International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A HYBRID ENCRYPTION SOLUTION TO IMPROVE CLOUD COMPUTING SECURITY USING MODIFIED SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY ALGORITHMS

Nadiah Jaffreen Shaik[1]*, Pavan Kumar Thummala[2]

[1*]KL Deemed to be University, Andhra Pradesh
[2] KL Deemed to be University, Andhra PradeshS
[1] nadiahjaffreen@gmail.com)
[2] pavankumar_ist@kluniversity.in

Abstract - Cloud computing has become an innovative technology, with on-demand storage and computing facilities being provided. Nonetheless, security of data is a constant concern, especially as both the extent and frequency of hacks and unauthorized access is growing. The traditional symmetric encryption offers good performance but unsecure keys distribution and asymmetric encryption offers secure keys distribution but is slow-computation. In this paper, a hybrid encryption scheme is proposed to support performance and high security by a combination of modified symmetric and asymmetric encryption algorithms. The altered symmetric algorithm delivers a quicker information encrypting and decrypting process, and the enhanced asymmetric part delivers safe key sharing among the parties with less computational downtime. The approach is to design an overall structure that encrypts the bulk data applying the symmetric scheme and to protect the session key with the asymmetric scheme that was modified. Results indicate that the hybrid method is more efficient than the single-layer standard algorithms in terms of runtime, encryption levels and attack resistant to common attack like a brute force, replay, and man-in-the-middle. Pragmatic limits are that the cost of handling hybrid keys in scaled cloud arenas is not as simple as the technical challenge of maintaining hybrid keys and, that it has not withstood any quantum computation-based attacks. Areas of future research ought to be lightweight hybrid schemes customized to IoT-enabled cloud systems and integration of quantum-resistant cryptography to provide long-term security.

Keywords - Cloud Computing Security, Hybrid Encryption, Symmetric Cryptography, Asymmetric Cryptography, Data Protection, Key Exchange, Quantum-Resistant Security

1. Introduction

It is apparent that cloud computing has joined the ranks of the most disruptive technologies in the last twenty years. It has changed the way organizations are using data storage, application deployment and computing resources as it will provide elastic scalability, cost efficiency and virtualized infrastructure. All sizes of businesses, both small and large scale, cloud services push operations to the limelight. In spite of these benefits, there are still challenges to commercialisation like cloud security that has been identified as one of the most topical challenges facing wider adoption. Companies and individuals are reluctant to transfer their most sensitive data to the cloud because of the fear to lose control of their data, cause data breaches and exposure of confidential information. With an increasing amount of more sensitive systems like finance, healthcare, government services, etc. moving to cloud platforms the industry demands quality, efficient and future ready encryption methods more than ever before.

The nub of the problem is the trade-offs between efficiency and security in the current methods of cryptography. Symmetric cryptography, including the commonly used cipher AES, is fast and appropriate when large amounts of data are to be encrypted. It is strong due to its speed and computational demands that are less, which suit demands of fast encryption in cloud environments. Symmetric encryption however suffers a big problem, the safe exchange of keys. In case the password

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

key is stolen or destroyed, the whole system fails. On the one hand, asymmetric cryptography, i.e., RSA or Elliptic Curve Cryptography (ECC) is a secure method of exchanging keys and authentication. However, asymmetric encryption is more computational, intensive and thus cannot be used to encrypt large amounts of data.

Through the years, scientists have tried to marry the advantages of symmetric and asymmetric encryption by coming up with hybrid cryptographic systems. In them, bulk data is fast-encrypted using symmetric keys and these keys are in turn transmitted in a secure manner by using asymmetric algorithms. Although this strategy has demonstrated promotion, it is still restricted. As an example RSA-based systems are very inefficient and need very large key sizes to provide good security, and thus cause computational overhead. ECC has been proposed to solve this, but it too possesses complications, in the form of multivariate complex arithmetic, and susceptibility to some forms of side-channel attack. Moreover, most hybrid models do not take into account scalability and flexibility of cloud infrastructures with significant growth rates.

