Kongunadu Research Journal **12 (1): 33-37, 2025** ISSN 2349-2694, All Rights Reserved,

Publisher: Kongunadu Arts and Science College, Coimbatore. https://krjournal.com/index.php/krj/article/view/678

DOI:10.26524/krj.2025.6

RESEARCH ARTICLE

Fortifying the Cloud for Comprehensive Survey of Data Protection Strategies and Emerging Challenges

[*1]Dr. S. Velmurugan

Assistant Professor, Department of Computer Science with Data Analytics,
Kongunadu Arts and Science College, Coimbatore, Tamilnadu, India
Email: svelmurugan_cs@kongunaducollege.ac.in

ABSTRACT

This paper presents a survey on the adoption of cloud use has increased among researchers, academia, government, and enterprises. Cloud advantages includinginitial investment, ideal scalability, and a variety of services are driving this trend. The cloud has many benefits, but data protection is a major problem in cloud computing and information security. Numerous strategies have been developed to address information security. These remedies exist, but the literature lacks a detailed study of their efficacy. This gap highlights the necessity to identify and assess the current body of work to see whether these solutions fit certain needs. This article fills this gap by meticulously examining cutting-edge cloud data exchange and protection approaches. Each approachis examined for its information security functions, potential breakthrough solutions, workflow, successes, scope, gaps, future directions, and more. A detailed assessment thatcompares methodologies is vital to the article. This review reveals method strengths and flaws. Then, these strategies' suitability for certain needs is addressed. The article finisheswith a discussion of research gaps and future perspectives, inspiring prospective researchers to study and contribute to safe cloud data management.

Keywords: Cloud Computing, Data Protection, Information Security, Cloud Security Strategies, Future Challenges in Cloud Adoption.

1.Introduction

Information is widely regarded as the most vital asset for any organization, defining the uniqueness of each enterprise. Data forms the essential foundation for generating information, building knowledge, and making informed decisions, impacting everything from disease treatment [1] to revenue growth and performance enhancement. To optimize their operations, organizations rely heavily on data analysis, sharing, and storage. However, as information continues to expand rapidly, organizations face significant challenges in managing large volumes of data locally, especially [2] when limited resources hinder data exploration. Cloud services offer a solution, providing accessible, flexible, scalable, and reliable support for data storage and sharing.

Figure 1 illustrates various functionalities and methodologies used in Secure Data Storage and Sharing Techniques for data protection.

Despite the numerous advantages of cloud computing, it faces challenges that could hinder its growth if left unaddressed. For example, when a company enables its employees or departments to use the cloud for data storage and sharing [6], it reduces the load of local data management but also introduces security risks, a major concern for cloud users. By outsourcing data to cloud servers, organizations lose a degree of control, which can be unsettling, particularly when sensitive information is involved. Furthermore, data sharing in open environments exposes cloud servers to potential attacks, increasing the risk of unauthorized access and the possibility of user data being misused for illegal purposes. Additionally, the need to share data with various stakeholders, both inside and outside the organization, introduces [8] potential risks. There is concern that the receiving party may misuse or intentionally disclose shared data to unauthorized third parties, jeopardizing data integrity and security. Effectively addressing these security challenges is essential for fostering the continued growth and widespread adoption of cloud computing.

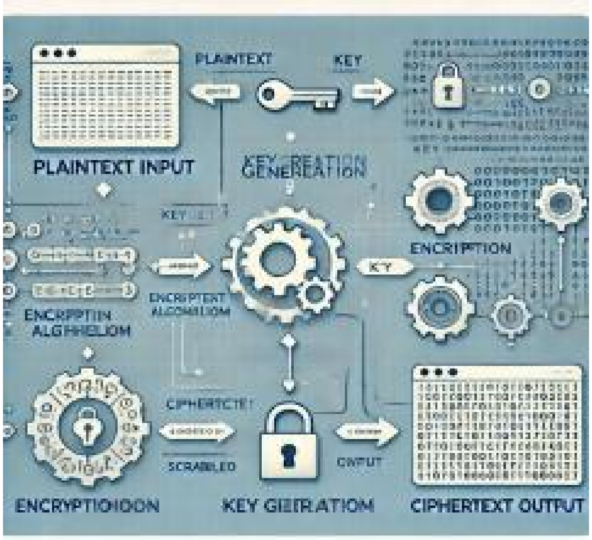


Figure 2: Overview of Secure Data Storage and Sharing Techniques for Data Protection

