INTI JOURNAL | Vol.2024:15
eISSN:2600-7320

Authorized Redundant Check Support in a Hybrid Cloud Environment

Durgadevi[1], Shreedhara N Hegde[1], Zuriani Hayati Abdullah[2]

[1]Dayananda Sagar Academy of Technology and Management, Karnataka, India.
[2]Faculty of Data Science and Information Technology, INTI International University, 71800 Nilai, Negeri Sembilan, Malaysia

***Email:** durganayak2727@gmail.com

Abstract

A hybrid cloud is made up of public and private clouds connected by standardized or proprietary technologies to provide data and application mobility. The deduplication with uneven privileges issue in cloud computing is addressed efficiently. an architecture for a hybrid cloud that employs both public and private clouds, with the data owners only using the public cloud for storage and the private cloud for data administration. To make data management in cloud computing scalable, duplication has lately become a commonly employed method. Deduplication reduces the amount of bandwidth you need, speeds up data transfers, and keeps your need for cloud storage to a minimum. To enable authorized duplicate checks in hybrid cloud architecture, the proposed system comprises a variety of new deduplication structures. Data confidentiality was protected before outsourcing by employing the convergent encryption method. A system authorized to use deduplication supports differential authorization duplicate checks. In the authorized duplication check approach, testbed tests are carried out using a prototype as proof of concept**.**

.

Keywords

Data De-duplication, Convergent Encryption, Confidentiality, Hybrid Cloud, Authorized Duplicate Check.

Introduction

Organizations are increasingly using hybrid cloud systems in today's digital world, fusing the advantages of public and private clouds with their own on-premises infrastructure. However, maintaining the security and integrity of data across these many contexts presents difficulties. Implementing approved redundant check support is a crucial part of data management in hybrid cloud architectonics (C. Ng & P. Lee,2013).

Implementing techniques and procedures to verify and authenticate data as it travels between multiple cloud providers or between the on-premises infrastructure and the cloud constitutes authorized redundancy check support (J. Li et.al,2013). Organizations can reduce their exposure to the risks of data loss, unauthorized access, and manipulation by implementing redundant checks at various stages of data transit and storage.

Submission: 4 May 2024; **Acceptance:** 26 June 2024

The authorized redundant check support that may be used in a hybrid cloud context is described in this abstraction. This includes data encryption, safe data transport, data verification, data storage, recurring audits, and disaster recovery plans, among other processes that are necessary to protect data integrity. Organizations may create a solid foundation that guarantees consistency, correctness, and safety of data throughout their hybrid cloud environment by separating these operations.

According to the degree of de-duplication, secure data de-duplication may be categorised as file-level de-duplication, block-level de-duplication, client de-duplication, and server de- duplication. In this study, we concentrate on server-side file-level secure de-duplication. Server de-duplication mandates users encrypt data files before transferring them to cloud servers to safeguard their privacy. Disappear et al. [1] proposed convergent encryption, which can effectively balance data de-duplication and data encryption to achieve secure de- duplication in the ciphertext. It computes the hash value of files as the key of encrypted files. The same file will generate the same key, and encrypting the same file with the same key will generate the same ciphertext, thus realizing the direct comparison of the duplicity of files in the ciphertext state. Through this mechanism, we can see that the key generated using the file does not have randomness, and each file will generate a key, which will lead to the problem of key management [2-5]. In order to increase the security and effectiveness of convergent encryption [6-7], Bellare et al. [8] developed the variant convergent encryption algorithms HCE1, HCE2, and HCE3. Convergent encryption checks if the file is duplicated by the ciphertext and uses the file hash value as the encryption key. Convergent encryption has been further enhanced by Message Locking Encryption (MLE). MLE creates a de-duplication tag for the file. The file encryption key is generated by MLE using a variety of methods in addition to the file hash. The file is mapped by a deterministic function, which is vulnerable to brute force assaults on predictable information, before the encryption key is created. The tag and encryption key are separate entities not connected in any way. Keelveedh et al developed a solution to the issue. The server-assisted secure data de-duplication method known as DupLESS, which was previously introduced by [9], significantly enhances the unpredictability of deterministic ciphertexts. Abadi and other people. To increase the security of data de-duplication, [10] built MLE2 for lock-dependent messages based on MLE. Liu and co.

Methodology

Implementing authorized redundancy checks to support the hybrid cloud environment necessitates a methodical approach to guarantee data security and integrity throughout the data lifecycle. Here is an approach that businesses may use:

Determine Privacy Specifications: To start, determine the precise privacy and compliance criteria that apply to your company and sector. This will make it easier to decide what data protection measures, such as redundant check support, are required.

Know the whole lifespan of your data, from its development or acquisition to its final destruction or archiving. Processes for creating, sending, storing, and retrieving data are included in this throughout the hybrid cloud environment.

Conduct a thorough risk analysis to detect any weaknesses or risks to the integrity of your data in your hybrid cloud arrangement. Data transport, storage, access restrictions, and disaster recovery should be considered during this review.

Choose redundant check techniques: Select the most appropriate redundant check methods to guarantee data integrity. This might use techniques like digital signatures, cryptographic hashes, checksums, or other verification procedures. Think about things like processing overhead, performance effect, and compatibility with your hybrid cloud infrastructure.