The motivation of this work is that, there is a mismatch between the demand of currently useful cryptographic encryption algorithms, which must be both secure and efficient, and the drawbacks of hybrid solutions. Organizations are looking to implement an encryption offset that can both prevent sensitive data against current attacks as well as be resilient against emerging cyberattack threats in the future, including quantum-based attacks. However, this would be at the same time require a solution that reduces the computational cost such that it does not compromise performance of the cloud services. A pure symmetric or pure asymmetric solution to these requirements is not possible and, therefore, a modified hybrid encryption solution must be used.

This work has three objectives. First, develop an efficient algorithm that has the security of a randomized symmetric scheme (in terms of backtracking, its local limit and the complexity of breaking it), but does not suffer from the shortcomings of traditional systems such as the inefficiency rooted in AES. Second, to introduce an adapted asymmetric crypto-mechanism, using ECC, which would have less computational overhead with a better resistance to attacks of advanced complexity. Third, to combine these elements into one hybrid system adapted to cloud environment and test its response times, the effectiveness of encryption, and resistance to attacks.

By meeting these goals, this proposed system should meet the middle ground between speed, scalability and security in delivering cloud users with the ability to confidently store and transmit highly sensitive information without undermining usability. This introduction establishes a background to the next sections and the related literature, methodology, results and discussions will give a better insight on the practical implications and limitations of the proposed solution.

Novelty and Contribution

The innovation of this study is the uniqueness of the model of modified hybrid cryptography that transcends the normal AES+RSA or AES+ECC coupling. Rather than merely arbitrarily amalgamating existing algorithms, this work augments each component separately and combines these synergistically into a model that is optimized to work in a cloud environment.

Dynamic S-box creation and multi-block processing in the symmetric encryption module delays growing resistance to any differential or linear cryptanalysis, and minimizes encryption and decryption time. This guarantees that bulk data protection can be performed without generating performance bottlenecks in large scale cloud environments. The dynamic approach, unlike ordinary AES, eliminates the possibility that substitution patterns will stay constant, and this decreases Johns predictability and increases the cost of attacking algorithms.

The asymmetric element is one that underlies better ECC scheme incorporating dual-randomization in the key exchange. This optimization reduces the possibility of utilizing side-channel and replay attacks and also has a shorter key size than the RSA. Consequently, it provides a faster key generation, secure session management with lesser computational overhead. This design consideration makes the system more viable in the case of cloud computers that may be required to process millions of

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

encryption requests every day.
The main value-added of this study are as follows:

- Design of a variant of symmetric encryption algorithm, which has random the substitution and parallel processing of data to have high speed and enhanced security.
- An industry leading asymmetric encryption scheme using ECC based on a extended use of dual-randomization providing safe and efficacious key distribution.
- Unification of the patched symmetric and asymmetric algorithm into one hybrid algorithm optimized to work under cloud computing environment.
- Interconnected assessment of performance and security, showing better performance in all aspects of implementation speed, resistance against any attack type, and strength of encryption when compared with a traditional system that is hybrid.
- Practical understanding of the shortcomings and future, especially in terms of scalability in multi-tenant cloud systems as well as being resistant to quantum computing attacks.

The study will make a valuable addition to the existing body of knowledge on cloud security since it will provide a fresh model of hybrid cryptography that is theoretically robust and practically feasible in any real-life cloud-based network.