Figure 2 illustrates the detailed process of encryption. In our survey paper, we reference various studies, each focusing on specific components of this system. The encryption process is composed of well-defined phases, including key expansion, key mixing, and the substitution-permutation network (SPN) [8] transformation ages collectively strengthen the security of the algorithm by adding complexity and obscuring the relationship between plaintext and ciphertext. The substitution phase introduces a non-linear layer, using a fixed substitution table (S-box) to replace bytes, which is crucial for defending against cryptanalysis attempts.

I. RELATED WORK

Kao et al. introduced a user-centric key management system for cloud security that leverages RSA encryption to secure data by indirectly using users' public keys, with private keys stored only on users' mobile devices rather than on servers or personal computers. In this system, the private key can be represented as a two-dimensional (2D) barcode image for decrypting sensitive information. Al-Haj et al. proposed two cryptographic methods that ensure data security, privacy, and verifiability. They devised an approach that combines hash codes and symmetric keys, with digital signatures based on the elliptic curve method to reinforce data integrity and authenticity. To further enhance security and confidentiality [9], their approach integrates the Whirlpool hash function with the advanced encryption standard in Galois counter mode. Liang et al. introduced a proxy re-encryption technique using ciphertext rules to enable secure data transmission in the cloud, focusing on reducing the computational and communication resources required for re-encryption [10]. This method allows data owners to selectively grant access to encrypted data in the cloud. Wang et al. proposed an encryption technique utilizing file hierarchy features to secure cloud-stored data through filter hierarchy-ciphertext policy-attribute based encryption (FH-CP-ABE). Proven secure against selected plaintext attacks (CPA) via Decisional Bilinear Diffie-Hellman (DBDH), this scheme uses a layered access control method to streamline the management of hierarchical files. However, it presents a challenge in dynamically increasing computation costs when integrating features and generating unified ciphertext.

Liu et al. introduced an equitable key rebuilding mechanism to prevent unauthorized data access in cloud storage [11]. Their approach generates numerous decoy keys to obscure the decryption key, ensuring each user's contribution remains integral to accessing shared data. Although the authentication process could be more efficient, the approach reduced computation time and communication costs.

Additionally, Liu et al. developed a CP-ABE approach to address the escalating computational demands placed on users by complex access policies. This solution supports outsourced decryption, user attribute revocation [12], and rule modification. While effective in managing performance metrics related to processing and storage, it does have limitations in terms of privacy protection.

II. PROPOSED SYSTEM

The current focus on this topic highlights information security and cloud computing. A major concern is the absence of a thorough evaluation of existing methods addressing this issue. This informational gap necessitates the study [13], analysis, and assessment of significant previous research to determine if these solutions fulfill specific requirements. There are several issues with the current approach.:

The lengthy processing times may make it unsuitable for applications requiring immediate or real-time responses.

Insufficient security: Existing systems do not provide adequate protection, potentially jeopardizing data integrity and confidentiality.

The method does not guarantee the privacy of sensitive information.

The proposed technique can enhance the security of cloud storage and sharing. We apply encryption to all actions using access control and cryptographic techniques, including SHA-256 hashing and [14] encryption methods. This approach ensures that textual information remains accurate and confidential. Data protection is achieved through hashing, with SHA-256 providing robust cryptography [15]. Various techniques are employed to develop a secure and advanced cloud storage and transmission system for sensitive information. Researchers have developed and refined data security solutions for various cloud applications. Common data protection strategies focus on preventing data leakage and identifying unauthorized [16] disclosures. This article addresses methods for preventing data breaches and identifying the responsible parties. Most data leakage prevention strategies involve customized encryption and access control measures.

III. MODULE DESCRIPTION

A proposed approach for secure data storage and exchange involves implementing a modular structure that clearly outlines the roles and responsibilities [17] of the cloud service provider, data owner, and data consumer.

