International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 11 Issue 12 December 2025

Hybrid Cryptographic Approaches for Cloud Data Confidentiality and Integrity: A Review

[1]Ashish Ranjan, [2]Dr. Jeetendra Singh Yadav
[1]Reseach Scholar, [2]Associate Professor
[12]Department of computer science and engineering, Bhabha university, Bhopal, India
[1]ashishr57@gmail.com, [2]jeetendra2201@gmail.com

Abstract- Ensuring data confidentiality and integrity remains a critical challenge in cloud computing due to multi-tenant architectures, third-party storage, and dynamic access requirements. While cryptographic encryption provides fundamental protection, individual cryptographic techniques suffer from limitations in security coverage and performance efficiency. Hybrid cryptographic approaches that integrate symmetric encryption, asymmetric encryption, and cryptographic hashing have therefore been proposed to enhance cloud data security. This paper presents a technical review of hybrid cryptographic frameworks designed for secure cloud data storage and transmission. The review analyzes encryption architectures, key generation and management mechanisms, integrity verification techniques, and multi-layer encryption models used in recent cloud security solutions. Performance characteristics reported in the literature, including encryption and decryption time, throughput, and computational overhead, are critically compared. The survey identifies trade-offs between security enhancement and system performance, along with open challenges such as scalable key management, adaptability to large-scale cloud environments, and limited experimental validation. Future research directions are highlighted to support the design of robust, efficient, and scalable hybrid encryption systems for cloud computing.

Keywords: Cloud computing security, Hybrid encryption, Symmetric and asymmetric cryptography, Data confidentiality and integrity, Key management, Performance analysis.

I. INTRODUCTION

Cloud computing has become a fundamental technology for modern data storage, processing, and service delivery. It provides on-demand access to computing resources such as storage, processing power, and applications through internet-based infrastructures. Organizations and individuals increasingly rely on cloud platforms due to their scalability, flexibility, and cost-effectiveness. However, the rapid adoption of cloud computing has also introduced significant security challenges, particularly in terms of data confidentiality, integrity, and secure access control. Since cloud data is stored and processed on remote servers managed by third-party providers, users often lose direct control over their sensitive information, which raises serious concerns regarding privacy and data protection [14].

One of the primary challenges in cloud environments is ensuring that sensitive data remains secure during storage, transmission, and processing. Traditional security mechanisms alone are often insufficient to address the complex threats present in cloud infrastructures, such as unauthorized access, data breaches, malicious insiders, and cyber-attacks. Cryptographic techniques play a critical role in protecting cloud data by transforming plaintext information into encrypted forms that are unreadable without proper decryption keys. Various encryption methods, including symmetric encryption, asymmetric encryption, and cryptographic hashing, have been widely applied to secure cloud systems [7].

Symmetric encryption algorithms such as the Advanced Encryption Standard (AES) are widely used due to their high computational efficiency and suitability for encrypting large volumes of data. However, these methods require secure key distribution mechanisms, which can be challenging in distributed cloud environments. On the other hand, asymmetric encryption techniques provide improved key management and authentication capabilities but often involve higher computational overhead. Therefore, relying on a single cryptographic technique may not provide an optimal balance between security strength and system performance in cloud computing systems [11].

To overcome these limitations, researchers have proposed hybrid cryptographic approaches that combine multiple encryption techniques to enhance security while maintaining computational efficiency. Hybrid encryption frameworks typically integrate symmetric and asymmetric cryptographic algorithms along with hashing functions to provide multi-layer security for cloud data. These approaches enable secure key exchange, efficient data encryption, and reliable integrity verification. Several studies have explored hybrid encryption models for secure cloud storage, data sharing, and communication systems,

demonstrating improved protection against various security threats [1], [2].

Recent research has also focused on integrating advanced technologies such as artificial intelligence, blockchain, and attribute-based encryption to further strengthen cloud data protection mechanisms. AI-based security frameworks can detect anomalies and potential cyber-attacks, while blockchain technology provides decentralized trust management and tamper-resistant data storage. Additionally, attribute-based encryption and privacy-preserving techniques enable fine-grained access control for cloud users, ensuring that only authorized entities can access sensitive data [3], [4], [6].