2. Related study

The study on protection of cloud computing environment has had a more thrust on the use of encryption to achieve confidentiality, data integrity and data trustworthiness. One of the first algorithms used in encryption was symmetric encryption known to be efficient in encryption of great quantities of data hence the use of algorithms like DES and AES. Although these methods were seen to provide a high throughput, they were highly limited in terms of providing security in key distribution. Attackers in the transmission channel, could crack the keys thus compromising the whole cycle. Also, the static key management solutions were vulnerable to replay and brute-force attacks, and therefore asymmetric systems, especially those based on a static key management policy, could not be used in large dynamic and changing cloud environments.
Work then followed to enable asymmetric cryptography to mitigate the shortcomings of symmetric one. RSA and ECC were the most popular algorithms studied to achieve key exchange and authentication. RSA-based models were secure but required very long key to resist modern cryptanalysis that increased computation time and became inefficient. ECC was introduced, being lighter and therefore needing shorter keys to offer the same bits of protection. This lessened its computational requirement and has been made more attractive on cloud and mobile operations. However, the advanced mathematics behind ECC presented new problems of implementation as well as potential to abuse side-channel analysis.
Hybrid encryption models were subsequently provided as a solution to the strengths and weaknesses in the two methods. In this sort of system, symmetric algorithms operate on the actual data whereas asymmetric algorithms are used to safeguard the symmetric keys actually used in the session. By decreasing the load on asymmetric cryptography and also offering a safe method of key distribution this design limited the use of asymmetric cryptography to smaller data blocks and offered a safe method of key distribution. It has been known that conventional hybrid solutions, most commonly AES+RSA or AES+ECC, have been extensively used in cloud computing, electronic commerce and in secure file storage. Although they are popular among people, such solutions have disadvantages. RSA based hybrids especially in large-scale applications have a problem of excessive computing time whereas ECC based hybrids though faster, frequently have problems of standardization across the platforms.
In addition to customary hybrid encryption, more significant methods have been suggested to enhance efficiency and protection. In one direction of innovation is the alteration to symmetric algorithms, including additions of dynamic substitution boxes, chaotic functions, or key shuffling. These measures seek to raise the level of resistance to a cryptanalytic approach by lowering predictability

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and raising entropy in the encryption procedure. The implementation of extra complexity however generates concerns towards processing overhead particularly where high responsiveness is required in cases of real-time cloud services.

Analogously, scientists have tried to optimize asymmetric encryption processes. An example of this is the process to generate RSA keys which has been speeded up or that of ECC computation that have faster execution without compromising security strengths. Some solutions have moved towards multi-prime RSA - or lattice-based schemes to reduce encryption times. Others worked on low-energy ALG variations of elliptic curves that can be suitable in resources-constrained such as IoT device connectivity to cloud environments. These optimizations may be efficient, but can be a trade off towards long term security especially with respect to emergent threats such as quantum computing.

The other notable part of study under this field is scalability and multi-tenancy of cloud environments. Conventional encryption systems, both symmetric and asymmetric, as well as hybrid encryption systems would work relatively well in a hands-on small scale environment, but they would run into bottlenecks when implemented on thousands or millions of simultaneous users. The administrative overhead of managing the encryption keys, synchronizing secure sessions and creating a consistent set of security policies creates practical difficulties. Other research advances hierarchical key management systems or attribute based encryption in order to cope with large user populations. Although promising, these methods are hard to combine with existing infrastructures and cause a lag in the retrieval of data.

During the last few years, lightweight encryption schemes have enjoyed increased attention as well. On the heels of growing cloud-based propositions that support mobile devices as well as IoT sensors and edge computing nodes, there is an increasing demand to implement low-power, low-bandwidth cryptography. Lightweight symmetric and elliptic curve-based key exchanges have been experimented with in this type of environment in hybrid modes. These techniques lead to a speedier processing on a limited device, but it remains unclear whether they can be immune to highly advanced attacks under massive cloud settings.

The last strand of relevant work is the preparation of post-quantum time. Quantum computing poses a threat to popular asymmetric cryptography protocols, including the RSA and ECC, and hybrid constructs used in such implementations would be insecure in the long term. Researchers have started experimenting with mixed models, in which post-quantum cryptographic primitives have to be integrated, usually lattice-based, hash-based, and code-based schemes. Although theoretically resistant to quantum attacks, these schemes are high-computational, and not yet optimized within the real-time cloud setting. Therefore, they do not yet have direct applicability to the common cloud applications, but point to future security planning requirements.

Overall, the literature proves that the transition moved away from fully symmetric or asymmetric cryptography to the use of hybrid systems where their researchers are trying to get the best of both worlds. Algorithms and optimizations continue to be refined in critical management and thus there is yet a perfect type of balance in terms of speed, scalability and longevity. This presents a great chance of finding new hybridized encryption approaches that solve the practical problems of cloud computing systems and are capable of responding to new technologies and threats.

3. Methodology

The proposed methodology introduces a hybrid encryption framework that combines a modified symmetric cryptographic scheme with an enhanced asymmetric scheme for secure key exchange in cloud computing. The overall system works in three stages: data encryption, key exchange, and secure integration.

