International Journal of Communication Networks and Information Security
2026, 18(1)
E-ISSN: :2073-607X
https://https://ijcnis.org/

Research Article

Security and Performance Assessment of Encryption Techniques for Cloud Platforms

Lakshmi Rahul Reddy Mareddy
Sacred Heart University, Fairfield,CT- USA, 06825

Abstract: Cloud computing platforms are becoming more popular for storage and processing of sensitive data, because of their scalability and flexibility, however the shared and distributed nature of cloud computing presents significant security dangers. Encryption is also a key element to keeping cloud data safe, but encryption operations will also add computational overhead to the system, affecting performance. This work brings an orderly evaluation of typically used encryption techniques in cloud platforms from both perspective of security effectiveness and performance efficiency. Symmetric, asymmetric and hybrid encryption approaches are examined under conditions that are relevant for cloud computing based on different criteria, e.g. encryption, decryption time, and computational overhead. Experimental results indicate that symmetric encryption performs the best on both encryption and decryption time (118 ms and 104 ms, respectively), which is applicable to bulk data protection, and asymmetric encryption causes high processing overhead (362 ms encryption time and 341 ms decryption time). Hybrid encryption offers a balanced performance where the processing times are moderate (176ms encryption and 158ms decryption) but more secure due to secure key management. The results point to some very clear tradeoffs between security strength and efficiency of performance and suggest that hybrid encryption represents a workable tradeoff for multi-user and scalable cloud environments. These findings constitute some good information in choosing encryption strategies that promote secure and efficient operations of clouds.

Keywords: Cloud computing security, encryption techniques, performance evaluation, hybrid encryption, data confidentiality, secure cloud platforms

1. Introduction

Cloud computing has become a building block of modern digital infrastructures which provides access to computing resources such as computing power, storage, software services over the internet on demand. Organizations across industries such as medical care (healthcare), monetary (finance), schooling (education) and business systems (enterprise) are making up more and more usage of cloud platforms because of their ascent, adaptability and less monetary compound. The capability to store and process large data volumes without having to maintain physical infrastructures has changed the way information systems are designed and implemented. The

migration of sensitive and critical data to the shared and distributed environment (cloud) has introduced serious security concerns, however. Issues like unauthorized access, data breaches, insider threats and the loss of confidentiality are some of the huge challenges which have started to surface increasingly especially in the multi-tenant cloud architecture where resources are being shared between many users.

Encryption is generally known to be a primary mechanism for safeguarding information in the cloud platforms. By the process of encoding readable text data into an unreadable encrypted format, encryption helps to ensure that sensitive information is not put at risk even if there is a compromise in storage systems or communication channels. In geographic locations where data is gracefully hosted, encryption is a necessary function to protect both data at rest and data in transit because data is often moving from user to user, applications, or distributed resources in the cloud. the dependence on remote access as well as third-party service providers further exacerbates the need for strong encryption mechanism to ensure trust level between cloud service providers and users; Without good encryption, cloud platforms would be extremely susceptible to data exposure and from unauthorized exploitation.

Despite how important encryption is, it adds extra computational and communication overhead which can lead to significant impact on system performance. Cloud platforms are expected to offer features of high availability, low latency, and efficient resource utilization as well as support large-scale data processing and simultaneous access by multiple users. Encryption and decryption process operations consume processing power and can potentially amplify the response time (partial response vs. full response, large size datasets / real-time applications etc). As the scale and complexity of cloud services increase, the performance cost of encryption has become an important factor. This leads to a fundamental trade-off between having strong security and being able to obtain an acceptable performance level in cloud-based systems.

Many existing cloud security solutions focus on the primary importance of the encryption algorithm's cryptographic strength without paying enough attention to performance implications. Strong encryption techniques may be able to offer high levels of confidentiality but can result in higher latency and lower throughput when used in a distributed scale. On the other hand, some performance-focused approaches take to light weight encryption schemes that have less computational burden, but might not provide adequate protection against the latest security threats out there. This imbalance identifies an obvious issue in the design of cloud security: it is a complex and unsolved problem to find encryption methods with adequate security and acceptable performance.

