International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 20s, 2025
https://www.theaspd.com/ijes.php

A Comparative Study Of Encryption Algorithms For Enhancing Data Confidentiality In Cloud Storage Systems

Puja Biswas*
*Assistant Professor. Sivananda Sarma Memorial RV Degree College (SSMRV), Bangalore, Karnataka
Email : puja6719@gmail.com

Abstract
The fast adoption of cloud storage in enterprise and personal computing has raised a lot of issues related to data confidentiality and security. As the number of data breaches and unauthorized access cases continues to increase, one of the most important priorities has become the need to ensure the safety of confidential information. One of the most essential answers to this problem is encryption, which provides a strong system of protecting the data even in the case of the cloud infrastructure being attacked. This paper provides a comparative study of the common encryption algorithms with emphasis on the effectiveness of the algorithms in ensuring confidentiality in cloud storage systems. The evaluation of key performance indicators such as encryption and decryption speed, key length, security strength, resource consumption (computational), and scalability was carried out systematically. As a result of this analysis, the research concludes that Advanced Encryption Standard is a recommended option when it comes to applications that require high speed and low latency of data processing. On the other hand, Elliptic Curve encryption is highly efficient on a resource-constrained system, i.e., a processing- and memory-constrained environment, and therefore, can be applied in mobile and edge computing. The normal algorithm, like Rivest-Shamir-Adleman, is secure, but it has been proven to be resource-consuming and cannot be used in dynamic cloud processes. The paper has come to the conclusion that the choice of an encryption method should be determined by the specific operational context and security requirements of the intended cloud deployment.
Keywords: *Cloud storage, Data confidentiality, Encryption algorithms, Security performance, Confidentiality metrics.*

1. INTRODUCTION

The last twenty years have witnessed an exponentially increasing digital data growth that has led to a paradigm change in the management, access, and storage of information. The advent and popularization of cloud computing technologies have brought scalable, flexible, and affordable alternatives to traditional data storage systems. The reliance on cloud-based platforms by business organizations and individuals to store sensitive information, including financial reports and medical data, intellectual property, and classified research results, is on the rise. The necessity to develop data-driven applications and the growing demand to have access to data all the time further add to the fact that the world is becoming dependent on cloud storage infrastructure [1].

It is not an ill-free trend of cloud adoption. With the fact that data is no longer stored on-premises servers but instead is stored in a multi-tenant architecture, the issue of data privacy and security has become more vocal. The concept of cloud storage systems is that they form a common infrastructure, which presents inherent weaknesses. When these vulnerabilities are exploited, they may have dire consequences such as unauthorized access, breach of data, and insider threat. These occurrences not only jeopardize sensitive information but also undermine the confidence in cloud service providers and increase compliance concerns, especially in the industries that have stringent regulatory requirements [2]. The question of cloud security is not easy. On the one hand, the external threats, including cyber-attacks, man-in-the-middle interceptions, and advanced persistent threats, are expected to take advantage of the loopholes within the system. At the opposite end of the spectrum are internal risks and they include inattentive workforce and malicious insiders. Security is also compounded by the fact that the cloud relies on virtualized resources, which in turn means that breaks in the hypervisor level can potentially leak out the entire volume of data [3]. Adding to these problems is the fact that users do not usually have access to the physical infrastructure of their data in the cloud or access logs of their data, which introduces a trust gap between the cloud consumer and the cloud provider [4].

Encryption has come out as a pillar in cloud security architecture in order to curb these risks. It offers a method of encryption of data in rest, as well as in motion, making sure that the information is confidential even in case it is obtained using unauthorized channels. Encryption reduces the effects of possible intrusion because even when intruded data is captured, it is unreadable without the decryption keys as the data is converted into ciphertext using algorithms. Encryption is also central to allow secure data sharing, implement access control, and meet regulatory compliance in terms of data protection [5]. Symmetric and asymmetric encryption

mechanisms are the most commonly used in the current cloud ecosystems in order to ensure confidentiality. Encryption is computationally effective and can be applied in encryptions of high volumes of data through symmetric encryption that uses the same key to encrypt and decrypt the information. Asymmetric encryption, whereby the key pairs are used in the form of public and private keys, provides greater security in key exchange, digital signature and identity authentication. Also, hybrid encryptions are being used more and more to give the performance of symmetric systems and the secure key distribution capability of asymmetric systems [6]. Although it is of utmost importance, the application of encryption in cloud environment comes with its challenges. The most significant of them are the key management, performance overhead, compatibility with current cloud workflows and multi-user scalability. As an example, encryption can be defeated by poor key storage or inadequate key rotation procedures that allow data to be subjected to unauthorized decryption [7]. Additionally, it is of utmost importance to balance the strength of encryption and its computational cost in latency-critical applications or platforms with limited resources like mobile and IoT-based cloud platforms [8].

To address these challenges, a large number of encryption algorithms are being developed and investigated by system designers and the researchers that differ in terms of complexity, the degree of security, and performance. Cryptography is constantly evolving with old standards like AES and RSA, and newer ones like elliptic curve cryptography (ECC), Blowfish and homomorphic encryption. The comparative analysis is becoming vital in determining which algorithms would be most applicable in particular cloud storage applications, including enterprise backup, real-time data analysis, or mobile cloud access [9]. Furthermore, the growing attention to data sovereignty, the adherence to legal regulations (such as GDPR, HIPAA, or CCPA), and zero-trust architecture pose further support to the fact that an encryption strategy should not only be robust but also capable of being implemented in different regulatory and operational contexts. In that sense, the performance of encryption algorithms compared should not be judged solely based on raw numbers but also on the consideration of the context such as how easy it is to integrate with cloud APIs, compatibility with distributed storage models, and support of key lifecycle automation [10].