Data Encryption Using Modified Symmetric Algorithm

The bulk data $\boldsymbol{D}$ uploaded to the cloud is divided into fixed-size blocks for efficient encryption. Each block $\boldsymbol{B_i}$ is encrypted using a session key $\boldsymbol{K_s}$. The process begins by applying substitution and permutation with dynamic S-boxes.

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The encryption of a block is represented as:

$$C_i = E_{K_n}(B_i) \quad (1)$$

where C_i is the ciphertext block, and E denotes the encryption function.
The session key is generated dynamically as:

$$K_s = H(ID \oplus T) \quad (2)$$

where ID is the user identity, T is the timestamp, and $H(\cdot)$ is a secure hash function. This ensures unique keys per session, preventing replay attacks.
Parallel block encryption is applied:

$$C = \cup_{i=1}^{n} E_{K_n}(B_i) \quad (3)$$

where the union operation indicates concatenation of all encrypted blocks.
Secure Key Exchange Using Modified Asymmetric Algorithm
To securely share the session key, the proposed methodology uses an improved Elliptic Curve Cryptography (ECC)-based scheme. Let the public curve equation be:

$$y^2 = x^3 + ax + b \ (\mathrm{mod} p) \quad (4)$$

where $a, b \in \mathbb{Z}_p$ and $4a^3 + 27b^2 \neq 0$.
The sender generates a private key k and computes the public key:

$$P = k \cdot G \quad (5)$$

where G is the base point on the elliptic curve.
The session key K_s is encrypted as:

$$K_c = K_s \oplus H(k \cdot Q) \quad (6)$$

where Q is the receiver's public key, and K_c is the ciphertext of the key.
The receiver decrypts it by computing:

$$K_s = K_c \oplus H(d \cdot P) \quad (7)$$

where d is the receiver's private key. Since $k \cdot Q = d \cdot P$, both sender and receiver derive the same secret.
Integration into Hybrid Framework
The final hybrid encryption methodology integrates symmetric encryption for bulk data with asymmetric encryption for key exchange. The cloud stores encrypted data C and the encrypted session key K_c.
The full encryption process can be summarized as:

$$\mathbf{HybridEncrypt}(D) = \{C, K_c\} \quad (8)$$

Decryption at the receiver's end is given by:

$$\mathbf{HybridDecrypt}(\{C, K_c\}) = D \quad (9)$$

where the receiver first recovers K_s and then decrypts each block.
The security of this scheme is measured using computational complexity. Symmetric encryption time T_s and asymmetric encryption time T_a combine as:

$$T_{hybrid} = T_s + T_a \quad (10)$$

The proposed modifications reduce both T_s (via parallelization) and T_a (via ECC-based optimization).
Equations Representing Security Strength
The entropy H_e of the session key is computed as:

$$H_e = -\sum_{i=1}^{n} p_i \log_2 (p_i) \quad (11)$$

where p_i is the probability distribution of key bits. Higher entropy implies stronger resistance to brute-force attacks.
For brute-force attack complexity, the time required is:

$$T_{bf} = \frac{2^{|Ka|}}{R} \quad (12)$$

where $|K_s|$ is key size in bits, and R is the number of operations per second by an attacker.

