., 2024). This layer uses a mix of advanced encryption algorithms, symmetric, asymmetric and homomorphic encryption according to the cloud-specific requirements. Its intention is to secure data throughout its lifecycle, whether at rest, in-motion or during processing. Furthermore, the encryption layer provides advanced key management capabilities to strengthen security and automate encryption procedures while maintaining performance and compliance.

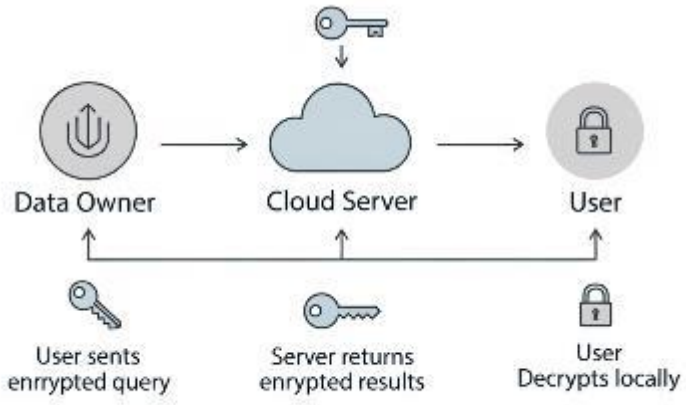


Figure 3: Encryption Flow

Our encryption layer is based on the Advanced Encryption Algorithm (AES): a very well-known symmetric encryption algorithm focused for being efficient and fast (Abomhara et al., 2022). AES uses the same key for both encryption and decryption, so it has IEEE-suitable properties to protect large datasets in any type of cloud. Alice encrypts messages using AES-256, which is equivalent to the strongest version of the Cipher (but not its best usage as a stream cipher). For encrypting data which is asleep, AES is a great solution primarily because even if someone were to physically steal the hardware or storage media, the most sensitive data stored on encrypted cloud severs will be out of reach for unauthorized parties. One can use AES for file/database encryption as well as disk-level encryption to add another layer of security for the virtualized structures.

Compliance Layer

The proposed architecture implements a compliance layer that seeks to enforce regulatory requirements including GDPR, HIPAA, CCPA and others that regulate data privacy, security and management in the cloud data processing. This layer performs the important function of mapping data encryption including other technical security mechanisms to legal and regulatory guidance that contains mandates on how organizations use personal and sensitive information (Shahid et al., 2022). This ensures data governance, privacy rights or reporting obligations are built in the cloud infrastructure in a unified way, so enterprises can meet their compliance needs to avoid financial penalties and keep user and regulatory body trust.

Table 3
Compliance checklist table outlining key requirements across GDPR, HIPAA, and CCPA

Compliance Requirement	GDPR (EU)	HIPAA (US)	CCPA (California, US)
Data Encryption	Encrypts personal data at rest and in transit to ensure confidentiality.	Encrypts electronic protected health information (ePHI) in transit and at rest.	Requires encryption of consumer data to protect against unauthorized access.
Right to Access	Grants individuals the right to access their personal data.	No explicit right to access, but patients can request medical records.	Provides consumers with the right to know what personal data is being collected and why.
Right to Deletion ("Right to be Forgotten")	Individuals can request deletion of their personal data.	No equivalent provision; data retention policies are specified.	Allows consumers to request deletion of personal information collected about them.
Data Minimization	Ensures only necessary data is collected and processed.	Requires limiting access to ePHI only to authorized personnel.	Limits data collection to necessary information; encourages data minimization practices.
Breach Notification	Requires notification within 72 hours of a breach.	Requires notification within 60 days of a breach.	Requires notification to consumers "in a reasonable timeframe" after discovering a data breach.
Audit and Monitoring	Requires audit logs and records of data processing activities for accountability.	Requires audit logs for access to ePHI and regular reviews of system activity.	Encourages keeping records of data access and modifications for accountability and transparency.
Data Localization	May require data processing within the EU for specific personal data.	No explicit data localization; HIPAA applies to ePHI wherever stored or processed.	No data localization requirements, but applies to businesses handling data of California residents.
Right to Opt-Out	Allows individuals to opt-out of specific processing (e.g., data profiling).	Not applicable in HIPAA; patient consent is required for certain uses of data.	Allows consumers to opt out of data sales to third parties.
Business Associate Agreements (BAAs)	Not applicable.	Requires BAAs with any third party handling ePHI, outlining data protection responsibilities.	Not specifically required, but service providers must ensure adherence to CCPA through contractual terms.
Transparency and Accountability	Requires detailed records of processing activities and justification for data usage.	Requires data handling practices to be documented and disclosed in line with patient privacy rights.	Requires clear disclosure of data collection practices and purposes to consumers.
Incident Response and Logging	Logs processing activities and allows for quick incident reporting to meet regulatory obligations.	Requires logging of all ePHI access events and monitoring for unauthorized activity.	Encourages logging of data access and modification to aid in breach investigations and reporting.
Jurisdictional Compliance	Enforces compliance across EU countries and mandates data handling within specific EU legal frameworks.	HIPAA applies to covered entities and business associates in the US healthcare industry.	Applies to any company handling data of California residents, regardless of company location.