As cloud computing is dynamic and the sophistication of the threat vectors is increasing, this paper has tried to present an analytical view of commonly used encryption algorithms and their relevance in improving data confidentiality within cloud storage systems. The review is based on the performance indicators including encryption/decryption rate, key size, resistance to cryptographic attack and resource consumption. By so doing, the paper aims at building a clear comparative picture of the abilities, weaknesses, and the viability of the algorithms in the real world.

Objectives of the Study

1. To compare specific encryption algorithms based on their confidentiality performance within cloud storage environments.
2. To assist researchers and system designers in selecting the most appropriate encryption algorithms tailored to specific use-case requirements in cloud ecosystems.

2. Cloud Storage Security and Confidentiality Needs

The era of cloud computing has made data confidentiality in the shared, virtualized infrastructures a basic need of enterprises as well as individual users. The nature of cloud-based systems is to work in distributed and frequently multi-tenant architecture, which makes them vulnerable to the risks that undermine data security. Since organizations have started to transfer sensitive data such as intellectual property, customer records, healthcare information and financial data to remote storage, it becomes important to secure such data so that it is not leaked to unauthorized parties. This requirement needs to be met by cloud environments with sound confidentiality preserving frameworks that are dynamic and scalable [11].

Confidentiality in the storage of the cloud means that only authorized individuals will get access to the data and interpret it. This will require the application of encryption process both in transit and at rest. The problem is not only to use powerful encryption but also to control who has the rights to decode the information and how. Although the cryptographic algorithm is mathematically sound, encryption may fail to provide protection against unauthorized access to the encrypted information because of compromised keys, access controls or misconfigurations of the system [12]. These threats may be caused by external attackers who use the vulnerabilities in the cloud infrastructure as well as internal actors who have legitimate access privileges and use them in a wrong way. Insider threats in particular contribute to a big number of data breaches in the clouds because of the inefficiently pursued identity and access management (IAM) policies.

Table 1 gives an overview of typical threats, related vulnerabilities, and examples of threats associated with the sources of data confidentiality threats in cloud environments.

Table 1. Threats to Data Confidentiality in Cloud Storage [13]

Threat Type	Description	Example
External Breach	Unauthorized access via malware, phishing, or exploits	Compromised VMs in multi-tenant systems
Insider Threat	Malicious or negligent misuse of access rights	Admin downloading sensitive records
Data Leakage	Accidental or intentional data exposure	Misconfigured S3 buckets
Weak Access Control	Poor IAM or absence of multi-factor authentication	Stolen login credentials
Shared Infrastructure Risk	Overlap in tenant data boundaries	Cross-VM access exploits

As the table highlights, cloud storage threats originate from multiple layers—network, application, hypervisor, and user access. These layered vulnerabilities require equally layered defense mechanisms to uphold confidentiality. In many cases, improper role-based access controls, outdated authentication models, and lack of contextual access policies allow attackers to bypass protections and gain unauthorized data access [13]. To effectively mitigate these threats, the design and deployment of cloud storage systems must embrace the core principles of information security. These principles, commonly referred to as the CIA triad—Confidentiality, Integrity, and Availability—are often extended in modern cloud security frameworks to include Authenticity. Confidentiality ensures that information is not disclosed to unauthorized entities, integrity guarantees that data remains unaltered during storage or transmission, availability ensures that authorized users can access data when needed, and authenticity verifies the legitimacy of data sources and communication endpoints [14]. Figure 1 illustrates the relationship between these four key security goals and how they map onto cloud storage functionalities.

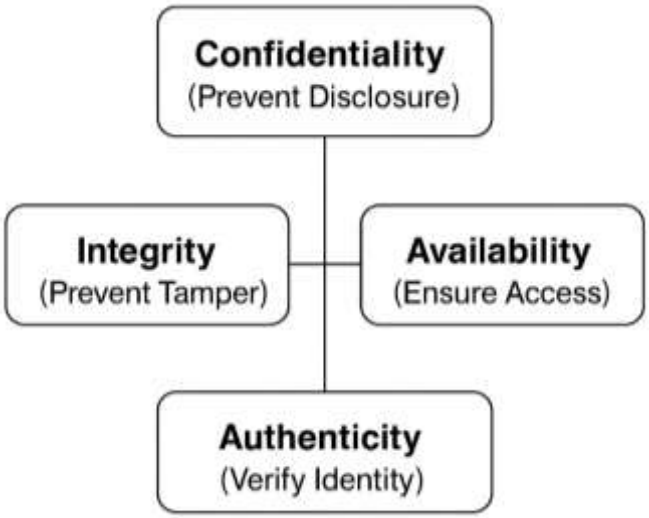

Figure 1. Core Security Goals in Cloud Storage Systems [14]

As shown in Figure 1, confidentiality and integrity are directly tied to cryptographic measures, such as encryption and hashing, whereas availability and authenticity are supported through high availability configurations, redundancy, and secure digital signatures. In cloud platforms, failure to address any one of these goals can undermine the entire storage security framework, emphasizing the need for holistic security strategies.