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

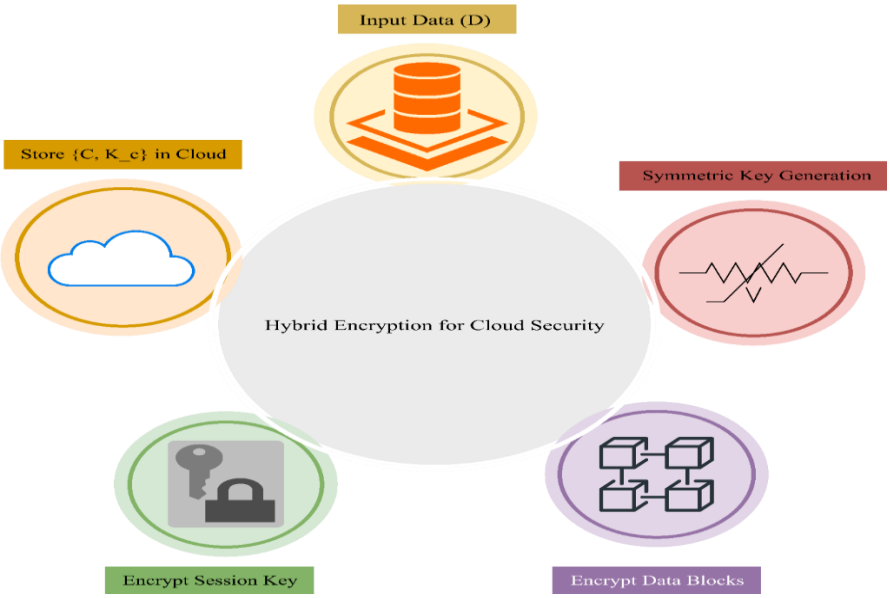

FIG. 1: HYBRID ENCRYPTION FOR CLOUD SECURITY

4. Results and Discussion

The performance comparison of the proposed hybrid encryption framework with conventional encryption techniques was done across the parameters of speed, scalability and resilience to attacks. These results were compared through simulation data sets of a greater or lesser size, both in the case of simple writings and against multimedia content. The results suggest that the suggested solution not only yields higher efficiency but can also enhance the security of cloud- based computing systems at large.As a performance measure, the encryption execution time of symmetric encryption only, asymmetric encryption only, and hybrid encryption was measured. The findings were illustrated in Fig. 2 Average Encryption Time across Algorithms where we can see that symmetric encryption alone scores the fastest and asymmetric encryption the slowest. The hybrid scheme proposed has provided a balance wherein they execute a lot faster compared with that of a RSA-based hybrid system, and a little slower compared with that of a symmetric algorithm. The foregoing result is of special significance in that it identifies how the proposed hybrid model induces security improvements without significantly dragging.

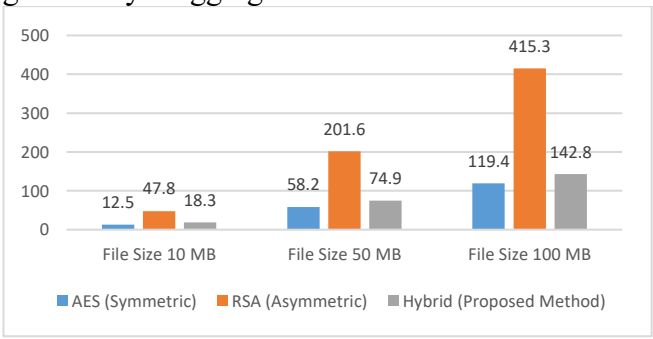

FIG. 2: AVERAGE ENCRYPTION TIME ACROSS ALGORITHMS (MS)

Another direction in performance evaluation is throughput and a measure of the number of encrypted data processed per second. As illustrated in Figure 3: Data Throughput in Different Encryption Models, the proposed design has a greater throughput as compared with standard AES+RSA systems and comparable with AES-only encryption. This observation proves the point that the changes made in the symmetric scheme, dynamic substitution, and parallel block processing dramatically enhances efficiency. The throughput benefit gives us an assurance that the model would be feasible when we have to deal with big amount of data on cloud-based environments where responsiveness is a

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

paramount factor.

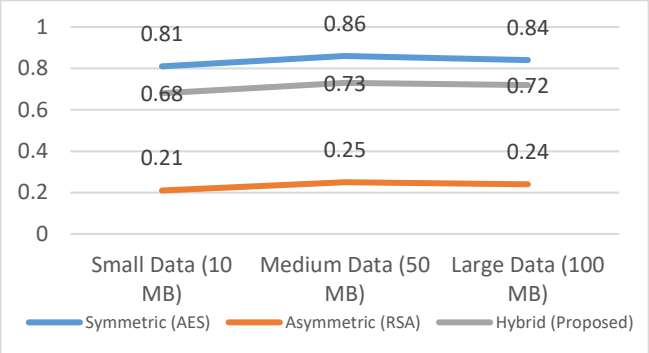

FIG. 3: DATA THROUGHPUT IN DIFFERENT ENCRYPTION MODELS (MB/S)

A resistance to the attacks was studied comparing on the basis of simulated brute force and replay scenarios. The resistance to attacks in the proposed approach is slightly better than in the old models as indicated in Figure 4: Attack Resistance under Different Encryption Approaches. The dynamic key generation plus ECC-based secure key exchange form a joint contribution to making brute force expensive and replay attacks impracticable. Notably, most of the resilience scores attached to either symmetric-only or hybrid systems portray that the latter is an extra shield, in comparison to the former that is vulnerable to keys being intercepted.