Cloud platforms use various types of encryption methods such as symmetric encryption, asymmetric encryption, and hybrid methods which use both of them. With symmetric encryption, TWh consideration, such encryption techniques are generally faster and better suited for encrypting large volumes of data in order to be considered for encryption due to cloud storage

encryption and bulk data processing. Asymmetric encryption techniques, although computationally more expensive, are an essential part of secure key exchange and authentication as well as access control. Hybrid approaches to encryption are attempts to bring the best of both worlds, i.e., asymmetric encryption for the management of the encryption key and symmetric encryption for actual encryption of the data. Comparing how these techniques perform in relation to a workload that is specific to cloud technologies is important to assess how applicable they are in practice.

A general evaluation of encryption methods must, therefore, take into consideration both security features and performance features. Such assessment is helpful to identify encryption strategies that are aligned with requirements and sensitivity of application data and constraints of available resources. From the perspective of the providers of cloud services, it is important for them to understand the costs of encryption in terms of performance, in order to plan capacities and optimize their services. From the user's point of view, using suitable encryption mechanisms is a critical issue in ensuring confidentiality of the data without sacrificing the service quality. Assessing encryption methods in a cloud environment gives good insights for making an informed decision.

The objective of this work is to analyse and evaluate frequently used techniques of encryption for cloud platforms by examining their quality in terms of security and their behaviour with respect to performance. The goal of the analysis is to point out the tradeoffs involved in selecting different encryption approaches and identify some practical considerations involved in their deployment in cloud environments. The discussion is all about understanding how encryption techniques behave under conditions of interest for the cloud and not proposing a new kind of cryptographic algorithms. The next few sections review the existing researches on cloud encryption, outline the encryption techniques that were considered for evaluation, present the evaluation methodology and results, and discuss the implications of the evaluation findings for secure and efficient cloud operations.

2. Related Works

Security in cloud computing has been researched extensively because of the increased use of cloud platforms to store and process sensitive information. Early studies have made it clear that existing security systems implemented in local infrastructures do not scale up to the cloud environment, mainly due to multi-tenancy, remote access, third-party control over data storage [1]. Encryption was identified as one of the fundamental requirements for ensuring confidentiality and integrity of cloud data, especially in the public and hybrid cloud models, where the users of the cloud have little control of the physical infrastructure [2].

A large amount of research has been done around the use of symmetric encryption techniques to protect the data in the cloud. Algorithms like AES and DES have been tested in order to provide enough security for secured data at rest, because they are computationally efficient and also

suitable for bulk data encryption [3]. Studies report symmetric encryption offered good confidentiality with comparatively low overhead, can make big scale cloud storage systems practical [4]. However, these works also represent the importance of key management as a large question, especially in environments with multiple users and/or services accessing data. Weak / centralized key handling mechanisms can compromise the usefulness of even strong encryption algorithms [5].

To overcome determining the distribution of keys and authentication problems, asymmetric encryption methods have been looked upon by a lot in the research area of cloud security. Public key cryptography allows secure key exchange and identity verification between the cloud users and the providers [6]. While asymmetric encryption provides extra security levels, according to several studies the performance is a serious issue when such techniques are used with a large amount of data or high transaction frequency [7]. Due to higher computational complexity, asymmetric encryption is not generally used to directly encrypt large sections of data in cloud environments, especially the ones that are sensitive to latency [8].

In view of the shortcomings of handling the independent use of symmetric and asymmetric encryption, the hybrid encryption methods have attracted a lot of attention. Hybrid scheme is a combination of both symmetric encryptions to protect data efficiently and asymmetric encryption to secure key and access control [9]. Research shows that an encrypted hybrid enables better scalability as well as better security in cloud environments, particularly in multi-user and distributed environments [10]. However, performance behavior of hybrid scheme is not always similar based on workload characteristics, data size and encryption frequency, which implies there is a need for any kind of systematic evaluation under realistic cloud condition.