Cloud Service Providers (CSPs):

The CSP establishes a strong framework for data security by enforcing strict access controls and encryption protocols within the cloud environment. Security Compliance: The CSP ensures compliance with regulations and legislation designed to protect data. Regular audits and assessments aim to identify and rectify any security vulnerabilities. The CSP must implement and routinely update a reliable backup and recovery system to guarantee [18] that, in the event of data loss or a security incident, data can be restored quickly and effectively without damage. The cloud environment is continuously monitored by incident response systems to detect any suspicious activities. Additionally, the CSP develops and evaluates an incident response plan to ensure timely detection and resolution of security issues.

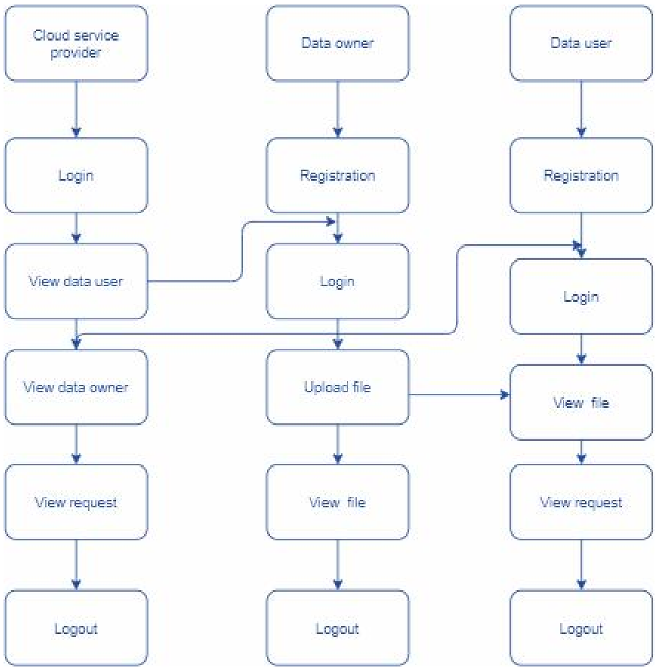
Data Owners:

The data owner categorizes data based on its importance and sensitivity, subsequently applying encryption to protect it. This encryption safeguards data during transmission and storage, ensuring that only authorized users can access it. The data owner controls access permissions using security mechanisms such as multi-factor authentication and role-based access control (RBAC) [19], ensuring that only individuals with proper authorization can manage confidential information. The data owner defines and enforces sharing rules, specifying who has permission to access certain data and how it can be accessed. Secure methods of sharing are utilized to oversee and monitor data dissemination. Data owners are also responsible for ensuring compliance with data protection regulations, such as GDPR and HIPAA, and they educate users on enhancing their internet security.

Data Users:

Users must securely authenticate themselves before accessing data, with their access determined by the permissions set by the data owner. Multi-factor authentication enhances security during this process. Data Security: Users are educated on how to securely store and transmit data, emphasizing the importance of protecting sensitive information. By adhering to sharing restrictions, data users help prevent unauthorized transmissions. Creating a Security Incident Report: Data users are responsible for promptly notifying the Cloud Service Provider (CSP) [20] and the data owner of any suspicious security activities. This enables a swift response according to the incident response strategy. This approach leverages the critical roles of each component to safeguard information and establish a robust data security framework, ensuring a collaborative and comprehensive strategy for secure data storage and sharing.

Figure.3. Workflow of Module Description



IV. RESULT AND DISCUSSION

The system's functionality relies on secure methods for data storage and transfer. It is essential for the system to generate data user keys. The effectiveness of data protection measures is assessed by comparing the expected results with actual outcomes. During inactive periods, no data should be in use, ensuring its protection remains confidential. It is recommended to employ AES-256 encryption before storing sensitive data in the cloud. Access to the contents of the storage system is restricted to those with the necessary decryption keys, preventing unauthorized physical access. Data transmitted between the client and the cloud is secured using SSL and TLS, allowing for communication without interception. For comprehensive functionality testing, all features and capabilities specified in user manuals, system documentation, and business and technical requirements must be addressed. Full functional testing safeguards all system documentation.

Processing illegal input is unacceptable, and it is impossible to ignore certain types of erroneous data. All responsibilities must be upheld, and the application's output should be checked for accuracy. The outcome of key generation involves unique test cases, critical functionalities, and requirements as part of functional testing. Every step, data field, method, and action within a company's process should undergo rigorous testing. Before concluding functional testing, the relevance of previous tests and the necessity for new tests must be evaluated.