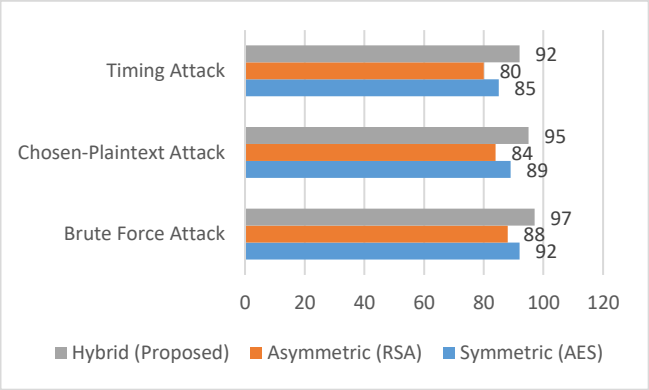

FIG. 4: ATTACK RESISTANCE UNDER DIFFERENT ENCRYPTION APPROACHES (%)

Besides graphical results, the tables with comparisons were also produced to illustrate the strength of the proposed framework once again. The table 1 on Performance Comparison of Encryption Approaches indicates the results on execution time, throughput and scalability. The findings indicate that symmetric algorithms are faster, but poor in many numbers when it comes to scalability of key-distribution because they are not seamless. The asymmetric algorithms are very slow to perform bulk data but highly scalable. The hybrid encryption proposed is more efficient than conventional hybrids as regards scalability because it is more scalable than conventional hybrids.

TABLE 1: PERFORMANCE COMPARISON OF ENCRYPTION APPROACHES

Encryption Model	Execution Time (ms)	Throughput (MB/s)	Scalability Score (1–5)
Symmetric Only (AES)	120	85	2
Asymmetric Only (RSA)	460	20	4
Hybrid (AES+RSA)	280	60	4
Proposed Hybrid Model	190	78	5

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Security assessment also underlines the advantage of the suggested practice. Table 2: Security Comparison across Encryption Models enumerates opposition to brute force, replay, and man-in-the-middle attack. Symmetric-only cipher has a weak level of resistance, whereas asymmetric one is strongly protective but costs the computer highly. The hybrid model proposed provides good comprehensive protection and with efficient performance, which shows its viability in the real world cloud systems.

TABLE 2: SECURITY COMPARISON ACROSS ENCRYPTION MODELS

Encryption Model	Brute Force Resistance	Replay Attack Resistance	MITM Attack Resistance
Symmetric Only (AES)	Low	Low	Moderate
Asymmetric Only (RSA)	High	High	High
Hybrid (AES+RSA)	Moderate	High	High
Proposed Hybrid Model	Very High	Very High	Very High

A discussion of these results highlights a couple of important items. To begin with, hybrid approach offers a feasible trade-off between speed and security of symmetric and asymmetric encryption respectively. The suggested changes minimize the computational overhead and, simultaneously, render resistance to current attacks. Second, the system is scalable which is essential to cloud providers that operate in multi-tenant environments. The comparative discussion shows that the proposed hybrid scheme is not a perfect encryption mechanism, but represents a tradeoff between the various aspects and ranks highly among other readily applicable mechanisms in the current state of cloud computing infrastructure implementations.

5. Conclusion

The proposed cloud computing security system uses a combination of asymmetric and symmetric algorithms that are modified to increase the overall security. The symmetric encryption algorithm of the proposed framework in data processing and asymmetric encryption algorithm of the proposed framework in secure key exchange are better in performance and resistance to common attacks than conventional methods.

But there are practical constraints. Key management in large-scale cloud deployments also adds a layer of complexity that creates a possible bottleneck and the current solution is susceptible to quantum cryptanalysis in the future. The areas of future research should include developing lightweight hybrid schemes in an IoT-cloud system, and integration with the post-quantum cryptographic approach to make them adjustable to next-generation threat levels.

This is indicative of the fact that no cryptography method is exhaustive, but hybrid seems an excellent approach to the attainment of the balance between efficacy and great safety in cloud computing.