A critical debate in cloud data protection revolves around the implementation of encryption: whether it should be handled by the cloud provider (server-side encryption) or by the data owner (client-side encryption). Server-side encryption is convenient and often automatic; however, it places key control in the hands of the provider. In contrast, client-side encryption enables end-users to retain full control over their data, as encryption occurs before data is uploaded to the cloud [15]. Both approaches have advantages and limitations. Server-side

encryption typically offers seamless integration with cloud services, better performance optimization, and compliance reporting. However, it suffers from potential provider-side trust issues. Client-side encryption offers stronger privacy guarantees and reduced reliance on the provider's security posture, but it introduces challenges in key distribution, searchability, and user-side key management [16].

To strengthen client-side encryption, researchers have proposed systems that combine encryption with ownership proof schemes and trusted execution environments (TEEs). These approaches aim to ensure that deduplication (a space-saving feature commonly used in cloud storage) does not compromise confidentiality. For instance, systems that support encrypted deduplication while proving ownership without revealing plaintext represent promising directions in privacy-preserving cloud storage [17]. In conclusion, the confidentiality of cloud-stored data is not merely a feature, but a necessity in today's risk-prone computing environments. It involves a comprehensive approach that encompasses secure architectural design, precise access control, robust encryption, and a clear understanding of potential vulnerabilities. The balance between operational efficiency and cryptographic rigor remains at the heart of cloud security research and implementation.

3. Selected Encryption Algorithms for Comparative Study

Encryption algorithms serve as the cornerstone of securing sensitive data in cloud environments. They provide mathematical mechanisms to transform plaintext into ciphertext, rendering it unintelligible to unauthorized users. The selection of appropriate algorithms must consider factors such as speed, scalability, key length, resistance to attacks, and computational efficiency, especially when applied in cloud computing contexts. This section presents a comparative overview of symmetric, asymmetric, and advanced/modern encryption algorithms, based on their performance, application suitability, and operational characteristics.

3.1 Symmetric Algorithms

Symmetric key encryption employs the same key for both encryption and decryption, making it computationally efficient for bulk data processing. Among the most prominent symmetric algorithms used in cloud storage are AES, Blowfish, and RC5. AES (Advanced Encryption Standard) has emerged as the industry standard due to its speed, flexibility in key lengths (128, 192, and 256 bits), and hardware acceleration support. It is widely adopted in commercial cloud services such as AWS, Azure, and GCP due to its consistent performance and strong security guarantees. Performance benchmarking demonstrates that AES consistently outperforms legacy algorithms like DES and 3DES in terms of encryption/decryption speed and memory efficiency [18].

Blowfish, known for its flexible key length ranging from 32 to 448 bits, was once considered a viable alternative to DES. Although it is computationally fast and consumes low memory, it is considered outdated due to known weaknesses in its key schedule and susceptibility to birthday attacks under specific conditions [19]. It is still used in some embedded or legacy cloud services that prioritize performance over cryptographic strength. RC5, a parameterized block cipher with variable block size, key length, and number of rounds, is well-suited to lightweight cryptographic tasks. Its configurability makes it adaptable to constrained environments such as cloud-based IoT systems. However, it lags behind AES in terms of resistance to modern cryptanalytic attacks and is generally limited to scenarios where simplicity and speed are favored over high-grade security [20]. A comparative summary of these symmetric encryption algorithms is presented in Table 2, based on multiple performance benchmarks.

Table 2. Performance Comparison of Symmetric Algorithms [21]

Algorithm	Key Size (bits)	Encryption Speed	Security Level	Memory Usage	Suitability in Cloud
AES	128/192/256	High	Very High	Low	Excellent
Blowfish	32–448	Very High	Medium	Low	Moderate (Legacy/IoT)
RC5	Variable	High	Low–Medium	Very Low	Limited (IoT use)

Table 2 highlights that while AES dominates in both performance and security, Blowfish and RC5 retain niche use in specific cloud scenarios where lightweight cryptography is essential [21].

3.2 Asymmetric Algorithms

Asymmetric encryption uses a public-private key pair, making it highly effective for secure key exchange and authentication. RSA and ECC are the two most prominent asymmetric algorithms utilized in cloud infrastructures.

RSA remains a robust solution, especially for digital signature verification and secure key exchange. A typical RSA-2048 bit key provides strong protection against brute-force attacks but comes at the cost of high computational overhead. Its performance in large-scale cloud systems is constrained by encryption/decryption latency and high resource consumption, particularly when used in combination with symmetric encryption for bulk data operations [22].

ECC (Elliptic Curve Cryptography) achieves equivalent levels of security with significantly smaller key sizes. For instance, a 256-bit ECC key is comparable in strength to a 3072-bit RSA key. This advantage translates to lower bandwidth consumption and faster computation, making ECC ideal for mobile and resource-constrained cloud environments [23]. ECC's adoption in modern cloud services is increasing due to its superior scalability and reduced power requirements.

Hybrid encryption models, combining AES with RSA or ECC, have become increasingly popular. These models leverage the speed of symmetric encryption and the secure key exchange mechanisms of asymmetric algorithms. Figure 2 shows a typical hybrid encryption process deployed in cloud-based data protection.