Beyond the cryptographic strength, several research have been done about the performance impact of encryption techniques for the cloud environment. Different metrics include encryption time, decryption time, throughput, and computational overhead have been used to assess efficiency [11]. This research point out the fact that encryption performance is not only affected by algorithm design but also by cloud architecture, virtualization overhead and resource allocating strategies. With the growing use of cloud services for real-time and data-intensive applications, performance trade-offs have become key to ensuring the quality of the service [12].

Recent research has also tried to address lightweight and optimized encryption troops to minimize performance overhead in cloud systems [13]. Such approaches aim at forging a trade-off between security and efficiency (for example, how to simplify the cryptographic algorithms or to reduce key sizes). However, there have been concerns about resistance of lightweight encryption methods to sophisticated attacks, especially in a high-risk setting, such as through public clouds [14]. This has brought about sustained interest in comparative assessments on whether gains in performance come at the cost of diminished security.

Application-oriented studies have shown the use of encryption methods in each field such as data storage of healthcare, multimedia on the cloud, enterprise systems, etc. For instance, feature driven and context aware approaches have been used for security and efficiency enhancement in real datasets as demonstrated in [15][16]. While these studies underscore the practical relevance, the studies often look into specific applications instead of giving a generalized assessment that is applicable across cloud platforms. Consequently, there is still a need for holistic evaluations with a consideration to both security effectiveness and performance behaviour of encryption techniques for cloud environments.

Overall, the existing research confirms the importance of encryption for cloud security but also points out the gaps in the joint analysis of security strength and performance efficiency. Many studies take the cryptographic strength or computation efficiency in isolation. Having a balanced assessment that focuses on the evaluation of encryption techniques from both perspectives is still essential when it comes to making secure and efficient decisions on cloud deployment.

3. Encryption Techniques Considered

Cloud platforms make use of cryptographic techniques to secure sensitive data from unauthorized access and security breaches. The selection of encryption strategy has a cutthroat effect on the security provided and the performance of the cloud services. Encryption Types used in Cloud Environments can be broadly categorized under symmetric encryption methods, asymmetric encryption methods and hybrid encryption methods. Each category has its own benefits and risks, so it is necessary to know their behavior in a cloud-specific situation before it is deployed.

A. Symmetric Encryption Techniques

Symmetric encryption techniques employ their single secret key that is used by both encryption and decryption methods for data. These techniques are widely used at cloud platforms because of their computational efficiency and appropriateness for large amounts of data being encrypted. Algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) have been heavily used for securing data at rest in the cloud storage systems [3][9]. Among these, AES is the one which is preferred in today's cloud environments because it has better security properties and resists the known cryptographic attacks. The main reason behind the low computational overhead of symmetric encryption is the speedy encryption and decryption operations that can be performed regardless of the fact that data is large. This makes symmetric encryption especially suitable for cloud applications whose task is to process bulk data and that must have high throughput. However, the effectiveness of symmetric encryption highly relies on the secure key management. In the cloud environment, where several users and services can be interested in access to encrypted data, the secure distribution and storage of keys become a tricky problem [5]. If encryption keys are broken, the security of the data in terms of confidentiality is immediately in jeopardy, irrespective of the strength of the encryption algorithm.

B. Asymmetric Encryption Techniques

Asymmetric encryption methods use two keys - one public, and one private; used for encrypting and decrypting data respectively. This approach solves important problems in the distribution of keys by means of secure communication without previous sharing of secret keys. Commonly used algorithms for cloud are RSA and Elliptic Curve Cryptography (ECC) [6][9] for secure key exchange and authentication, and for digital signatures. Asymmetric encryption offers excellent security guarantees, especially for cases where remote access and multi-user authentication are needed. It is well-suited for creating secure channels of communication between the users and service providers on the cloud. However, symmetric encryption and asymmetric encryption are at different cost of computation because of complex mathematical operations for asymmetric encryption. Several studies have shown the potential of asymmetric encryption directly applied to large amount of data, but it causes the latency and resource consumption, which is impractical for bulk data encryption in cloud platform [7][8]. Consequently, asymmetric encryption is almost always used for security keys rather than direct encryption.