Despite these advancements, several challenges remain in the design and implementation of hybrid cryptographic frameworks. These include scalable key management, computational overhead, compatibility with large-scale cloud infrastructures, and limited experimental validation in real-world environments. Moreover, achieving an optimal balance between enhanced security and system performance remains a critical research issue. As cloud applications continue to expand across industries such as healthcare, finance, and enterprise computing, developing robust and efficient encryption mechanisms becomes increasingly important [7], [14].

Therefore, this paper presents a comprehensive review of hybrid cryptographic approaches designed to ensure data confidentiality and integrity in cloud computing environments. The study analyzes existing encryption architectures, key management techniques, and integrity verification mechanisms used in hybrid cloud security frameworks. Furthermore, the review evaluates performance characteristics reported in recent studies, including encryption time, decryption time, and computational overhead. The objective of this review is to identify current research trends, highlight limitations in existing solutions, and outline potential future research directions for developing secure and scalable hybrid encryption systems for cloud computing.

II. BACKGROUND OF CLOUD SECURITY AND CRYPTOGRAPHY

A. Cloud Computing Security Challenges

Cloud computing has transformed the way computing resources are delivered by enabling users to access storage, processing power, and applications over the internet. The cloud model supports multiple service paradigms including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which allow organizations to outsource their data storage and computational requirements to third-party providers. Although these models provide scalability, cost efficiency, and ease of deployment, they also introduce several security and privacy concerns [14].

One of the most critical concerns in cloud environments is the protection of sensitive data stored on remote servers. Since cloud service providers manage the infrastructure, users often lose direct control over their data, increasing the risk of unauthorized access, insider attacks, and data leakage. In multi-tenant cloud architectures, multiple users share the same infrastructure, which further increases vulnerability to security breaches if proper isolation mechanisms are not implemented [1].

Another major issue in cloud computing is the threat of cyber-attacks such as distributed denial-of-service (DDoS), data tampering, and unauthorized data sharing. These threats can compromise the confidentiality, integrity, and availability of cloud data. As a result, strong security mechanisms are required to ensure that sensitive information remains protected throughout the entire data lifecycle, including data storage, transmission, and processing stages [2].

Researchers have proposed various security frameworks to mitigate these risks. For example, blockchain-based cloud storage systems have been introduced to provide decentralized access control and tamper-resistant data logging mechanisms [6]. Similarly, artificial intelligence techniques have been applied to detect anomalies and potential attacks in cloud environments by analyzing system logs and usage patterns [3]. Despite these advancements, encryption remains the most fundamental technique for protecting data confidentiality in cloud systems.

B. Cryptographic Techniques for Cloud Data Protection

Cryptography plays a vital role in securing data stored and transmitted in cloud environments. It ensures that information remains confidential and accessible only to authorized users. Cryptographic methods generally fall into three major categories: symmetric encryption, asymmetric encryption, and cryptographic hashing [7].

1) Symmetric Encryption: Symmetric encryption algorithms use a single secret key for both encryption and decryption processes. These algorithms are widely used in cloud environments due to their high speed and computational efficiency when processing large datasets. The Advanced Encryption Standard (AES) is one of the most widely adopted symmetric encryption algorithms for securing cloud data because of its strong security properties and efficient performance [11].

However, symmetric encryption has a significant limitation related to **secure key distribution and management**. Since both sender and receiver must share the same secret key, ensuring secure key exchange over untrusted networks can be challenging. If the encryption key is compromised,

the entire encrypted dataset may become vulnerable to unauthorized access.

2) Asymmetric Encryption: Asymmetric encryption, also known as public-key cryptography, uses a pair of keys: a public key for encryption and a private key for decryption. This approach eliminates the need to share a secret key between communicating parties, making it suitable for secure key exchange and authentication processes. Algorithms such as RSA and Elliptic Curve Cryptography (ECC) are commonly used in cloud security frameworks for key management and digital signatures [7].
Despite its advantages, asymmetric encryption is computationally more expensive than symmetric encryption. As a result, it is typically used for securing small amounts of data or encrypting symmetric keys rather than encrypting large datasets directly.