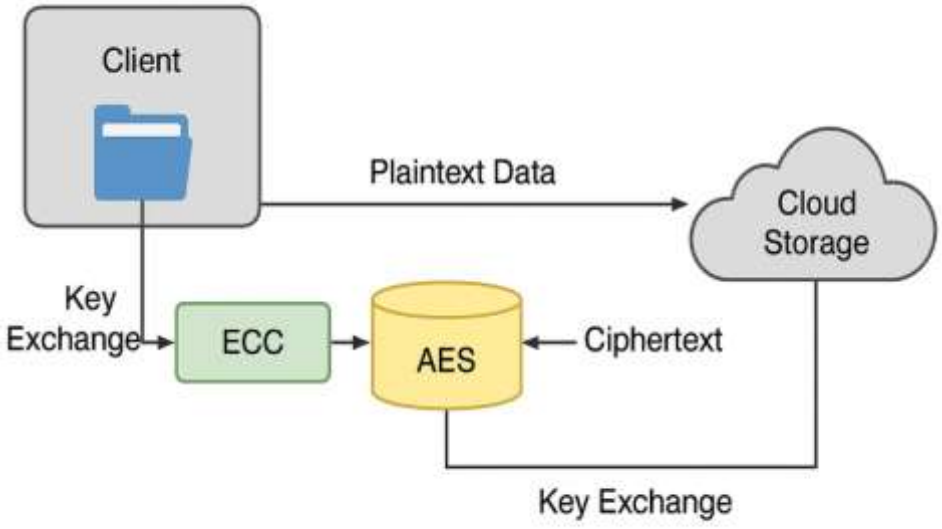

Figure 2. Hybrid Encryption Model Using AES and ECC in Cloud Storage [24].

As illustrated in Figure 2, symmetric encryption (AES) handles the bulk data, while ECC facilitates secure key transmission, resulting in a balance between performance and security in distributed cloud systems [24]. In real-time evaluations, ECC-based solutions demonstrated better throughput and lower key generation time compared to RSA, particularly in mobile cloud environments [25].

3.3 Advanced/Modern Approaches

Beyond traditional symmetric and asymmetric cryptography, advanced methods such as homomorphic encryption and post-quantum encryption are being explored to future-proof cloud data protection. Homomorphic encryption allows computation on ciphertexts, enabling secure data processing in untrusted environments without the need for decryption. Although it holds transformative potential for privacy-preserving analytics and encrypted machine learning, current implementations suffer from excessive computational complexity and are not yet practical for general-purpose cloud storage [26]. Benchmarks show that homomorphic schemes are orders of magnitude slower than conventional algorithms, making them viable only in niche applications where confidentiality outweighs latency. Nonetheless, cloud-based research infrastructures are integrating partial homomorphic encryption (PHE) for limited operations such as addition or multiplication. Table 3 provides a brief comparison of partial, somewhat, and fully homomorphic encryption models.

Table 3. Types of Homomorphic Encryption [27]

Type	Supported Operations	Efficiency	Cloud Suitability
Partial (PHE)	Single operation	High	Selective tasks
Somewhat (SHE)	Multiple but limited	Medium	Research-only
Fully (FHE)	Arbitrary operations	Very Low	Not yet practical

Table 3 outlines the operational scope and limitations of homomorphic encryption schemes in cloud systems [27].

Another major development is post-quantum encryption (PQE), which aims to withstand cryptanalytic attacks from quantum computers. Algorithms based on lattice problems, such as NTRU and LWE (Learning with Errors), are being standardized by NIST and considered promising for quantum-resistant cloud security. These schemes, while still under research, are gaining traction due to the anticipated obsolescence of RSA and ECC in the quantum era [28]. Quantum-safe encryption is especially critical for data with long confidentiality lifespans, such as governmental, medical, or intellectual property archives. Research shows that post-quantum lattice-based algorithms can be integrated into hybrid cloud environments, though current implementations still face performance bottlenecks [29]. Furthermore, PQE requires re-engineering of key exchange protocols and secure storage strategies, making it a subject of ongoing evaluation [30].

As illustrated in recent theoretical models, integrating post-quantum frameworks into existing cloud infrastructures demands both algorithmic robustness and scalable key distribution mechanisms. Current efforts focus on developing forward-compatible systems that support PQE alongside classical encryption, enabling a smooth transition once quantum computing becomes commercially viable [31].

4. EVALUATION METHODOLOGY

Evaluating encryption algorithms for cloud storage requires a multifaceted assessment of key performance indicators that determine not only the security level but also the feasibility of deployment at scale. These indicators include encryption/decryption speed, key size vs. security strength, CPU/memory usage, resistance to known cryptographic attacks, ease of key management, and scalability in multi-user environments.

4.1 Encryption and Decryption Speed

The speed of encryption and decryption operations directly affects user experience and system responsiveness in cloud-based services. Symmetric algorithms, such as AES and Blowfish, are generally faster due to their lightweight mathematical operations, whereas asymmetric algorithms like RSA or ECC are more computationally intensive. A comparative study across symmetric and asymmetric schemes indicates that symmetric methods can encrypt large volumes of data in significantly less time, making them suitable for storage-layer protection [20].

4.2 Key Size and Security Level

The size of the encryption key is directly proportional to the complexity of decryption by brute-force methods. However, longer keys often require more processing power and memory. In symmetric cryptography, AES supports 128-, 192-, and 256-bit keys, offering high levels of security with minimal latency. Asymmetric methods like RSA typically require 2048-bit or longer keys, while ECC achieves comparable security with smaller key sizes (e.g., ECC-256 ≈ RSA-3072), resulting in faster computations with less overhead [23]. This advantage becomes critical for mobile cloud environments and edge computing scenarios. **Table 3.** below summarizes the relationship between key size and security level across major encryption algorithms.