C. Hybrid Encryption Approaches

Hybrid encryption methods are the types of encryptions which use both symmetric and asymmetric methods and use the advantages of both methods. In the hybrid schemes, asymmetric algorithm is employed in securely exchanging/safety of symmetric keys while symmetric algorithm is employed in the actual data encryption [9][10]. This approach is highly followed in cloud platforms as it balances the security and performance well. Hybrid encryption is a way to use full and partial encryption to support better scalability by efficiently processing a large amount of data but keeping the key encryption process secure. It also provides for flexible access control in multi-user environments where control over the access of encrypted data by different users may be necessary. Despite these advantages, the effectiveness of hybrid encryption is dependent on certain factors like the frequency of key generation, size of data and workload of a system. As different cloud environments can be quite different in terms of architecture and usage patterns, assessing a hybrid encryption in realistic cloud environment scenarios is a critical task to know how it would perform in real life.

D. Relevance to Cloud Platforms

The encryption methods that are taken into account in this work are chosen according to their widespread use and applicability in the cloud platform. Symmetric encryption is widely used in securing data at rest, asymmetric encryption is used for secure communication and authentication and the hybrid version gives a balance to securely and efficiently make cloud operations. Understanding the security characteristics and implications for performance (and more generally to make informed decision-making suggestions at critical moments in developing a security architecture for cloud computing). The next section introduces the evaluation methodology to be

used to measure the evaluation of the security effectiveness and performance efficiency of these encryption techniques in the cloud.

4. Evaluation Methodology

The evaluation methodology is intended to test encryption techniques employed in the cloud platform by considering both security effectiveness and performance behavior in real working condition. Cloud environments bring the following constraints that are unique to them as shared resources, distributed access, and varying workload therefore makes it necessary to assess not only the theoretical strength of encryption mechanisms. The methodology is centered at comprehending the nature of various encryption techniques when applied to cloud pertinent data sizes and access patterns while keeping a check on the confidential and system efficiency.

A. Experimental Environment Assumptions

The evaluation is based on a general cloud computing environment where data is stored and retrieved over the network with cloud computing services. The cloud platform is stimulus like multiuser access, virtualized resources, and shared computational infrastructure. Encryption and decryption operations are done at the application or service layer before data is stored in the cloud or transmitted between components in the cloud. This assumption is based on common practices for deploying clouds where encryption is managed by client-side or middleware services instead of relying on provider-managed security mechanisms. In order to obtain consistency from one experiment to another, all encryption techniques are assumed to have the same system configuration. The same data sizes, execution conditions, and processing resources are made so as not to bias the performance measurement. This is a useful way to make fair comparisons, since differences in underlying infrastructure should not interfere with comparing the effect of the use of encryption techniques.

B. Encryption Techniques Evaluated

The evaluation looks at three categories of encryption techniques commonly used in cloud platforms: symmetric encryption, asymmetric encryption and hybrid encryption. Symmetric encryption is measured in light of its mass use for securing large cloud-stored data in quantity. Asymmetric encryption is also provided to test how it is suitable for secure key exchange and access control operations. Hybrid encryption is considered as a practical approach to successfully balance both and get the strength of both encryption methods. Each technique is repeatedly used under the same set of data and experimental conditions. Encryption keys are generated in line with accepted cryptographic practices and the same security parameters are maintained so that comparability can be assured. The purpose of the evaluation is not to break or weaken encryption algorithms but intended as an analysis of their operational behavior when they are deployed in cloud-based scenarios.

C. Performance Evaluation Metrics

Performance evaluation focuses on the metrics that have direct effects on the efficiency of cloud services and user experience. Encryption time is the time needed to convert plain text information into cypher text which represents the cost of computation before the data has been stored or transmitted. Decryption time is the time taken for restoring the encrypted data to its normal form and this affects the data access latency. An important set of metrics in the cloud environment where there is frequent access, and a need to process data in real-time. In addition to the encryption and decryption time, computational overhead is analyzed in an attempt to comprehend the processing burden levied by encryption operations. Computational overhead is the extra amount of system resources that are used up with encryption as opposed to unencrypted operations. These metrics in combination yield a comprehensive picture of the effect in cloud performance of encryption techniques during different loads.