V. CONCLUSION

There have been several attempts to address and alleviate the worries around the enormous problem of guaranteeing data protection in the context of cloud computing and information security. The literature is noticeably lacking in a complete examination of the available solutions, despite the volume of effort committed to solving this topic. To fill this need, this article presents an in-depth evaluation of the most popular methods for safe data sharing in the cloud, with the goal of bolstering data security there. The report dives intothe practicality and relevant solutions linked to each method, going beyond a cursory review. The main components of each approach are shown, together with study gaps and potential avenues for further investigation, thanks to the inclusion of critical and adequate facts. In addition, in order to find out what works and what doesn't, the study compares and analyses all of the above methods extensively. An in-depth analysis of each method's usefulness in the complicated cloud data security environment is provided by analyzing it within the given context.

REFERENCE

1. K. Singh and I. Gupta, "Online information leaker identification scheme for secure data sharing," *Multimedia Tools Appl.*, vol. 79, no. 41, pp. 31165-31182, Nov. 2020.
2. E. Zaghloul, K. Zhou, and J. Ren, "P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing," *IEEE Trans. Big Data*, vol. 6, no. 4, pp. 804-815, Dec. 2020.
3. I. Gupta and A. K. Singh, "GUIM-SMD: Guilty user identification model using summation matrix-based distribution," *IET Inf. Secur.*, vol. 14, no. 6, pp. 773-782, Nov. 2020.
4. W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 331-346, Feb. 2019.
5. I. Gupta and A. K. Singh, "An integrated approach for data leaker detection in cloud environment," *J. Inf. Sci. Eng.*, vol. 36, no. 5, pp. 993-1005, Sep. 2020.
6. R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, "A lightweight secure data sharing scheme for mobile cloud computing," *IEEE Trans. Cloud Comput.*, vol. 6, no. 2, pp. 344-357, Apr. 2018.
7. I. Gupta, N. Singh, and A. K. Singh, "Layer-based privacy and security architecture for cloud data sharing," *J. Commun. Softw. Syst.*, vol. 15, no. 2, pp. 173-185, Apr. 2019.
8. J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, et al., "An efficient attribute-based encryption scheme with policy update and file update in cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6500-6509, Dec. 2019.
9. C. Suisse, "2018 Data Center Market Drivers: Enablers Boosting Enterprise Cloud Growth," May 2017. [Online]. Available: https://cloudscene.com/news/2017/12/2018-data-center-predictions/.
10. I. Gupta and A. K. Singh, "A framework for malicious agent detection in cloud computing environment," *Int. J. Adv. Sci. Technol.*, vol. 135, pp. 49-62, Feb. 2020.11.
11. Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 1, pp. 72-83, Jan./Feb. 2019.
12. I. Gupta and A. K. Singh, "A probabilistic approach for guilty agent detection using bigraph after distribution of sample data," *Proc. Comput. Sci.*, vol. 125, pp. 662-668, Jan. 2018.
13. L. Zhang, Y. Cui, and Y. Mu, "Improving security and privacy attribute-based data sharing in cloud computing," *IEEE Syst. J.*, vol. 14, no. 1, pp. 387-397, Mar. 2020.
14. I. Gupta and A. K. Singh, "Dynamic threshold based information leaker identification scheme," *Inf. Process. Lett.*, vol. 147, pp. 69-73, Jul. 2019.
15. S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1265-1277, Jun. 2016.
16. I. Gupta and A. K. Singh, "SELI: Statistical evaluation based leaker identification stochastic scheme for secure data sharing," *IET Commun.*, vol. 14, no. 20, pp. 3607-3618, Dec. 2020.
17. W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, "Attribute-based access control with constant-size ciphertext in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 5, no. 4, pp. 617-627, Oct./Dec. 2017.
18. I. Gupta and A. K. Singh, "A probability-based model for data leakage detection using bigraph," *Proc. 7th Int. Conf. Commun. Netw. Secur. (ICCNS)*, pp. 1-5, 2017.
19. L. Columbus, "83% of Enterprise Workloads Will Be in the Cloud by 2020," Jan. 2018. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise workloads-will-be-in-the-cloud-by-020/#50d375286261.
20. Gartner, "Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019," 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-world wide-public-cloud-revenue-to-grow-17-percent-in-2019.

About The License