Table 3. Key size and security levels of common encryption algorithms [23].

Algorithm	Key Size	Security Level	Application Context
AES	128–256 bits	Very High	General-purpose cloud storage
RSA	≥2048 bits	Very High	Key exchange, digital signatures
ECC	256 bits	Very High	Mobile, IoT, cloud APIs
Blowfish	32–448 bits	Medium	Fast encryption, legacy systems
RC5	Variable	Low–Medium	Lightweight/embedded systems

4.3 CPU and Memory Usage

Resource usage is a crucial performance metric in cloud services, especially in multi-tenant architectures where CPU and memory are shared. Symmetric algorithms generally consume fewer computational resources, while asymmetric algorithms like RSA are heavy on CPU, particularly during key generation and encryption. Benchmarking results confirm that AES demonstrates optimal memory consumption with hardware acceleration, while hybrid schemes integrating symmetric and asymmetric methods achieve a balance between security and performance [26].

4.4 Resistance to Cryptographic Attacks

Each encryption scheme's resilience to attacks determines its long-term applicability in security-critical applications. AES has been extensively tested and shown high resistance to differential and linear cryptanalysis. Meanwhile, RSA and ECC remain effective against traditional attacks if key sizes are sufficient. The emergence of quantum computing, however, threatens RSA and ECC with Shor's algorithm, necessitating exploration into post-quantum cryptographic models. Lattice-based and multivariate polynomial schemes are currently among the most promising in resisting quantum-level threats [31].

4.5 Ease of Key Management

Key management, particularly in distributed cloud ecosystems, introduces a significant challenge. It includes the generation, distribution, rotation, and revocation of cryptographic keys. Centralized key management systems (KMS) simplify administration but are also single points of failure. Studies show that cloud-native solutions like AWS KMS or Azure Key Vault, when integrated with secure hardware modules (HSMs), offer scalable and audit-ready frameworks for encryption key handling. ECC-based schemes are especially beneficial due to smaller key sizes and lower exchange times [32].

4.6 Scalability in Multi-User Cloud Environments

The ability to scale encryption mechanisms for thousands or millions of concurrent users is critical for public and hybrid cloud platforms. AES stands out in this regard due to its high throughput and support for hardware acceleration. However, the computational overhead of RSA makes it less suited for data-at-rest scenarios and more appropriate for initial key negotiation or digital signatures. ECC, by offering security with reduced computational cost, scales better across mobile clients and distributed storage nodes. Modern hybrid frameworks combining AES with RSA or OTP, backed by adaptive key management, have demonstrated strong performance under concurrent access scenarios [33], [34]. **Figure 3** below shows a performance comparison of CPU usage among encryption schemes under concurrent user load.

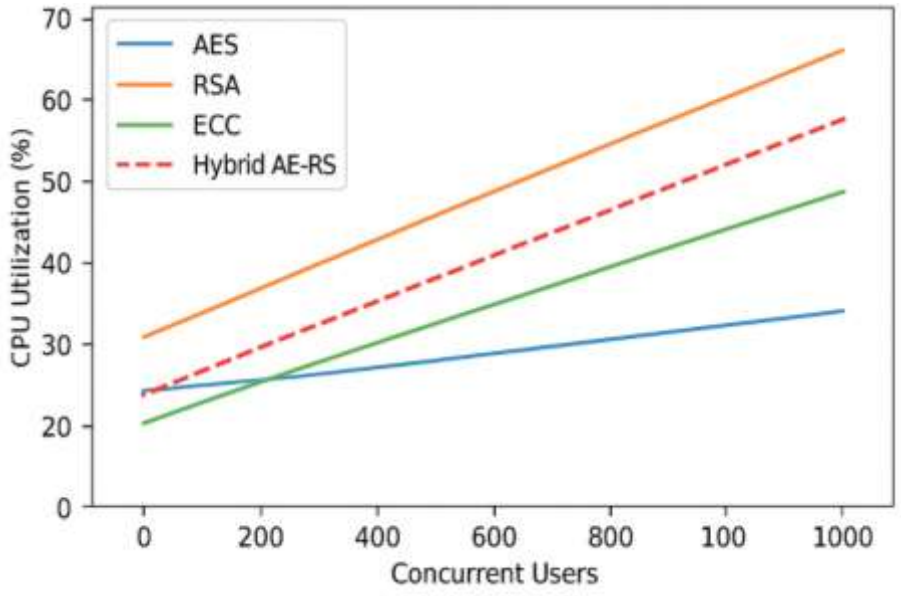

Figure 3: Comparative CPU Utilization of Cryptographic Algorithms in Cloud Storage Environments [34]

Figure 3. AES shows consistent low CPU usage even under high concurrency, while RSA and ECC demonstrate increasing overhead.

5. Comparative Analysis Table

A structured comparison of encryption algorithms is vital for understanding their relative advantages and limitations in the context of cloud storage. The comparative analysis includes performance indicators such as key size, encryption speed, security level, memory footprint, cloud compatibility, and algorithmic drawbacks. These parameters are essential when deciding upon an algorithm for a specific cloud environment—whether public, private, or hybrid. Symmetric algorithms such as AES and Blowfish typically offer faster execution and lower resource consumption, while asymmetric and advanced algorithms emphasize security robustness and specialized use cases. **Table 4** presents a side-by-side evaluation of the most widely adopted and emerging encryption techniques.