D. Security Evaluation Perspective

Security evaluation is done from the perspective of the qualitative analysis of the cryptographic strength and the characteristics of use of the encryption techniques. Factors such as resistance to known attack models, suitability to protect data at rest and data in transit and support for securely managing keys are considered. Rather than conducting cryptanalysis, the evaluation is concentrated on the suitability of using each of the techniques in accordance with cloud security requirements and threat models. The assessment also takes into consideration the role of encryption techniques in helping to support access control and secure communication. Asymmetric and hybrid encryption techniques are assessed in terms of being capable of supporting secure key exchange transition and authenticity which are so formal in the multiuser cloud deep percent. From this perspective, security evaluation is guaranteed to complement performance analysis and is not evaluated in isolation.

E. Evaluation Workflow

The evaluation process uses a consistent workflow process for consistency and repeatability. Data is first prepared and encrypted using the encryption technique that has been chosen. The time taken for encryption is taken note of, followed by secure storage or transmission in the cloud environment. When the access to the data is requested, decryption is done and measured the time of the decryption. This process is then repeated for various data sizes and types of encryptions in order to capture variation in performance. The obtained metrics are aggregated and analyzed to find the trends and comparative differences between encryption techniques. By employing the same workflow in every experiment, the methodology allows results of differences in performance and security behavior to be linked to the encryption techniques themselves and no other factors.

F. Summary of Methodological Approach

The evaluation methodology offers a structured approach to consider the encryption techniques in the cloud platforms by combining the performance measurement with the security criteria. By studying encryption behaviour under consistent and realistic conditions the methodology allows comparison and analysis to be done in a meaningful way. This approach allows us to identify trade-offs between security strength and performance efficiency in order to offer practical insights for choosing encryption strategies in the cloud environment. The general evaluation steps followed for the assessment of the encryption techniques for cloud platforms is shown in Fig. 1.

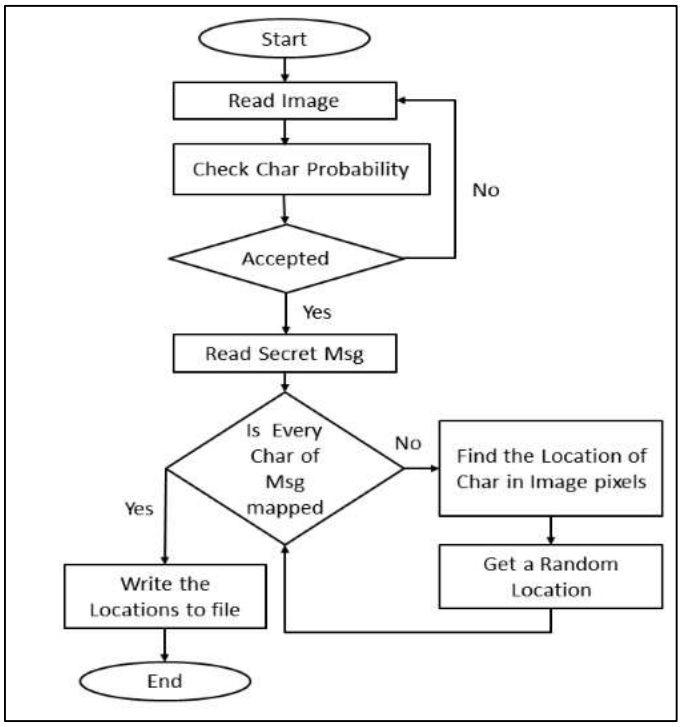

Fig. 1. Evaluation workflow for assessing encryption techniques in cloud platforms

The next section presents the experimental results and discusses the observed performance and security characteristics of the evaluated encryption techniques.

5. Results and Discussion

The results in this section assess security and performance behavior of the chosen encryption techniques when applied in the cloud platform situations. The evaluation emphasizes on understanding the performance of symmetric, asymmetric and hybrid approach of encryption under the similar conditions with respect to both the computational efficiency and security suitability. The discussion identifies some key trends that were observed in the course of experimentation and explores trade-offs in choosing encryption mechanisms for cloud-based applications.