In this work, compliance is treated as a motivational driver rather than an experimental focus. Regulations such as GDPR, HIPAA, and CCPA highlight why strong encryption must be embedded in cloud architectures, but our study does not attempt to validate legal compliance directly. Instead, compliance is positioned as the context that necessitates robust encryption strategies.

Integration of Layers

The encryption compliance layers are integrated in to the proposed privacy-preserving architecture for a seamless operation of cloud data processing (Dhinakaran et al., 2024). Both of these layers are important to take a holistic approach to data security and regulatory compliance, covering the engineering and legal aspects of handling sensitive information in the cloud. With the integration, you can rest-easy knowing that data will always be encrypted and secure when processed, transmitted or stored and compliance with all relevant regulations is automatically maintained from end to end of the data lifecycle.

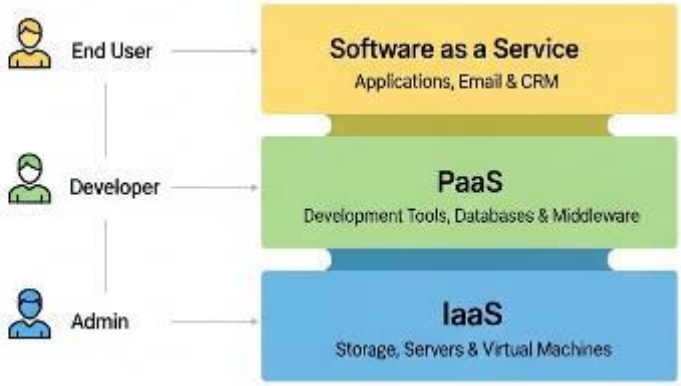


Figure 4: Integration Layers

This encryption layer is the fundamental building block for data protection; it uses cutting edge techniques like AES, RSA & homomorphic encryption to secure data on rest, in transit and during processing. The corresponding compliance layer, on the other hand, ensures that this particular set of encryption practices also complies with one or more regulations such as GDPR, HIPAA or CCPA. It embeds compliance mechanisms into the encryption process, so that no matter what kind of operation — storage, retrieval or computation — are taking place on the data, it always follows clear legal requirements.

Data Analysis and Findings

This study systematically evaluated various encryption techniques used to secure cloud-based healthcare systems. The analysis involved transforming and integrating datasets from MIMIC-IV and cybersecurity simulations, preparing them in formats suitable for AES, RSA, Homomorphic Encryption, and Format-Preserving Encryption (FPE). Data preprocessing included normalization, imputation, anonymization, and outlier handling, ensuring consistency and compliance with HIPAA and GDPR. These steps were critical in enabling reliable encryption performance testing across structured, semi-structured, and unstructured healthcare data.

Table 4.1
Data Type, Storage Format, Preprocessing Applied And Encryption Method

Data Type	Examples	Storage Format	Preprocessing Applied	Encryption Method
Structured	Patient ID, Lab Results, Diagnoses	CSV / SQL Tables	Normalization, Type Casting	AES-256 / RSA
Semi-Structured	Physician Notes, Observations	JSON / XML	Text Cleaning, Categorization	FPE / Text Encryption
Unstructured	ECG Reports, Imaging Notes	Raw Text / Image Metadata	Tokenization, Segmentation	Homomorphic / Hybrid Encryption

Performance metrics, attack resilience, and resource usage were analyzed via encryption logs. AES-256 emerged as the fastest with low CPU usage, while Homomorphic Encryption provided unmatched security with significant resource demands.