Table 4: Comparative Analysis of Major Encryption Algorithms in Cloud Storage

Parameter	AES-256	RSA-2048	ECC-256	Blowfish	RC5	Homomorphic
Type	Symmetric	Asymmetric	Asymmetric	Symmetric	Symmetric	Advanced
Key Size (bits)	256	2048	256	Up to 448	Variable	Large
Encryption Speed	High	Low	Moderate	Very High	High	Very Low
Security Level	Very High	Very High	Very High	Medium	Low–Medium	High
Memory Usage	Low	High	Low	Low	Very Low	Very High
Cloud Suitability	Excellent	Moderate	High	Good	Limited	Poor
Limitations	Key distribution	CPU intensive	Complexity in implementation	Aging algorithm	Weak security	Not practical

This comparative matrix highlights how AES continues to dominate in cloud applications due to its balance between performance and security [18], [21]. Blowfish, though fast, is gradually being phased out due to its aging cryptographic foundation and lack of modern resilience [21], [26]. RSA, while offering robust confidentiality, incurs substantial computational cost, rendering it suitable primarily for secure key exchanges and not for large-scale data encryption [22]. Emerging schemes such as ECC provide significant improvements in efficiency without compromising on security, particularly for cloud and mobile-integrated environments [19], [26]. RC5, due to its tunable block sizes and rounds, provides flexibility but lacks modern cryptographic strength [22]. Homomorphic encryption represents a futuristic approach that supports operations on encrypted data, which could revolutionize secure computing in cloud environments. However, current implementations are computationally intensive and impractical for broad deployment [27].

6. Real-World Application in Cloud Storage Platforms

The deployment of encryption algorithms in commercial cloud platforms is foundational to preserving data confidentiality and regulatory compliance. Leading providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and widely used consumer-oriented services like Dropbox, iCloud, and OneDrive have integrated robust cryptographic frameworks to meet growing security demands [35]. In AWS, encryption is embedded both at rest and in transit. Server-side encryption mechanisms, particularly SSE-S3 and SSE-KMS, use AES-256 by default. The infrastructure supports secure key management and allows integration with AWS Key Management Service (KMS) for centralized control of key rotation and auditing. For in-transit data protection, AWS leverages Transport Layer Security (TLS) protocols utilizing RSA and ECC for handshake encryption, thereby ensuring a multi-layered approach to data security in motion [36].

GCP adopts a default policy of encrypting all stored data using AES-256, while also supporting customer-managed and customer-supplied encryption keys. The platform further enables organizations to define custom cryptographic policies for granular control over access and rotation. The flexibility of Google's Cloud Key Management Service (Cloud KMS) plays a critical role in mitigating insider threats and enhancing compliance with privacy regulations [37]. Microsoft Azure follows a similar approach, offering storage service encryption that automatically encrypts data before persisting it to storage and decrypts it during retrieval. AES encryption underpins this service, combined with RSA and ECC support within Azure Key Vault for key lifecycle

management. Azure's architecture aligns with the NIST Cybersecurity Framework, delivering modularity for enterprise-grade security controls and incident response [38]. Beyond these enterprise-scale providers, mainstream services like Dropbox, iCloud, and OneDrive have integrated symmetric encryption methods—typically AES-256—for securing data at rest. RSA is often employed for secure key exchange mechanisms, particularly during data synchronization across multiple devices or while accessing data through browser-based sessions. These platforms emphasize usability without compromising confidentiality, enabling secure access across global networks [39]. The table 5 below summarizes the real-world encryption strategies adopted by major cloud platforms:

Table 5: Encryption Features and Key Management Capabilities Across Major Cloud Storage Platforms

Platform	Encryption at Rest	Encryption in Transit	Key Management	Cryptographic Standards
AWS	AES-256 (SSE-S3, KMS)	TLS with RSA/ECC	AWS KMS, custom key support	AES, RSA, ECC
GCP	AES-256 (default)	TLS with RSA/ECC	Cloud KMS, BYOK/CSK options	AES, RSA, ECC
Microsoft Azure	AES-256 (Storage Service Encryption)	TLS with RSA/ECC	Azure Key Vault	AES, RSA, ECC
Dropbox, iCloud, OneDrive	AES-256	TLS with RSA/ECC	Limited custom key control	AES, RSA

This comparative assessment illustrates that while AES-256 remains the industry standard for symmetric encryption, the integration of RSA and ECC for asymmetric operations reflects the evolving need for both performance efficiency and cryptographic strength. As user demands grow and compliance frameworks evolve, these platforms continually refine their encryption methodologies to safeguard data across hybrid and multi-cloud ecosystems [38].

7. Challenges in Encryption for Cloud Storage

Cloud encryption, while essential for data protection, faces several critical challenges. Key management remains a complex task, especially when comparing centralized and decentralized models. Centralized approaches are easier to manage but risk single points of failure, whereas decentralized systems improve security but add coordination complexity [4], [7]. Additionally, implementing key rotation and revocation demands robust automation and synchronization mechanisms to avoid data access disruptions [8]. A significant trade-off exists between encryption strength and system performance. Algorithms with high security often increase CPU and memory usage, which may hinder scalability in real-time or resource-constrained cloud environments [40]. Furthermore, advanced encryption methods like homomorphic encryption are still impractical due to their computational overhead and limited platform support [33].

Regulatory compliance with frameworks such as GDPR and HIPAA also imposes constraints, requiring encryption standards that align with legal mandates. Finally, client-side encryption—though secure—introduces integration burdens, as it shifts encryption responsibility to users or developers, complicating implementation and usability [35].