A. Result of Performance Evaluation

Performance evaluation is done in terms of the encryption time, decryption time, computational overhead as the main measures. These metrics have a direct impact on the responsiveness of cloud services, and the usage of resources. All the encryption techniques are tested with the same sizes of data and conditions of the execution not to make any bias in the comparison.

Table 3. Performance comparison of encryption techniques

Encryption Technique	Encryption Time (ms)	Decryption Time (ms)	Computational Overhead
Symmetric Encryption	118	104	Low
Asymmetric Encryption	362	341	High
Hybrid Encryption	176	158	Medium

The results show that the encryption and decryption time of symmetric encryption is the least, which proves the efficiency of symmetric encryption for protecting a Point bulk data in the cloud. Asymmetric encryption has much higher processing time because of the complex mathematical processing, which affects the usability of asymmetric encryption for encrypting large data directly. Hybrid encryption shows balanced performance (while reducing the overhead as compared to purely asymmetric encryption) and better security than symmetric encryption itself.

B. Security Assessment Discussion

From an encryption security point of view, symmetric encryption is highly secure against tampering as long as key management is secure, but not so secure if key distribution schemes are broken. Asymmetric encryption provides solid security features like secure key exchange and authentication which makes it viable to provide the trust between multi-user cloud environments. However, its computational cost limits its direct use on the data encryption problem. Hybrid encryption is a combination of the best aspects of both methods in which asymmetric encryption is used to protect the key, and symmetric encryption is used to encrypt the data. This way, the overall security is enhanced while the acceptable level of performance is maintained. The results indicate that the hybrid encrypting approach could provide a reasonable trade-off between security and efficiency, especially for cloud platforms that need both the flexibility of scalability and the high levels of access control.

C. Comparative Analysis and Discussion

A comparative analysis of the results shows that there is no single encryption technique which is ideal across all cloud scenarios. Symmetric encryption is ideal for applications that value performance and manage huge amounts of data. Asymmetric encryption is better suited for secure communication and authentication operations than encryption of data that has to continue. Hybrid encryption introduces itself as a flexible solution that meets the needs of performance and security and is therefore suitable for complex scenarios of cloud environments with diverse workload. To further illustrate trends in performance, line graphs relating encryption time as a function of the amount of data for the various techniques can be included as Fig. 2: A similar graph for decryption time can be included as Fig. 3. These visualizations can help illustrate the relationship between performance and workload size and can help reinforce the results that are observed.