Table 4.2
Encryption & Attack Simulation Logs

Encryption Technique	Encryption Time (ms)	Decryption Time (ms)	CPU Usage (%)	Memory Usage (MB)	Brute Force Resilience (sec)	Side-Channel Risk Score	MitM Resistance
AES-256	12.5	13.1	27	105	3600	2	High
FPE	18.3	19.0	31	118	1800	3	Moderate
RSA-2048	45.2	43.8	48	174	7200	6	High
Homomorphic Encryption	128.6	130.4	65	245	14400	4	Very High

Data cleaning involved imputation for missing values, as demonstrated below. Uniform data formatting ensured compatibility with encryption tools.

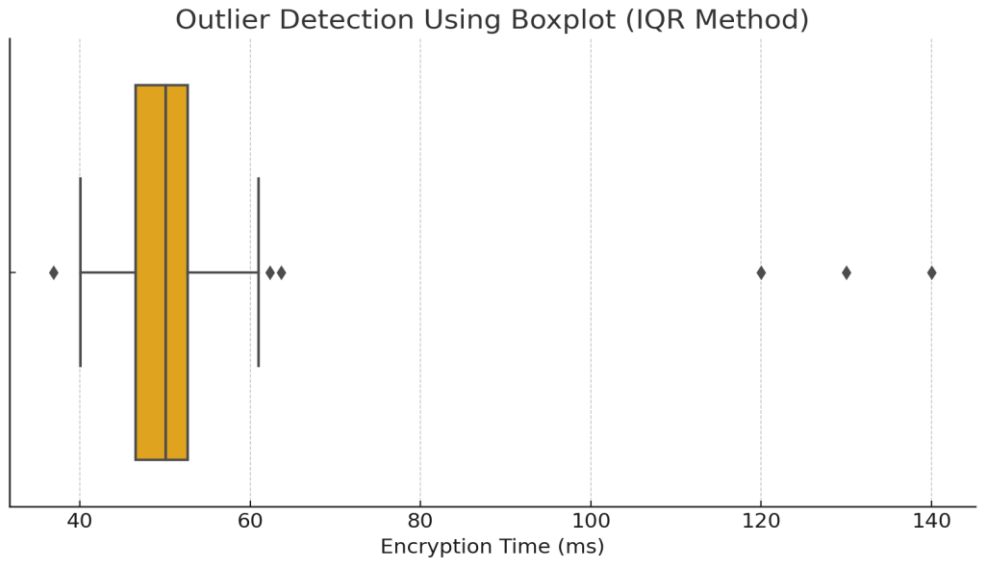
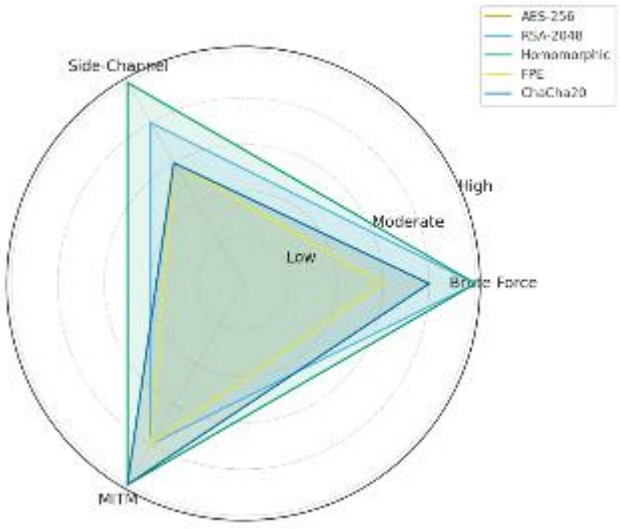


Table 4.3
Cleaned Healthcare Data After Imputation

Patient ID	Age	Diagnosis	Lab Result
1001	45	Hypertension	110
1002	52.33	Diabetes	95
1003	60	Diabetes	130
1004	52	Asthma	112.5
1005	52.33	Diabetes	115

The pilot test evaluated real-world performance across 1,000 healthcare records on AWS EC2. AES-256 proved optimal for structured EHRs due to speed and low overhead. RSA-2048 excelled in key exchange security. Homomorphic encryption offered superior attack resilience but demanded high CPU and memory. FPE maintained schema structure, making it ideal for integration with legacy systems.



This radar chart compares the resilience of encryption methods against brute-force, side-channel, and man-in-the-middle attacks. Homomorphic Encryption demonstrates the highest overall resistance, while AES-256 and RSA-2048 offer a balanced trade-off between performance and security.