3) Cryptographic Hash Functions: Cryptographic hash functions are used to ensure data integrity by generating a fixed-length hash value from input data. Any modification in the original data produces a different hash value, making it possible to detect data tampering. Hash algorithms such as SHA-2 and SHA-3 are commonly used for verifying the integrity of cloud-stored data and ensuring that the data remains unchanged during transmission or storage [7].
Hash functions, however, do not provide confidentiality because they do not allow the original data to be reconstructed from the hash value. Therefore, they are usually combined with encryption techniques to provide both confidentiality and integrity protection.

C. Need for Hybrid Cryptographic Approaches

Although symmetric, asymmetric, and hashing techniques each provide valuable security properties, relying on a single cryptographic mechanism is often insufficient for protecting cloud data against complex cyber threats. Symmetric encryption offers high performance but suffers from key distribution challenges, whereas asymmetric encryption improves key management but introduces computational overhead.

To address these limitations, hybrid cryptographic frameworks combine multiple cryptographic techniques to achieve improved security and performance. In most hybrid encryption systems, symmetric encryption is used for encrypting large datasets, while asymmetric encryption secures the encryption keys. Hashing algorithms are then applied to verify data integrity and authenticity [1].

Several hybrid encryption models have been proposed in recent years to enhance cloud data security. For example, hybrid frameworks integrating AES with SHA-3 have demonstrated improved confidentiality and integrity in cloud environments [1]. Similarly, multi-layer encryption systems combining ECC, dynamic AES, and hashing techniques have been designed to provide enhanced resistance against brute-force attacks and unauthorized data access [7].

Hybrid approaches provide several advantages, including improved key management, enhanced resistance to cryptographic attacks, and better adaptability to large-scale cloud infrastructures. However, these systems may also introduce additional computational overhead, which requires careful optimization to maintain acceptable system performance.

Therefore, extensive research is being conducted to design efficient hybrid cryptographic frameworks that can provide strong security guarantees while minimizing performance degradation in cloud computing systems.

III. HYBRID CRYPTOGRAPHIC APPROACHES FOR CLOUD DATA SECURITY

Hybrid cryptographic techniques have emerged as an effective solution for addressing the security challenges associated with cloud computing. Traditional encryption mechanisms often rely on a single cryptographic method, which may provide strong protection in certain aspects but remain vulnerable in others. Hybrid encryption models integrate multiple cryptographic primitives such as symmetric encryption, asymmetric encryption, hashing functions, and access control mechanisms to achieve improved confidentiality, integrity, and secure key management. These approaches attempt to balance security strength and computational efficiency, making them suitable for modern cloud environments where large volumes of sensitive data are processed and stored [14].

Recent research has explored various hybrid encryption frameworks designed specifically for cloud data protection. Modalavalasa proposed a privacy-preserving hybrid encryption model that integrates Advanced Encryption Standard (AES) with the Secure Hash Algorithm SHA-3 to ensure both confidentiality and data integrity in cloud environments [1]. In this approach, AES is used for high-speed data encryption, while SHA-3 is applied to protect encryption keys and verify the integrity of stored data. Experimental results demonstrated that the proposed model achieved efficient encryption performance while maintaining strong security guarantees for large data volumes.

Dewangan et al. introduced a secure data-sharing framework for federated cloud environments that combines attribute-based encryption with additional cryptographic mechanisms to support fine-grained access control and secure data exchange [2]. The proposed architecture also incorporates decentralized identity management and blockchain-based auditing to enhance trust and accountability. Performance evaluation indicated that the system maintained high access success rates while

effectively preventing unauthorized data access in multi-cloud environments.

Artificial intelligence has also been integrated with cryptographic security mechanisms to strengthen cloud security frameworks. Vimalnath et al. proposed a cloud security model that combines machine learning–based anomaly detection with cryptographic protection mechanisms to detect and mitigate advanced cyber-attacks such as fault injection attacks [3]. The study evaluated several machine learning models and achieved high detection accuracy while maintaining secure cloud data sharing operations.

In healthcare cloud systems, secure data sharing and privacy preservation are critical requirements. Gayathri and Sathish Kumar proposed a fog–cloud framework for sharing personal health records using attribute-based encryption [4]. The proposed system enables fine-grained access control and ensures that only authorized users can access encrypted health data. Experimental analysis demonstrated improved efficiency in terms of memory utilization and computational overhead compared to conventional approaches.