Data encryption should be used to safeguard data privacy during transmission and storage. Set up safe key management procedures and select powerful encryption methods. Both at rest and in transit, encryption needs to be used.

Flow Chart:

The private cloud manages the private keys for the privileges and responds to user requests for file tokens using this interface, which enables users to submit files and queries for safe storage and computation, respectively.

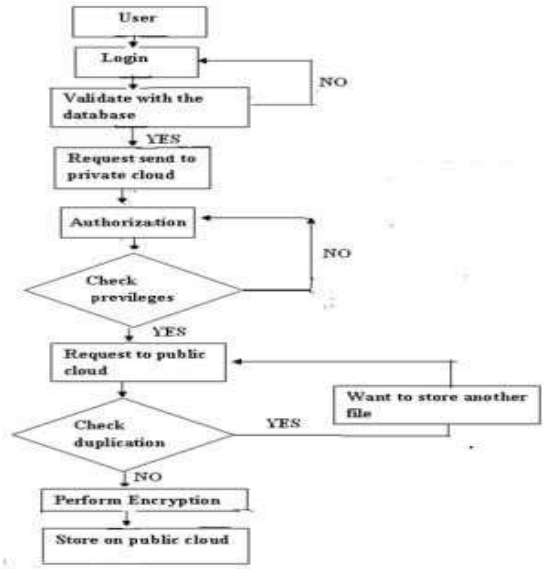

Figure 1. Flow Chart

Hybrid cloud architectonics is used in de-duplication systems to address file de-duplication. Users will not be given access to the private keys for privileges directly; instead, the private cloud server will store and manage them. To obtain a file token, the user must submit a request to the private cloud server. To execute a duplicate file check, the user needs to obtain the file token from the private cloud server. Either the user uploads this file or provides proof. According to the findings of the duplication check, their ownership If it is successful, the private cloud server will locate the user's matching rights from a list of stored tables and send them to the user, allowing them to upload files. The user can download his file from cloud storage in the same way.

Conclusion

Organizations have confidence in the dependability and legitimacy of their data thanks to authorized redundant check support in a hybrid cloud environment. It supports effective data management, safe access to sensitive information, and seamless collaboration. Providing authorized redundancy check support is becoming more essential for data security and preserving the overall integrity of the hybrid cloud architecture as businesses continue to use hybrid cloud models.

Acknowledgments

The authors would like to express our heartfelt gratitude to Dayananda Sagar Academy of Technology and Management (DSATM) for providing us with the necessary resources and facilities to conduct this research project on "Authorized Redundant Check in Hybrid Cloud Environment". The support and encouragement from the institution have been instrumental in the successful completion of this endeavor.

References

Stanek, J., Sorniotti, A., Androulaki, E., Kencl, L. (2014). A Secure Data Deduplication Scheme for Cloud Storage. In: Christin, N., Safavi-Naini, R. (eds) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science(), vol 8437. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_8

Bellare, M., Keelveedhi, S., & Ristenpart, T. (2013). Message-locked encryption and secure deduplication. In *Advances in Cryptology – EUROCRYPT 2013* (Lecture Notes in Computer Science, Vol. 7881, pp. 296–312). Springer. https://doi.org/10.1007/978-3-642-38348-9_18

Bellare, M., Keelveedhi, S., & Ristenpart, T. (2013). DupLESS: Server-aided encryption for deduplicated storage. In *22nd USENIX Security Symposium (USENIX Security 2013)* (pp. 179–194). USENIX Association.

Chen, X., Li, J., Li, M., Li, J., Lee, P. P. C., & Lou, W. (2013). Secure deduplication with efficient and reliable convergent key management. *IEEE Transactions on Parallel and Distributed Systems, 24*(6), 1190–1208. https://doi.org/10.1109/TPDS.2013.284

Ng, C. H., & Lee, P. P. C. (2013). RevDedup: A reverse deduplication storage system optimized for reads to latest backups. In *Proceedings of the 4th Asia-Pacific Workshop on Systems (APSYS)* (pp. 1–9). ACM. https://doi.org/10.1145/2500727.2500731

Storer, M. W., Greenan, K., Long, D. D. E., & Miller, E. L. (2008). Secure data deduplication. *Proceedings of the 4th ACM International Workshop on Storage Security and Survivability (StorageSS '08)*, 1–10. Association for Computing Machinery. https://doi.org/10.1145/1456469.1456471

Xu, J., Chang, E.-C., & Zhou, J. (2013). Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIA CCS '13)*, 195–206. Association for Computing Machinery. https://doi.org/10.1145/2484313.2484340

Yuan, J., & Yu, S. (2013). Secure and constant cost public cloud storage auditing with deduplication. *IACR Cryptology ePrint Archive, 2013*, 149. https://doi.org/10.1109/TPDS.2013.284

Zhang, K., Zhou, X., Chen, Y., Wang, X., & Ruan, Y. (2011). Sedic: Privacy-aware data intensive computing on hybrid clouds. *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS '11)*, 515–526. Association for Computing Machinery. https://doi.org/10.1145/2046707.2046767