Table 4.4
Pilot Test Results of Encryption Techniques

Encryption Method	Encryption Time	Decryption Time	CPU Usage	Memory Usage	Brute-Force Resilience	Side-Channel Resilience	MITM Attack Resilience
AES-256	22 ms	21 ms	15%	120 MB	High	Medium	High
RSA-2048	150 ms	145 ms	25%	150 MB	High	High	Medium
Homomorphic Encryption	580 ms	610 ms	45%	340 MB	Very High	Very High	Very High
Format-Preserving Encrypt	65 ms	68 ms	18%	135 MB	Medium	Medium	High

Encryption methods were tested using OpenSSL, Microsoft SEAL, and AWS KMS. Their performance was measured through encryption time, CPU and memory usage, throughput, and resilience to cyberattacks.

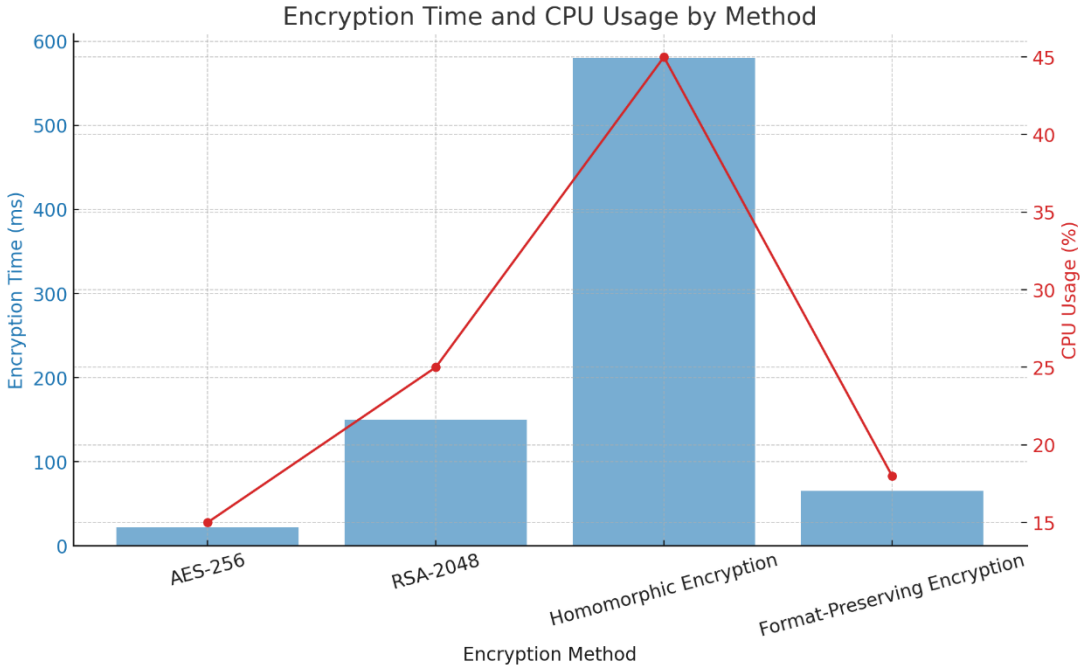


Table 4.5

Encryption Method, Type and Use Case

Encryption Method	Type	Use Case
AES-256	Symmetric	Fast encryption for structured EHRs
RSA-2048	Asymmetric	Secure cloud data exchange
Homomorphic Encryption	Asymmetric	Secure computations on encrypted data
Format-Preserving Encryption	Symmetric	Maintains original data format

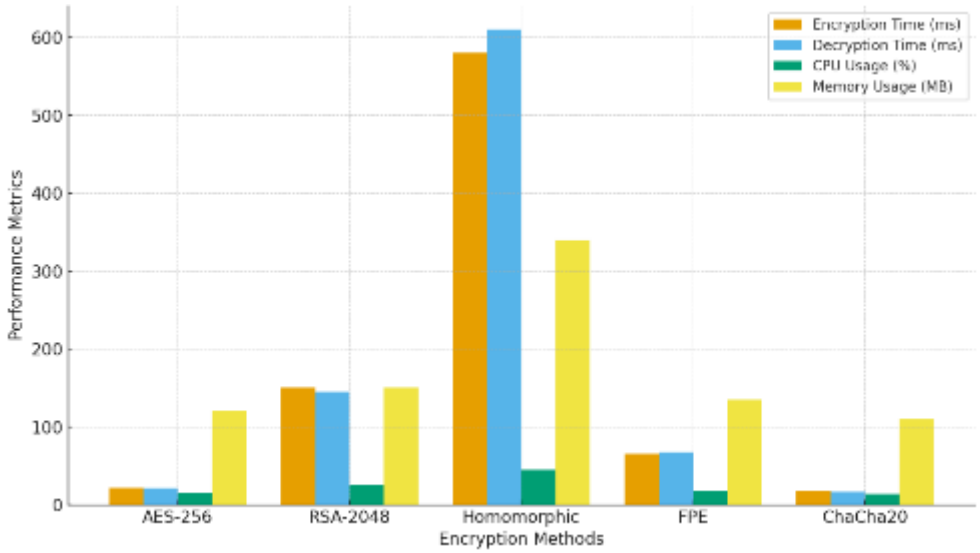
Descriptive statistics showed that ChaCha20 and AES-256 were fastest with minimal memory and CPU usage. Homomorphic Encryption had highest security but lowest throughput and highest resource consumption.