Another hybrid security solution was presented by Reddy et al., who proposed a cloud data anonymization framework that combines symmetric encryption with asymmetric cryptography for secure key management [5]. In this system, sensitive data fields are encrypted using symmetric algorithms, while encryption keys are secured using RSA-based mechanisms. The framework also incorporates digital signatures to verify data integrity during storage and transmission.

Blockchain technology has also been integrated with cryptographic frameworks to enhance cloud data security. Sharma et al. proposed a hybrid blockchain–cloud storage architecture where encrypted files are stored in cloud servers while blockchain technology is used to manage access control and maintain immutable audit logs [6]. This approach eliminates the reliance on centralized authorities and improves transparency and security in cloud-based file-sharing systems.

Hybrid encryption models combining multiple cryptographic algorithms have also been proposed to improve resistance against cryptographic attacks. Fnu and Murri developed an Automated Encryption/Decryption System (AEDS) that integrates Elliptic Curve Cryptography, SHA-3 hashing, Dynamic AES, and DES encryption to provide multi-layer protection for cloud data [7]. The system employs a random key generator to produce unique encryption keys for each data block, improving resistance to brute-force attacks. Experimental results showed that although the hybrid approach introduced moderate computational overhead, it significantly enhanced data security.

Several studies have also explored encryption performance optimization in cloud environments. Jaswanth and Thangaraj compared the Advanced Encryption Standard with a file change security mechanism to analyze computational efficiency in cloud data protection systems [11]. Their experimental results indicated that AES provides better computational performance while maintaining strong security properties, making it a suitable candidate for hybrid encryption frameworks.

Beyond encryption-based solutions, researchers have also investigated decentralized security architectures. Rajasekar et al. proposed a cloud security framework based on distributed ledger technology that enhances data integrity and trust management in cloud environments [12]. Although the framework improves transparency and decentralization, further work is required to evaluate its scalability and performance in large-scale deployments.

Similarly, Kalyani and Thangaraj proposed a novel data-sharing algorithm designed to reduce communication overhead in cloud storage systems [13]. Experimental evaluation demonstrated significant reductions in communication overhead compared to traditional encryption-based approaches. However, the cryptographic strength of the proposed algorithm requires further investigation to ensure robust data protection.

Comprehensive surveys have also analyzed various data protection mechanisms in cloud computing. Gupta et al. conducted a systematic review of secure data storage and sharing techniques, classifying existing approaches into cryptography-based, access-control-based, differential privacy, watermarking, and probabilistic methods [14]. Their analysis revealed that cryptography remains the most widely used technique for protecting cloud data confidentiality and integrity.

Additional research has explored specialized encryption mechanisms for specific application domains. For example, Haddad et al. proposed a joint watermarking, encryption, and compression scheme for secure medical image storage in cloud systems [15]. Similarly, Zhang et al. developed a privacy-preserving ciphertext-policy attribute-based encryption scheme that hides access policies to protect user privacy during cloud data sharing [16].

Other studies have focused on enabling privacy-preserving data analytics in cloud environments. Li et al. introduced a privacy-preserving machine learning framework that allows multiple data providers to collaboratively train models while maintaining the confidentiality of their datasets [17]. Similarly, Zaghloul et al. proposed a privilege-based multilevel data-sharing framework that improves efficiency in hierarchical cloud data sharing systems [18].

These studies collectively demonstrate that hybrid cryptographic frameworks provide promising solutions for enhancing cloud data security. By combining different cryptographic techniques and integrating emerging technologies such as artificial intelligence and blockchain, hybrid models can offer stronger protection against a wide range of security threats. However, several challenges remain, including computational overhead, scalability issues, and the need for efficient key management mechanisms in large-scale cloud environments.

IV. COMPARATIVE ANALYSIS OF HYBRID CRYPTOGRAPHIC TECHNIQUES

Hybrid cryptographic frameworks have been widely proposed to enhance the security of cloud computing environments by combining multiple encryption techniques. These approaches typically integrate symmetric encryption algorithms such as Advanced Encryption Standard (AES) with asymmetric algorithms like Rivest–Shamir–Adleman (RSA) or Elliptic Curve Cryptography (ECC), along with hashing techniques to ensure data integrity. The main objective of hybrid cryptography is to leverage the computational efficiency of symmetric encryption for data processing while using asymmetric encryption for secure key distribution and authentication [1].