8. Future Research Directions

As cloud adoption accelerates, future research must focus on advancing encryption strategies to stay ahead of emerging threats. Quantum-safe encryption algorithms are essential to defend against the looming risks posed by quantum computing. Homomorphic encryption, though promising, requires breakthroughs to become practical for real-time, searchable operations in cloud environments. AI-driven key management and threat detection could offer dynamic, context-aware security models. Lightweight encryption tailored for cloud IoT and edge computing is crucial for balancing speed and protection. Lastly, developing cross-cloud key federation mechanisms will enable seamless and secure interoperability between multiple cloud providers.

9. Conclusion

This study comprehensively analyzed various encryption algorithms to evaluate their suitability for securing cloud storage environments. Through a structured comparative framework, both symmetric and asymmetric algorithms were examined alongside emerging advanced cryptographic techniques. The analysis revealed that AES and ECC

currently offer the most balanced trade-off between performance, computational efficiency, and strong security, making them highly suitable for a wide range of cloud storage applications. AES excels in speed and resource efficiency, particularly for server-side encryption, while ECC provides equivalent security with smaller key sizes, making it ideal for mobile and resource-constrained environments. RSA, despite its long-standing reliability and widespread use, poses significant performance limitations due to its computational overhead and high memory consumption, rendering it less optimal for real-time or large-scale cloud deployments. On the other hand, modern encryption methods like homomorphic and post-quantum encryption present promising innovations but are not yet mature enough for mainstream cloud use due to complexity, overhead, and scalability issues. Ultimately, the choice of encryption algorithm must align with specific use-case requirements, including regulatory compliance, user load, access patterns, and data sensitivity. In multi-tenant environments, scalability and key management flexibility become crucial, whereas mobile-first platforms may prioritize lightweight encryption. As cloud architectures evolve, continuous assessment of cryptographic solutions will be essential to ensure robust and future-proof data protection. This study serves as a practical guide for researchers and cloud architects to make informed encryption choices tailored to their operational and security objectives.

REFERENCES

[1] A. Keshavarzi, A. T. Haghighat, and M. Bohlouli, "Research challenges and prospective business impacts of cloud computing: A survey," in *Proc. 2013 IEEE 7th Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. (IDAACS)*, Berlin, Germany, Sept. 2013, vol. 2, pp. 731–736.

[2] M. E. Moudni and E. Ziyati, "Advances and challenges in cloud data storage security: A systematic review," *Int. J. Saf. Secur. Eng.*, vol. 15, no. 4, 2025.

[3] B. T. Rao, "A study on data storage security issues in cloud computing," *Procedia Comput. Sci.*, vol. 92, pp. 128–135, 2016.

[4] B. John, *The Role of Machine Learning in Preventing Cyber Attacks on Cloud Platforms*, 2025.

[5] K. Chitreddy, A. M. Anthony, C. M. Bandaru, and O. Abiona, "Information security in the cloud: Emerging trends and challenges," *Int. J. Commun. Netw. Syst. Sci.*, vol. 17, no. 5, pp. 69–80, 2024.

[6] R. Buyya, "Introduction to the IEEE Transactions on Cloud Computing," *IEEE Trans. Cloud Comput.*, vol. 1, no. 1, pp. 3–21, 2013.

[7] K. Kamatchi and E. Uma, "Insights into user behavioral-based insider threat detection: Systematic review," *Int. J. Inf. Secur.*, vol. 24, no. 2, p. 88, 2025.

[8] C. K. Ejeofobiri, J. E. Ike, M. D. Salawudeen, D. A. Atakora, J. D. Kessie, and T. Onibokun, *Securing Cloud Databases Using AI and Attribute-Based Encryption*, 2025.

[9] P. Prajapati and P. Shah, "A review on secure data deduplication: Cloud storage security issue," *J. King Saud Univ.–Comput. Inf. Sci.*, vol. 34, no. 7, pp. 3996–4007, 2022.

[10] M. N. Ul Haq and N. Kumar, "A novel data classification-based scheme for cloud data security using various cryptographic algorithms," *Int. Rev. Appl. Sci. Eng.*, 2021.

[11] M. M. Sindhu and M. R. Divya, "Ensuring data integrity in cloud computing: A review of threats and protection strategies," *Int. J. Adv. Res. Interdiscip. Sci. Endeavours*, vol. 2, no. 5, pp. 673–689, 2025

[12] O. M. C. Osazuwa, O. Mitchell, and C. Osazuwa, "Confidentiality, integrity, and availability in network systems: A review of related literature," *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 12, pp. 1946–1953, 2023.

[13] P. Goswami, N. Faujdar, S. Debnath, A. K. Khan, and G. Singh, "Investigation on storage level data integrity strategies in cloud computing: Classification, security obstructions, challenges and vulnerability," *J. Cloud Comput.*, vol. 13, no. 1, p. 45, 2024.

[14] M. Aminzade, "Confidentiality, integrity and availability–finding a balanced IT framework," *Netw. Secur.*, vol. 2018, no. 5, pp. 9–11, 2018.

[15] A. Musa and A. Mahmood, "Client-side cryptography based security for cloud computing system," in *Proc. 2021 Int. Conf. Artif. Intell. Smart Syst. (ICAIS)*, Coimbatore, India, Mar. 2021, pp. 594–600.