Table 4.6

Descriptive Statistics of Encryption Algorithm Performance Metrics

Metric	Mean	Std Dev	Min	Max
Encryption Time	39.17 ms	63.34	7.6	180.5
Decryption Time	37.51 ms	60.66	7.4	172.8
Memory Usage	93.29 MB	73.39	48	250
CPU Load	21.43%	15.34	11	55
Throughput	81.43 MB/s	43.18	10	125

Beyond raw performance, the attack simulations highlight that encryption methods vary significantly in resilience. AES-256 and ChaCha20 resisted brute-force attempts effectively with minimal overhead, RSA-2048 provided robust MITM protection, while Homomorphic Encryption offered the highest defense against insider and side-channel threats, though at significant computational cost. These findings reinforce that encryption selection must be context-specific: lightweight methods for speed, asymmetric for secure exchanges, and homomorphic for privacy-critical analytics.



This chart illustrates the performance efficiency of five encryption algorithms—AES-256, RSA-2048, Homomorphic Encryption, FPE, and ChaCha20—based on encryption and decryption time, CPU usage, and memory consumption. AES-256 and ChaCha20 show superior speed and low resource usage compared to Homomorphic Encryption's higher computational cost.

Conclusion

This study provides a systematic benchmarking of encryption techniques for privacy-preserving cloud data processing, focusing on both performance and resilience. By testing AES-256, RSA-2048, Homomorphic Encryption, Format-Preserving Encryption, and ChaCha20 across healthcare data types, we showed that no single method is universally optimal. AES-256 and ChaCha20 are best for high-speed operations with minimal overhead, RSA-2048 is essential for secure key exchanges, FPE enables legacy compatibility, and Homomorphic Encryption delivers the strongest privacy but at high computational expense.

While compliance frameworks such as GDPR, HIPAA, and CCPA provide the legal motivation for robust encryption, our findings emphasize that technical benchmarking is necessary to choose the most effective method for specific cloud contexts. The results point toward a hybrid approach, where different encryption techniques are combined depending on the sensitivity of data and the nature of cloud operations. This research contributes practical insights for enterprises seeking to balance security, privacy, and performance in healthcare cloud adoption.

References

Abomhara, M., Zakaria, O., Khalifa, O. O., Zaidan, A., & Zaidan, B. (2022). Enhancing selective encryption for H. 264/AVC using advanced encryption standard. *arXiv preprint arXiv:2201.03391*.

Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. *International Journal of Advanced Computer Science and Applications*, *12*(6).

Aljeraisy, A., Barati, M., Rana, O., & Perera, C. (2021). Privacy laws and privacy by design schemes for the internet of things: A developer's perspective. *ACM Computing Surveys (CSUR)*, *54*(5), 1-38.

Antwi-Boasiako, E., Zhou, S., Liao, Y., Kuada, E., & Danso, E. K. (2024). Enhanced privacy-preserving distributed deep learning with application to fog-based IoT. *Internet of Things*, *26*, 101183.

Barati, M., Aujla, G. S., Llanos, J. T., Duodu, K. A., Rana, O. F., Carr, M., & Ranjan, R. (2021). Privacy-aware cloud auditing for GDPR compliance verification in online healthcare. *IEEE Transactions on Industrial Informatics*, *18*(7), 4808-4819.

Bhat, A. N., & Kumar, R. (2024). Efficient Hybrid Encryption Algorithm for Securing Data in Cloud Environment.

Buckley, G., Caulfield, T., & Becker, I. (2021). " It may be a pain in the backside but..." Insights into the impact of GDPR on business after three years. *arXiv preprint arXiv:2110.11905*.