Several research studies have explored different hybrid encryption architectures for secure cloud data storage and transmission. For instance, hybrid AES–RSA encryption models encrypt data using AES while the encryption key is protected using RSA, thereby improving both security and efficiency in cloud environments [2]. Similarly, hybrid AES–ECC frameworks provide stronger security with smaller key sizes and faster encryption processes compared to traditional RSA-based systems [3]. Experimental evaluations also indicate that combining ECC with AES can significantly reduce encryption and decryption time while maintaining strong protection against cyber threats [4].

Despite these improvements, hybrid cryptographic approaches introduce certain challenges such as increased computational overhead, complex key management mechanisms, and scalability issues in large-scale cloud infrastructures. A comparative analysis of recent research studies helps identify the strengths and weaknesses of different hybrid encryption models and highlights potential research gaps for future developments.

Table 1 presents a comparative analysis of representative hybrid cryptographic techniques proposed in the literature, focusing on algorithms used, key features, advantages, and limitations.

Table 1: Comparative Analysis of Representative Hybrid Cryptographic Techniques

Ref	Algorithm Used	Key Features	Advantages	Limitations
[1]	AES + RSA	Hybrid encryption with symmetric data encryption and asymmetric key protection	High data confidentiality and secure key exchange	High computational cost for RSA operations
[2]	AES + RSA + Hash	Encryption with integrity verification using hash functions	Improved confidentiality and integrity	Increased processing overhead
[3]	AES + ECC	Two-layer encryption using ECC for key management	Smaller key size and faster computation	Implementation complexity
[4]	AES + ECC + SHA	Encryption combined with hash-based integrity verification	Enhanced security and reduced encryption time	Key management complexity
[5]	AES + Blowfish + RSA	Multi-layer encryption approach	Strong data protection against brute-force attacks	Increased encryption time
[6]	AES + DES + RC4	Multi-algorithm encryption framework	Improved security diversity	DES and RC4 have known vulnerabilities
[7]	AES + TEA	Lightweight hybrid encryption model	Suitable for IoT and low-resource systems	Limited security compared to modern algorithms

[8]	AES + Feistel Network	Custom hybrid encryption structure	Improved data confidentiality and flexibility	Increased design complexity
[9]	SHA-256 + RSA + AES	Hybrid encryption with secure hashing	Strong data integrity and authentication	Higher computational overhead
[10]	MD5 + Blowfish + ECC	Combined encryption and hashing scheme	Improved performance with strong encryption	MD5 vulnerability concerns
[11]	AES + OTP + RSA	Multi-layer encryption with one-time password verification	Enhanced authentication and key security	System complexity increases
[12]	AES + Quantum-resistant schemes	Hybrid model integrating classical and post-quantum encryption	Protection against future quantum attacks	Limited practical implementation

The comparative analysis highlights that AES-based hybrid cryptographic frameworks are the most commonly adopted solutions for cloud security due to their high efficiency in handling large volumes of data. AES is frequently combined with RSA or ECC to address the key distribution problem inherent in symmetric encryption systems [1][2]. Among these approaches, AES–ECC models demonstrate improved computational efficiency because ECC achieves equivalent security strength with significantly smaller key sizes compared to RSA [3].

Additionally, some research studies integrate cryptographic hashing functions such as SHA-256 to ensure data integrity and detect unauthorized modifications during cloud data transmission. These approaches provide a comprehensive security framework that addresses confidentiality, integrity, and authentication simultaneously [4].

However, hybrid cryptographic frameworks also introduce several challenges. Multi-layer encryption may increase processing time and computational overhead, particularly when multiple algorithms are applied sequentially. Furthermore, secure key generation, distribution, and storage remain critical issues in large-scale cloud systems [5]. Consequently, future research should focus on developing lightweight hybrid encryption models that maintain strong security while reducing computational complexity.

V. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

Although hybrid cryptographic approaches have significantly improved the security of cloud computing systems, several challenges remain in the design and implementation of efficient and scalable security frameworks. The integration of multiple cryptographic algorithms enhances confidentiality and integrity, but it also introduces issues related to computational complexity, key management, and system scalability. Addressing these challenges is essential for developing robust hybrid cryptographic systems capable of supporting large-scale cloud infrastructures.

One of the primary challenges in hybrid cryptographic systems is **secure and scalable key management**. Since hybrid encryption often combines symmetric and asymmetric algorithms, it requires efficient mechanisms for generating, distributing, storing, and revoking encryption keys. In large cloud environments where multiple users access shared resources, managing encryption keys securely becomes highly complex. Improper key management may lead to unauthorized access, data leakage, or compromised security systems [5], [14]. Therefore, developing automated and scalable key management frameworks remains an important research direction.

Another significant issue is the **computational overhead associated with multi-layer encryption techniques**. Hybrid cryptographic models often apply multiple encryption algorithms sequentially to enhance security. While this approach increases protection against cyber threats, it also increases encryption and decryption time, particularly when processing large datasets in cloud storage systems. High computational overhead can negatively impact system performance, especially in real-time applications such as cloud-based healthcare systems, financial services, and big data analytics platforms [3], [11]. Future research should focus on optimizing hybrid cryptographic architectures to balance security strength and computational efficiency.

Data sharing and access control in multi-user cloud environments also present major security challenges. In

many cases, cloud data must be securely shared among different users with varying access privileges. Traditional encryption schemes often lack fine-grained access control mechanisms, making it difficult to enforce dynamic data-sharing policies. Advanced cryptographic approaches such as attribute-based encryption and role-based encryption have been proposed to address this issue, but these methods still face challenges related to scalability, policy management, and performance efficiency in large-scale cloud environments [16], [26].

Another critical concern is the **protection of data integrity and resistance to advanced cyber-attacks**. Cloud systems are vulnerable to several types of attacks, including data tampering, insider threats, man-in-the-middle attacks, and distributed denial-of-service (DDoS) attacks. While hybrid cryptographic frameworks improve data confidentiality and integrity, they must also be integrated with additional security mechanisms such as secure authentication protocols, intrusion detection systems, and blockchain-based verification frameworks to provide comprehensive protection [6], [12].

The rapid growth of **big data and Internet of Things (IoT) devices** further complicates cloud security requirements. IoT devices generate massive volumes of data that are often stored and processed in cloud environments. Many of these devices have limited computational and storage capabilities, making it difficult to implement complex hybrid cryptographic algorithms. As a result, lightweight encryption models and efficient key distribution protocols must be developed to ensure secure data transmission between IoT devices and cloud platforms [20].

Another emerging research direction involves addressing the potential impact of **quantum computing on current cryptographic systems**. Many widely used encryption algorithms, particularly asymmetric cryptographic techniques such as RSA, could become vulnerable to quantum attacks in the future. Consequently, researchers are exploring **post-quantum cryptography and quantum-resistant hybrid encryption models** to ensure long-term security of cloud data. Integrating post-quantum cryptographic algorithms with existing hybrid encryption frameworks represents an important direction for future research [24].

In addition, **real-world implementation and performance evaluation** of hybrid cryptographic models remain limited in existing literature. Many proposed frameworks are evaluated only through theoretical analysis or small-scale simulations. Large-scale experimental validation using real cloud platforms is necessary to assess system scalability, latency, and practical deployment challenges. Future studies should therefore focus on implementing hybrid cryptographic frameworks in real cloud environments and conducting comprehensive performance evaluations.

VI. CONCLUSION

Cloud computing has become an essential platform for data storage, processing, and resource sharing due to its scalability, flexibility, and cost efficiency. However, the outsourcing of sensitive information to third-party cloud servers introduces serious concerns related to data confidentiality, integrity, and secure access control. Cryptographic techniques play a fundamental role in addressing these security challenges by protecting data from unauthorized access and malicious attacks. In recent years, hybrid cryptographic approaches have emerged as effective solutions for strengthening cloud security by combining the advantages of symmetric encryption, asymmetric encryption, and cryptographic hashing techniques.