[16] S. Li, C. Xu, and Y. Zhang, "CSED: Client-side encrypted deduplication scheme based on proofs of ownership for cloud storage," *J. Inf. Secur. Appl.*, vol. 46, pp. 250–258, 2019.

[17] M. da Rocha, D. C. G. Valadares, A. Perkusich, K. C. Gorgonio, R. T. Pagno, and N. C. Will, "Secure cloud storage with client-side encryption using a trusted execution environment," *arXiv preprint arXiv:2003.04163*, 2020.

[18] D. Commey, S. Griffith, and J. Dzisi, "Performance comparison of 3DES, AES, Blowfish and RSA for dataset classification and encryption in cloud data storage," *Int. J. Comput. Appl.*, vol. 177, no. 40, pp. 17–22, 2020.

[19] P. Panahi, C. Bayılmış, U. Çavuşoğlu, and S. Kaçar, "Performance evaluation of lightweight encryption algorithms for IoT-based applications," *Arab. J. Sci. Eng.*, vol. 46, no. 4, pp. 4015–4037, 2021.

[20] A. R. Wani, Q. P. Rana, and N. Pandey, "Performance evaluation and analysis of advanced symmetric key cryptographic algorithms for cloud computing security," in *Soft Computing: Theories and Applications: Proc. SoCTA 2017*, Singapore: Springer, pp. 261–271, 2018.

[21] K. Patel, "Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files," *Int. J. Inf. Technol.*, vol. 11, no. 4, pp. 813–819, 2019.

[22] P. Jindal and B. Singh, "Analyzing the security-performance tradeoff in block ciphers," in *Proc. Int. Conf. Comput., Commun. Autom.*, May 2015, pp. 326–331.

[23] H. A. Abughali and U. Kose, "Image encryption techniques: A survey," in *Proc. 2024 Int. Jordanian Cybersecurity Conf. (IJCC)*, Dec. 2024, pp. 62–69.

[24] S. Kumar and D. Kumar, "Securing of cloud storage data using hybrid AES-ECC cryptographic approach," *J. Mobile Multimed.*, vol. 19, no. 2, pp. 363–388, 2023.
[25] I. Peter, *Performance Analysis of AES, RSA, and ECC in Real-Time Applications*, 2025.
[26] R. Bhanot and R. Hans, "A review and comparative analysis of various encryption algorithms," *Int. J. Secur. Its Appl.*, vol. 9, no. 4, pp. 289–306, 2015.
[27] D. Shivaramakrishna and M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control," *Alex. Eng. J.*, vol. 84, pp. 275–284, 2023.
[28] A. Epishkina and V. Ermakov, "Homomorphic encryption for data protection in cloud computing," *J. Comput. Virol. Hacking Tech.*, vol. 21, no. 1, p. 8, 2025.
[29] R. Awadallah and A. Samsudin, "Homomorphic encryption for cloud computing and its challenges," in *Proc. 2020 IEEE 7th Int. Conf. Eng. Technol. Appl. Sci. (ICETAS)*, Dec. 2020, pp. 1–6.
[30] J. S. Murthy and K. G. Srinivasa, "SCiphered clouds and quantum secrets: Navigating secure information flow with emerging encryption technologies," in *Cloud Security*, Chapman and Hall/CRC, 2024, pp. 216–237.
[31] H. C. Ukwuoma, G. Arome, A. Thompson, and B. K. Alese, "Post-quantum cryptography-driven security framework for cloud computing," *Open Comput. Sci.*, vol. 12, no. 1, pp. 142–153, 2022.
[32] T. L. Moore, S. S. Conlon, A. U. Hewarathna, and A. B. Mailewa, "Encryption methods and key management services for secure cloud computing: A review," *Comput. Syst. Sci. Eng.*, vol. 46, no. 3, pp. 967–984, 2022.
[33] D. Patel, B. Patel, J. Vasa, and M. Patel, "A comparison of the key size and security level of the ECC and RSA algorithms with a focus on cloud/fog computing," in *Int. Conf. Inf. Commun. Technol. Intell. Syst.*, Singapore: Springer Nature, Apr. 2023, pp. 43–53.
[34] D. Shivaramakrishna and M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control," *Alex. Eng. J.*, vol. 84, pp. 275–284, 2023.
[35] W. Almuseelem, "Enhance the security of data based on server-side encryption in a cloud environment," *Int. J. Online Biomed. Eng.*, vol. 21, no. 8, 2025.
[36] A. Anthony, *AWS: Security Best Practices on AWS: Learn to Secure Your Data, Servers, and Applications with AWS*. Birmingham, UK: Packt Publishing Ltd., 2018.
[37] M. Saminathan, *Mastering Big Data Engineering: AWS, GCP, & Azure Showdown*. Libertatem Media Private Ltd., 2024.
[38] P. Udayakumar, "Design and deploy a protect solution: Part 2," in *Design and Deploy a Secure Azure Environment: Mapping the NIST Cybersecurity Framework to Azure Services*, Berkeley, CA: Apress, 2023, pp. 281–365.
[39] J. Mwikya, J. Karani, and J. Obura, "Secure management of encryption keys for small and medium enterprises in Africa: A comparative study," in *Proc. 5th KyU Int. Conf.*, 2022.
[40] S. Rana, F. K. Parast, B. Kelly, Y. Wang, and K. B. Kent, "A comprehensive survey of cryptography key management systems," *J. Inf. Secur. Appl.*, vol. 78, p. 103607, 2023