Phoenix: International Multidisciplinary Research Journal
Vol 1, No. 3, July-Sep, 2023
ISSN:2583-6897

DUAL ACCESS CONTROL FOR CLOUD-BASED DATA STORAGE AND SHARING

First Author[1], Second Author[2]

[1] *Arati, Master of Computer Application BKIT-Bhalki*
[2]Prof . Yogesh G V,, Master of Computer Application BKIT-Bhalki

Abstract -Due to its efficiency and low cost administration, cloud-based data storage service has attracted rising attention from both academia and business in recent years. Given that it operates on an open network, it is critical that service providers use safe methods of storing and exchanging customer data. Encryption is the most popular approach for keeping private information that way. However, the actual need of data management cannot be completely met by just encrypting data (e.g., using AES). So that Economic Denial of Service (EDoS) attacks cannot be performed, it is also important to think about how to effectively manage access to download requests. We create a control mechanism over both data access and download request without sacrificing security or efficiency, and we discuss the dual access control in the context of cloud-based storage. This article presents the design of two different dual access control systems, each tailored to a specific environment. Additionally, the systems' experimental analysis and security findings are detailed..

***Key Words*:** Dual Access Control for Cloud-Based Data Storage and Sharing

1.INTRODUCTION

Recently, cloud storage services have garnered a lot of interest from both enterprises and universities. Many web-based programs (like Apple's iCloud) make use of this because of a plethora of advantages, such as easy accessibility and no need for stringent data management. Most companies and individuals nowadays choose to store their data on faraway clouds. This way, they won't have to replace any of their current on-site hardware or database management systems. The most significant barrier to mass adoption of cloud storage services among Internet users is the concern that their data may be compromised if stored remotely. In many practical situations, the outsourced information may be shared with others afterwards. For instance, Alice may use Dropbox to transmit her photos.

Before data is encrypted, it is necessary to identify the group of authorized users. To safeguard against "insiders" reading shared images with access to the system. However, Alice may not always know who will be seeing her images. Alice, being a single person, probably knows what makes a good camera receiver. Since it is not possible to determine the identity of the data's encryptor in advance, traditional public key encryption methods like Paillier encryption cannot be employed here. For Alice to be able to control who has access to her encrypted images, it is preferable to have policy-based encryption techniques available for external photos. Only those who have been granted access will be able to see the pictures.

A rudimentary method for verifying download requests is to use fake ciphertexts to guarantee the recipient has the necessary rights to decode the material. To be more precise, Alice, the data's owner, must also upload some "test" ciphertexts to the cloud, where the "real" data encryption already resides. Access to encrypted fake messages is just as restricted as to "real" data. Cloud solicits Bob, a user, to randomly download and decode one of the "test" ciphertexts. If the decryption is successful or returned to Alice, then Bob has valid authority in decrypting the "current" data. Bob is now able to access the appropriate ciphertext in the cloud.

2. Literature survey:

As a primary function of storage services, data synchronization (sync) enables the client to automatically update local file changes to the remote through network communications. Mobile storage services have gained phenomenal success in recent few years. In this paper, we identify. For example, a minor document editing process in Dropbox may result in sync traffic 10 times that of the modification. Synchronization efficiency is

determined by the speed of updating the change of client files to the , and considered as one of the most important performance metrics for storage services. We further implement QuickSync to support the sync operation with Dropbox and Seafile. Our extensive evaluations demonstrate that QuickSync can effectively save the sync time and reduce the significant traffic overhead for representative sync workloads.

Using computing, individuals can store their data on remote servers and allow data access to public users through the servers. As. This, however, significantly limits the usability of outsourced data due to the difficulty of searching over the encrypted data. In this paper, we address this issue by developing the finegrained multi-keyword search schemes over encrypted data. Our original contributions are three-fold. First, we introduce the relevance scores and preference factors upon keywords which enable the precise keyword search and personalized user experience. [6]. simply encrypting the data may still cause other security concerns. For instance, Google Search uses SSL (Secure Sockets Layer) to encrypt the connection between search user and Google server when private data, such as documents and emails, appear in the search results. We have investigated on the fine-grained multi keyword search (FMS) issue over encrypted data, and proposed two FMS schemes. The FMS I includes both the relevance scores and the preference factors of keywords to enhance more precise search and better users' experience, respectively. The FMS II achieves secure and efficient search with practical functionality, i.e., "AND", "OR" and "NO" operations of keywords.