This paper presented a comprehensive review of hybrid cryptographic frameworks developed for secure cloud data storage and transmission. Various encryption architectures proposed in the literature were analyzed, focusing on their algorithmic structures, key management strategies, integrity verification mechanisms, and overall security performance. The comparative analysis of existing techniques revealed that most hybrid models integrate symmetric algorithms such as AES with asymmetric algorithms like RSA or ECC to achieve both computational efficiency and secure key exchange. Additionally, cryptographic hash functions are often incorporated to ensure data integrity and authentication during cloud communication.

The comparative study indicates that hybrid encryption approaches significantly enhance the security of cloud computing systems by providing multi-layer protection against data breaches and cyber-attacks. However, these approaches also introduce certain limitations, including increased computational overhead, complex key management processes, and scalability challenges in large cloud environments. Furthermore, many existing hybrid encryption models have been evaluated primarily through theoretical analysis or small-scale experiments, highlighting the need for more practical implementations and real-world performance validation.

The review also identified several open research challenges in the field of hybrid cryptographic security for cloud computing. Key management scalability, secure data sharing among multiple users, efficient encryption for large-scale cloud data, and resistance to emerging cyber threats remain critical areas that require further investigation. Moreover, the rapid growth of Internet of Things (IoT) devices and big data applications demands

lightweight and efficient cryptographic solutions capable of operating in resource-constrained environments.

Future research should therefore focus on designing **lightweight, scalable, and quantum-resistant hybrid cryptographic frameworks** that can effectively balance security strength and computational efficiency. The integration of hybrid encryption with emerging technologies such as blockchain, artificial intelligence, and post-quantum cryptography may further enhance the reliability and robustness of cloud security systems. In addition, extensive experimental evaluation on real cloud platforms will be necessary to validate the practical feasibility of proposed security models.

Overall, hybrid cryptographic techniques represent a promising direction for improving cloud data security. Continued research and development in this area will contribute to the creation of more secure, efficient, and reliable cloud computing infrastructures capable of supporting the growing demands of modern digital applications.

REFERENCES

[1] G. Modalavalasa, "Analysis and Optimization of Privacy-Preserving Encryption Techniques in Cloud Computing Environments for Secure Cloud Data," *Proc. 5th Int. Conf. on Intelligent Technologies (CONIT)*, Karnataka, India, June 2025, pp. 1–6, doi: 10.1109/CONIT65521.2025.11167685.

[2] O. Dewangan *et al.*, "Secure Data Sharing and End-to-End Encryption in Federated Cloud Computing Systems," *Proc. Int. Conf. on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC³)*, 2025, pp. 1–10, doi: 10.1109/ISAC364032.2025.11156403.

[3] S. Vimalnath, K. Janani, R. Janapriya, V. Jayarisha, and C. Karnikashree, "Secure Cloud AI: Leveraging Artificial Intelligence to Safeguard Cloud Data Sharing Against Fault Injection Attacks," *Proc. 2025 5th Int. Conf. on Expert Clouds and Applications (ICOECA)*, Karur, India, 2025, pp. 23–26, doi: 10.1109/ICOECA66273.2025.00016.

[4] S. Gayathri and M. Sathish Kumar, "Scalable and Secure Sharing of Personal Health Records in Fog Cloud Computing Using Attribute-Based Encryption," *Proc. 2025 Int. Conf. on Computing Technologies & Data Communication (ICCTDC)*, Hassan, India, July 2025, pp. 1–5, doi: 10.1109/ICCTDC64446.2025.11158734.

[5] Anusha C. Reddy, G. Varun, S. Rossan, and B. M. Beena, "PrivCloud: Data anonymization service for secure cloud environments," in *Proc. 6th Int. Conf. Emerging Technology (INCET)*, Karnataka, India, May 2025, pp. 1–5, doi: 10.1109/INCET64471.2025.11140353.

[6] S. Sharma, A. Garg, and P. Singh, "Blockchain-Enabled Cloud Storage: A Secure and Decentralized Approach to Access Control and Data Sharing," *Proc. 2025 Global Conf. Emerging Technology (GINOTECH)*, Pune, India, May 2025, pp. 1–6, doi: 10.1109/GINOTECH63460.2025.11076732.

[7] H. Fnu and S. Murri, "Evaluating efficiency of advanced encryption algorithms for cloud data security," in *Proc. 1st Int. Conf. Secure IoT, Assured and Trusted Computing (SATC)*, 2025, pp. 1–6, doi: 10.1109/SATC65530.2025.11137050.