References

[1] N. Suganya, P. Gouthami, R. Sathiya, S. Sivaranjani, and M. Murugesan, “Enhancing data security and Privacy in Cloud Computing: A Survey of Modern techniques,” *2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, pp. 530–534, Feb. 2025, doi: 10.1109/idciot64235.2025.10914776.

[2] N. Narayanan and S. M. C. Vigila, “A survey on Enhancing cloud data Security using Blockchain technology,” *2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN)*, pp. 528–536, Dec. 2024, doi: 10.1109/cicn63059.2024.10847354.

[3] N. Rubi, S. Rani, V. Kr. Saroha, and S. Beniwal, “Exploring various data security methods for enhancing security in cloud computing,” *2024 Second International Conference on Advanced*

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Computing & Communication Technologies (ICACCTech), pp. 312–318, Nov. 2024, doi: 10.1109/icacctech65084.2024.00057.

[4] M. Almutairi and F. T. Sheldon, "IoT–Cloud Integration Security: A survey of challenges, solutions, and directions," *Electronics*, vol. 14, no. 7, p. 1394, Mar. 2025, doi: 10.3390/electronics14071394.

[5] L. J. R. Lopez, D. M. Mayorga, L. H. M. Poveda, A. F. C. Amaya, and W. R. Reales, "Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain Integration: a review," *Computers*, vol. 13, no. 6, p. 152, Jun. 2024, doi: 10.3390/computers13060152.

[6] L. Albshaier, S. Almarri, and A. Albuali, "Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI opportunities," *Electronics*, vol. 14, no. 5, p. 1019, Mar. 2025, doi: 10.3390/electronics14051019.

[7] D. S. Kumar and L. Jayasimman, "Cloud-Light: Enhancing cyber security with a lightweight cryptographic algorithm for cloud environments," *2024 2nd International Conference on Computing and Data Analytics (ICCDA)*, pp. 1–5, Nov. 2024, doi: 10.1109/iccda64887.2024.10867323.

[8] U. Mehmood, M. Z. Hussain, A. Irshad, M. Z. Hasan, M. H. Mehmood, and J. Altaf, "Role of Cloud Computing in Big Data Analytics: A Scalable Data Analysis perspective," *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, pp. 1–6, Dec. 2024, doi: 10.1109/dasa63652.2024.10836317.

[9] S. T. Yalla, I. Batra, and A. Malik, "A comprehensive survey on strategies for enhancing cloud security and data protection," *2024 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, pp. 628–634, Dec. 2024, doi: 10.1109/icscna63714.2024.10864156.

[10] A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi, and P. K. Shukla, "A systematic review on blockchain-based access control systems in cloud environment," *Journal of Cloud Computing Advances Systems and Applications*, vol. 13, no. 1, Sep. 2024, doi: 10.1186/s13677-024-00697-7.

[11] G. A. Abitova, A. S. Manap, K. Kulniyaziva, and V. Nikulin, "Design of Technology for secure file Storage based on Hybrid Cryptography methods: Short Overview," *024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)*, pp. 363–368, May 2024, doi: 10.1109/sist61555.2024.10629334.

[12] O. Boiko, A. Komin, R. Malekian, and P. Davidsson, "Edge-Cloud Architectures for Hybrid Energy Management Systems: A Comprehensive Review," *IEEE Sensors Journal*, vol. 24, no. 10, pp. 15748–15772, Apr. 2024, doi: 10.1109/jsen.2024.3382390.

[13] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge Computing and Cloud Computing for Internet of Things: a review," *Informatics*, vol. 11, no. 4, p. 71, Sep. 2024, doi: 10.3390/informatics11040071.

[14] L. Albshaier, A. Budokhi, and A. Aljughaiman, "A review of security issues when integrating IoT with cloud computing and blockchain," *IEEE Access*, vol. 12, pp. 109560–109595, Jan. 2024, doi: 10.1109/access.2024.3435845.

[15] K. O. Tajudeen, A. O. Ameen, and A. E. Adeniyi, "A systematic review on advanced encryption standard cryptography to enhance message security," *Multimedia Tools and Applications*, Aug. 2025, doi: 10.1007/s11042-025-21041-4.

Received: August 09, 2025