Computing has been envisioned as the nextgeneration architecture of IT Enterprise. This work studies the problem of ensuring the integrity of data storage in Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the client, to verify the integrity of the dynamic data stored in the . The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the indeed intact, which can be important in achieving economies of scale for Computing. Although envisioned as a promising service platform for the Internet, this new data storage paradigm in "" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with data storage is that of data integrity verification at untrusted servers. Although schemes. Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. In the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks.

Handling of Big Data and computing are the two important prime concerns which have become more and more popular in recent years. In this paper, we Cloud File System is a client-based application which permits its users to access, process and modify the data which isstored on a remote server as if it existed on their local systems. Centralized cache management is a mechanism which significantly improves the Query response time of the file system. It allows users to specify paths to be cached in main memory by HD-FS. In this, the Name Node will communicate with its Data Nodes that have analyzed the evolution of cloud file systems, their origin, specialty and their development. We started our discussion with the analysis of Network File system and Andrew File System. We have also discussed the detailed architectures of GFS and HDFS, the two most significant cloud file systems of their time capable enough to handle the Big Data Management. A comparative study between both GFS and HDFS has been done which has resulted in the occurrence of some similarities as well as differences between both GFS and HDFS.

4. SYSTEM ANALYSIS:

Existing System:

1. A single, reliable party that stores all of the data and monitors all of the qualities.

2. We begin by going through some of the most significant identity-based encryption, signature, and encryption approaches.

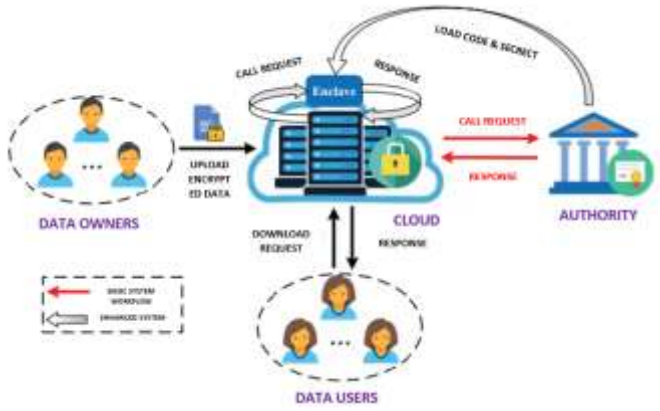
3. The issue may constitute a risk to the information owner's internal security system.

4. The taxonomy of attribute-based techniques covered significant criteria such as the access management mode, the design, the revocation mode, the revocation methodology, the revocation problem, and the revocation controller.