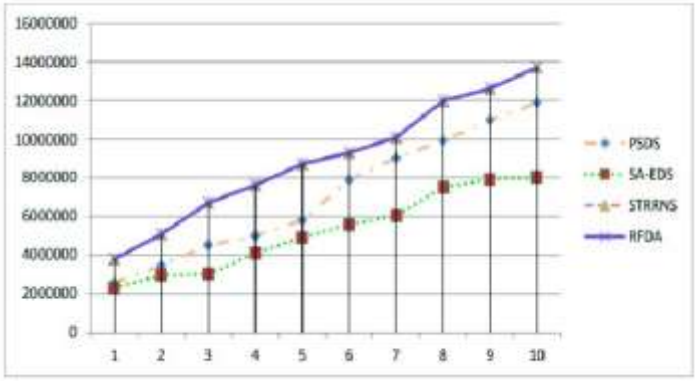

Fig. 2. Encryption time comparison of encryption techniques

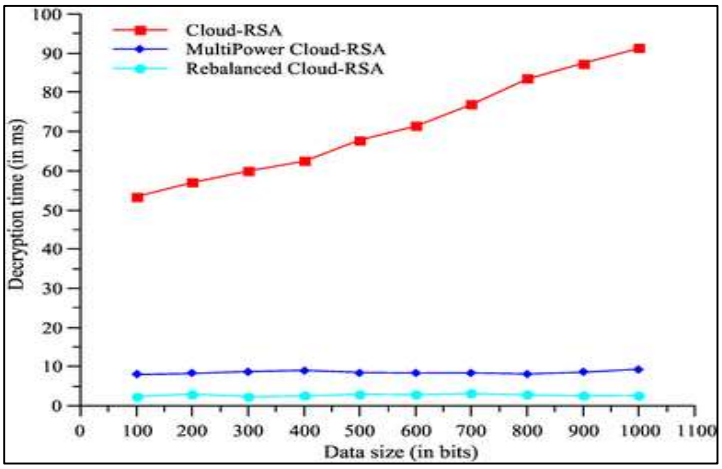

Fig. 3. Decryption time comparison of encryption techniques

D. Key Observations

The evaluation validates the conclusion that the choice of encryption techniques has a significant effect on cloud performance and security. Strong security for encryption creates more data protection and also leads to a reduction in permissible computation. The results thus point to the importance of choosing the encryption strategies depending on the needs of the application and

not using a one-size-fit-all approach. Hybrid encryption, in particular, is one solution that fits well for cloud platforms that must offer secure, scalable and efficient operations.

6. Conclusion

Ensuring data security in the cloud platforms is an important requirement towards the rising dependence on shared and distributed infrastructure for storing and processing sensitive information. Encryption is a fundamental mechanism for safeguarding data in the cloud; however, it cannot be ignored as it affects the performance of the systems. The analysis presented in this article shows that the choice of suitable encryption techniques must be able to carefully consider the security effectiveness and performance efficiency, especially in the cloud environment where not only scalability but also responsiveness is crucial. The results of the evaluation show that symmetric encryption techniques show good performance advantages because of their low computational overhead, which makes them appropriate for encrypting a performing volume of encrypted data in the cloud. However, their dependence on the secure key management introduces some problems in the case of multi-user and distributed environments. Asymmetric encryption techniques provide greater security capabilities such as security key exchange and authentication, but their computational cost restricts their use for direct encryption of bulk data in cloud platform. Hybrid encryption approaches become a sensible solution covering the shortcomings of symmetric and asymmetric encryption in certain ways. By forming a hybrid of efficient data encryption and secure key management, the hybrid techniques offer better security while making the usage of data acceptable in terms of performance. The results confirm that hybrid encryption is especially suitable for cloud platforms that need to accommodate various types of workloads, multiple users and strict security requirements. Overall, the findings emphasize the fact that no single encryption technique is best for all cloud applications. Instead, the selection of the encryption strategies should be dictated by the requirements of the application, the sensitivity of the data, as well as the constraints regarding performance. A balanced evaluation of security and performance helps cloud service providers and systems designers to deploy encryption mechanisms that support secure, scalable and efficient cloud operations. Future work may explore options for adaptive encryption strategies and real-world cloud deployments in order to increase security even further and also optimize performance.

References

1. Armbrust, M., et al. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58.
2. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1–11.
3. Ristenpart, T., et al. (2009). Hey, you, get off of my cloud. *ACM CCS*.

4. Zhang, Q., Chen, M., Li, L., & Li, Z. (2014). Security and performance evaluation of cloud data encryption. *Future Generation Computer Systems*.
5. Li, J., Chen, X., & Li, M. (2013). Secure data sharing in cloud computing. *IEEE Transactions on Cloud Computing*.
6. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*.
7. Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *STOC*.
8. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges. *Journal of Network Security*.
9. Stallings, W. (2017). *Cryptography and Network Security*. Pearson.
10. Kumar, R., & Rajalakshmi, S. (2016). Hybrid encryption for secure cloud storage. *Procedia Computer Science*.
11. Kaufman, L. (2009). Data security in the world of cloud computing. *IEEE Security & Privacy*.
12. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*.
13. Al-Hamami, A., & Al-Jamali, S. (2018). Lightweight encryption for cloud applications. *International Journal of Computer Science and Security*.
14. Kaur, G., & Singh, M. (2019). Performance analysis of encryption algorithms in cloud. *Journal of Cloud Computing*.
15. Rashi, A., & Madamala, R. (2022). Minimum relevant features to obtain an explainable system for predicting breast cancer. *Journal of Healthcare Engineering*.
16. Rachiraju, S. C., & Revanth, M. (2020). Feature extraction and classification using advanced machine learning models. *International Journal of Computer Applications*.