[8] A. P. A. Singh and N. Gameti, "Leveraging Digital Twins for Predictive Maintenance: Techniques, Challenges, and Application," IJSART, vol. 10, no. 09, pp. 118–128, 2024.

[9] R. Arora, A. Kumar, and A. Soni, "AI-Driven Self-Healing Cloud Systems: Enhancing Reliability and Reducing Downtime through Event- Driven Automation," 2024.

[10] K. Ullah et al., "Ancillary services from wind and solar energy in modern power grids: A comprehensive review and simulation study," J. Renew. Sustain. Energy, vol. 16, no. 3, 2024, doi: 10.1063/5.0206835.

[11] T. V. Jaswanth and S. J. J. Thangaraj, "Minimized Computational Time in Cloud Using Advanced Encryption Standard Algorithm Over File Changed with Security," in 2024 Second International Conference on Advances in Information Technology (ICAIT), 2024, pp. 1–6. doi: 10.1109/ICAIT61638.2024.10690288.

[12] P. Rajasekar, K. Kalaiselvi, R. Shanmugam, S. Tamilselvan, and A. P. Pandian, "Advancing Cloud Security Frameworks Implementing Distributed Ledger Technology for Robust Data Protection and Decentralized Security Management in Cloud Computing Environments," in 2024 Second International Conference on Advances in Information Technology (ICAIT), 2024, pp. 1–6. doi: 10.1109/ICAIT61638.2024.10690718.

[13] K. Kalyani and S. J. J. Thangaraj, "Reducing the Communication Overhead in Novel Data Sharing Algorithm in Cloud Data Storage Over Triple Data Encryption Standard Algorithm," in 2024 Second International Conference on Advances in Information Technology (ICAIT), 2024, pp. 1–4. doi: 10.1109/ICAIT61638.2024.10690317.

[14] I. Gupta, A. K. Singh, C.-N. Lee, and R. Buyya, "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions," *IEEE Access*, vol. 10, pp. 71247–71305, 2022.

[15] S. Haddad *et al.*, "Joint watermarking-encryption-compression scheme for secure medical image storage," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 310–322, 2020.

[16] Y. Zhang *et al.*, "Privacy-preserving CP-ABE with hidden access policy," *IEEE Access*, vol. 8, pp. 102345–102357, 2020.

[17] J. Li *et al.*, "Privacy-preserving machine learning with multiple data providers," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 4, pp. 593–607, 2019.

[18] A. Zaghloul *et al.*, "P-MOD: Privilege-based multilevel organizational data sharing in cloud computing," *IEEE Trans. Big Data*, vol. 5, no. 4, pp. 448–460, 2019.

[19] M. Backes *et al.*, "LIME: Data lineage in malicious environments," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 1, pp. 1–15, 2018.

[20] J. Li *et al.*, "LDSS: A lightweight data sharing scheme for mobile cloud computing," *IEEE Access*, vol. 6, pp. 40198–40210, 2018.

[21] R. Yonetani *et al.*, "Privacy-preserving visual recognition using doubly permuted homomorphic encryption," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 5, pp. 1159–1173, 2017.

[22] M. Backes *et al.*, "LIME: Data lineage in malicious environments," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 2, pp. 1–14, 2017.

[23] A. Zaghloul *et al.*, "Privilege-based multilevel organizational data sharing in cloud computing," *IEEE Trans. Big Data*, vol. 2, no. 4, pp. 335–347, 2016.

[24] J. Li *et al.*, "LDSS: A lightweight data sharing scheme for mobile cloud computing," *IEEE Access*, vol. 4, pp. 597–608, 2016.

[25] X. Liu *et al.*, "Fair data access control for cloud storage," *IEEE Trans. Cloud Comput.*, vol. 4, no. 1, pp. 67–80, 2016.

[26] C. Wang *et al.*, "File hierarchy attribute-based encryption for secure data sharing in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2136–2147, 2015.

[27] Y.-H. Kao *et al.*, "uCloud: A user-centric key management scheme for secure cloud storage," *IEEE Access*, vol. 3, pp. 2015–2024, 2015.