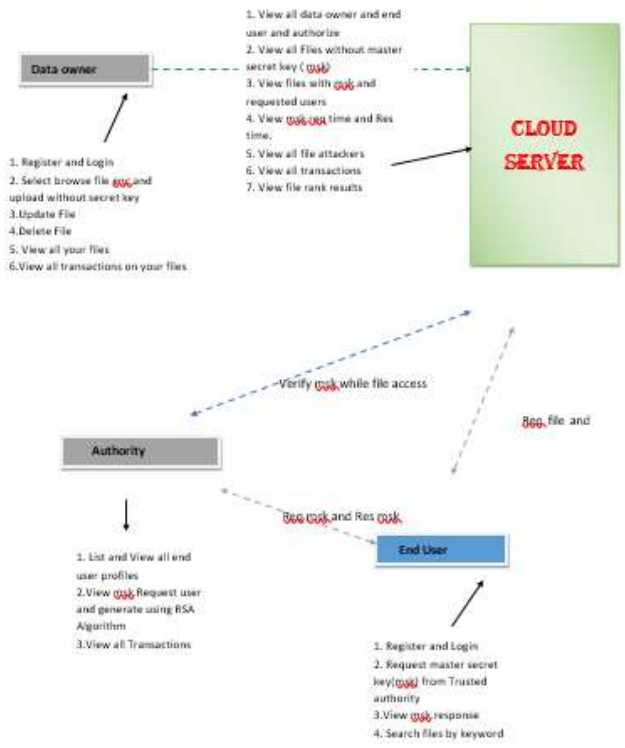
Proposed System

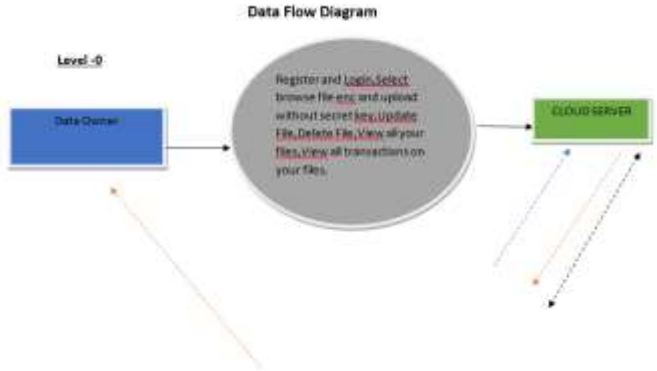
Offers regulated access based on context-specific details. In this context, users who choose to keep insured data specifically in the cloud will be allocated access controls and given anonymous authentication. [14]The production of a certain sort of key is the primary determinant of which users are granted access. Access policy details are provided, on which user profiles may be built. In this case, security is provided for user-type data via an attribute-based encryption method. Here, protection of data is based on access policy and access control method[10]. To minimize, neutralize, or decrease the danger of security related to personal type, security type controls are guarded or countertype measures are adopted.

4. ARCHITECTURE



Architecture Diagram





6. Results and Analysis:

This Survey offers a two-tiered approach of data security. Confidentiality of outsourced data is made possible with the help of Attribute based encryption (ABE). Those interested in applying and those who need fine-grained management over their data that has been outsourced would find this useful. Cloud services provide a safe place to store the data backups.
In particular, the CP-ABE may offer a trustworthy means of encrypting data. Allows the recipient of encrypted material to get access based on the rules it specifies. The value and utility of the CP-ABE approach may be explored in this research. The system's reliance on CP-ABE provides granular management of user requests for both data and downloads. The following are examples of how the fake ciphertext may be used to check the legitimacy of a recipient's data: The requests' management and download processes are managed by the Crude Solution. Data may be uploaded to the cloud with "real" encryption using "test" Ciphertexts that encrypt communications according to comparable standards seen in "real" clouds.
If user Bob wants to download an encrypted file, the cloud may communicate with Bob and tell him how to unlock the file. Alice and Bob "test" the ciphertext, and if the result is valid (if Bob's decryption is privileged), they grant the user permission to retrieve the data from the cloud.

Conclusion:
We covered a broad variety of ground by adopting two separate techniques for controlling access. The suggested system is resistant to DoS and EDOS assaults. We contend that distinct CP-ABE architectures have the potential to "port" existing implementation techniques. Management of download requests. Our investigations show that the suggested solution does not need much more computational or communication effort (than the underlying CP-ABE) than the baseline. One benefit of enclaves is that they may be used to store secret data, from which a hardened system would be unable to get it. Memory access patterns or comparable channel assaults may be used to stop an enclave from disclosing sensitive information to the host. As a result, it fosters openness and improves enclave execution. Developing a two-factor authentication system for cloud-based data storage and data exchange via transparent enclaves is an intriguing challenge.

ACKNOWLEDGEMENT

The heading should be treated as a 3rd level heading and should not be assigned a number.

REFERENCES

[1]. Ittai Anati, Shay Gueron, Simon Johnson and Vincent Scarlata. Innovative technology based on processor certificat ion and sealing.Hardware and Architectural Assistance for Security and Privacy (HASP) Workshop,Volume 13, Pa ge 7. ACM New York, NY, USA, 2013.
[2]. Jiguo Li, Xiaonan Lin, Yichen Zhang and Jingguang Han. Ksfoabe: Outsourced signature-based encryption with keyword search for cloud storage. IEEE Transactions on Service Computing,10(5):715–725, 2017.

[3]. Alexandre Vacas and Antonis Michalas. Modern Family: A reversible hybrid encryption scheme based on the attribute cipher, symmetric lookup cipher, and SGX. In Secure Comm 2019, p. 472-486, 2019.
[4]. J. Ning, X. Huang, E. Susilo, K. Liang, X.Liu and Y. Zhang, "Dual Access Control for CloudBased Data Storage a ndShares", in IEEE Transactions on Trusted and Secure Computing, vol. 19, Number 2, p. 1036_1048, March 1- April 2022.
[5]. Byali, Ramesh & Jyothi, & Shekadar, Megha. (2022). "Dual Access ControlSecurity for CloudBased Data Sharing and Storage. International Journal of Research Publishing and Review. 170-172.