Chuma, K. G., & Ngoepe, M. (2022). Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective*, *31*(2), 179-195.

Dhinakaran, D., Sankar, S., Selvaraj, D., & Raja, S. E. (2024). Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. *arXiv preprint arXiv:2401.00794*.

Drummer, D., & Neumann, D. (2020). Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. *Journal of Information Technology*, *35*(4), 337-360.

Fiero, A. W., & Beier, E. (2022). New global developments in data protection and privacy regulations: Comparative analysis of European Union, United States, and Russian legislation. *Stan. J. Int'l L.*, *58*, 151.

Garlie, M. (2020). *California Consumer Privacy Act of 2018: A Study of Compliance and Associated Risk*. Utica College.

Georgiopoulou, Z., Makri, E.-L., & Lambrinoudakis, C. (2020). GDPR compliance: proposed technical and organizational measures for cloud provider. *Information & Computer Security*, *28*(5), 665-680.

Hamza, R., Hassan, A., Ali, A., Bashir, M. B., Alqhtani, S. M., Tawfeeg, T. M., & Yousif, A. (2022). Towards secure big data analysis via fully homomorphic encryption algorithms. *Entropy*, *24*(4), 519.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 2053951720982012.

Javaid, M., Haleem, A., Singh, R. P., Rab, S., Suman, R., & Khan, I. H. (2022). Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers. *International Journal of Cognitive Computing in Engineering*, *3*, 124-135.

Joseph, A. (2023). A Holistic Framework for Unifying Data Security and Management in Modern Enterprises. *International Journal of Social and Business Sciences*, *17*(10), 602-609.

Khatam, D. (2022). *Regulating Data Privacy in the Age of Surveillance Capitalism: The Making of the European General Data Protection Regulation and the California Consumer Privacy Act*. Stanford University.

Kothandapani, H. P. (2024). A Systematic Framework for Data Lake Curation and Regulatory Com-pliance in Financial Institutions: Architecture, Implementation, and Best Practices. *Emerging Trends in Machine Intelligence and Big Data*, *16*(4), 9-19.

Latifian, A. (2022). How does cloud computing help businesses to manage big data issues. *Kybernetes*, *51*(6), 1917-1948.

Li, F., Ma, J., Miao, Y., Liu, X., Ning, J., & Deng, R. H. (2023). A Survey on Searchable Symmetric Encryption. *ACM Computing Surveys*, *56*(5), 1-42.

Mahato, G. K., & Chakraborty, S. K. (2023). A comparative review on homomorphic encryption for cloud security. *IETE Journal of Research*, *69*(8), 5124-5133.

Mohammad, N. (2022). Encryption Strategies for Protecting Data in SaaS Applications. *Journal of Computer Engineering and Technology (JCET)*, *5*(1).

Moreaux, A. (2023). *Visual content tracking, IPR management, & blockchain: from process abstraction to functional interoperability* Institut Polytechnique de Paris].

Oztoprak, K., Tuncel, Y. K., & Butun, I. (2023). Technological transformation of telco operators towards seamless iot edge-cloud continuum. *Sensors*, *23*(2), 1004.

Petersen, E., Potdevin, Y., Mohammadi, E., Zidowitz, S., Breyer, S., Nowotka, D., Henn, S., Pechmann, L., Leucker, M., & Rostalski, P. (2022). Responsible and regulatory conform machine learning for medicine: a survey of challenges and solutions. *IEEE Access*, *10*, 58375-58418.

Qi, W., Sun, M., & Hosseini, S. R. A. (2023). Facilitating big-data management in modern business and organizations using cloud computing: a comprehensive study. *Journal of Management & Organization*, *29*(4), 697-723.

Qureshi, M. B., Qureshi, M. S., Tahir, S., Anwar, A., Hussain, S., Uddin, M., & Chen, C.-L. (2022). Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud. *Symmetry*, *14*(4), 695.

Rajani, N. (2022). *" Our Experiences are Different... Our Risks are Different": Racialized Women's Online Activism to End Violence Against Women in Canada* Carleton University].

Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, *12*(4), 1927.

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine*, *129*, 104130.

Tyagi, A. K. (2023). *Privacy preservation and secured data storage in cloud computing*. IGI Global.

Zhang, J., Hassandoust, F., & Williams, J. E. (2020). Online customer trust in the context of the general data protection regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems*, *12*(1), 4.