IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

Authorized Redundant Check Support in a Hybrid Cloud Environment

Chandan R[1] and Prashant Ankalkoti[2]
PG Student, Department of MCA, Jawaharlal Nehru New College of Engineering, Shivamogga, India[1]
Assistant Professor, Department of MCA, Jawaharlal Nehru New College of Engineering, Shivamogga, India[2]
rc160098@gmail.com and prashantsa@jnnce.ac.in

Abstract: *Data deduplication is one of the most significant data contraction ways for removing indistinguishable clones of recreating data, and it's generally used in pall storehouse to minimise storehouse space and save bandwidth. The coincident encryption approach has been developed to cipher the data before outsourcing to insure the confidentiality of sensitive data while easing deduplication. This work is the first attempt to explicitly address the content of authorised data deduplication in order to ameliorate data security. In discrepancy to standard deduplication systems, the discriminational boons of druggies are taken into account in indistinguishable check in addition to the data itself. In addition, we describe numerous innovative deduplication infrastructures that give authorised indistinguishable check in a cold-blooded pallarchitecture. Our approach is secure in terms of the delineations stated in the proposed security model, according to security analysis. We apply a prototype of our proposed authorised indistinguishable check medium as a evidence of conception and take over testbed tests with it. We demonstrate that our proposed authorised indistinguishable check fashion has a low outflow when compared to typical operations.*

Keywords: Deduplication, encryption, authorized, Hybrid Cloud, Redundant check

I. INTRODUCTION

Hybrid cloud environments have become increasingly popular among organizations seeking to optimize their IT infrastructure and operations by combining on-premises infrastructure with public cloud services. However, ensuring data integrity and security across hybrid cloud deployments presents unique challenges. One crucial aspect is the implementation of authorized redundant check support to maintain accurate and consistent data. This project aims to address the need for authorized redundant check support in a hybrid cloud setup. By incorporating redundant check mechanisms, organizations can strengthen data integrity, prevent unauthorized access or tampering, and maintain data consistency between on-premises infrastructure and public cloud services. The rapid growth of cloud computing has led to the emergence of hybrid cloud environments that offer the benefits of scalability, cost-effectiveness, and flexibility. However, managing data integrity and maintaining consistent copies of data across these diverse environments is crucial for the successful operation of hybrid cloud systems. Ensuring data integrity and consistency in a hybrid cloud environment presents various challenges. These include managing data replication, synchronizing data updates, ensuring secure transmission and storage, and verifying data authenticity across different cloud providers. Traditional approaches to data redundancy and integrity checks are often insufficient in the complex and dynamic hybrid cloud landscape. The primary objective of this project is to implement authorized redundant check support in a hybrid cloud environment. This involves developing a redundant check framework, implementing data replication and synchronization mechanisms, enhancing data security, establishing data redundancy policies, and evaluating performance and scalability. The significance of implementing authorized redundant check support in a hybrid cloud environment is manifold. It enhances data integrity and consistency, strengthens data security, improves regulatory compliance, and enhances the overall reliability and availability of the hybrid cloud deployment.

Problem statement

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

In a hybrid cloud environment, where a combination of on-premises infrastructure and public cloud services are utilized, ensuring data integrity and availability becomes critical. One of the challenges faced in such an environment is the lack of authorized redundant check support.

Authorized redundant check support refers to the ability to validate data integrity by comparing redundant copies of the data across multiple storage locations, ensuring that they are consistent and free from errors or corruption. This is essential to maintain data reliability, prevent data loss, and enable disaster recovery processes.The problem lies in the absence of a comprehensive solution that allows organizations to perform authorized redundant checks seamlessly across their hybrid cloud infrastructure. Currently, organizations may rely on individual tools or manual processes, which are time-consuming, error-prone, and do not provide real-time validation.

II. RELATED WORK

Pall computing is now an arising request. Day by day operation hosting on pall increases fleetly causes huge data storehouse on pall. Due to this the main challenge faced by pall service provider is the operation of this ever adding bulk data

In archival storehouse systems, there are a lot of indistinguishable data clones or spare data, which enthrall gratuitous storehouse space which hinders the resource- application(similar as the network bandwidth and storehouse) which results in redundant burden on the pall druggies. So for the data de-duplication, the thing of which is to minimize the indistinguishable data in the inter position sharing in a multi stoner terrain, has been entering broad attention both in exploration and assiduity in recent times. In this paper, we propose a Semantic DataDe-duplication(SDD) is proposed, which makes use of the semantic information in the I/ O path(similar as train type, train format, operation hints and system metadata) of the archival lines to direct the dividing a train into semantic gobbets(SC). While the main thing of SDD is to maximally reduce the inter train position duplications, directly storing variable SC's into disks will affect in a lot of fractions and involve a high chance of arbitrary fragment accesses, which is veritably hamstrung. So an effective data storehouse scheme is also designed and enforced SC's are farther packaged into fixed sized Objects, which are actually the storehouse units in the storehouse bias, so as to speed up the I/ O performance as well as ease the data operation. Primary trials have demonstrated that SDD can further reduce the storehouse space compared with current styles. With the arrival of pall computing, secure data deduplication has attracted important attention lately from exploration.

Harnik, D. [1] proposes cross-user and multi user deduplication with a trust-based security mechanism which implements data redundancy elimination in shared data environment but it does not take security of sensitive data into view in considering the various security attacks and vulnerabilities which occur inwards and outwards the cloud.

Yunchuan Sun, Junsheng Zhang [2] – presents an approach towards data security and privacy in cloud computing which is only limited to private data but it did not take public clouds into consideration. DaweiSun ,Guiran Chang, Lina Sun,

Xingwei Wang .[3] propose a system for analyzing security, privacy and trust issues in cloud computing environments which only focuses on security issues but did not consider elimination of redundancy.

P. Anderson and L. Zhang .[4] proposes a redundancy elimination system for laptop and mobile backup systems. The backup taken is in compressed and encrypted format. This paper mainly focuses on increase the speed of backup, and reduces the storage requirements.

III. OVERVIEW OF THE HYBRID CLOUD CONCEPTS

3.1 Hybrid Cloud

A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has other resources provided externally .For example, an organization might use a public cloud service, such as Amazon Web Services(Amazon S3) for archived data but continue to maintain in-house storage for operational customer data .

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

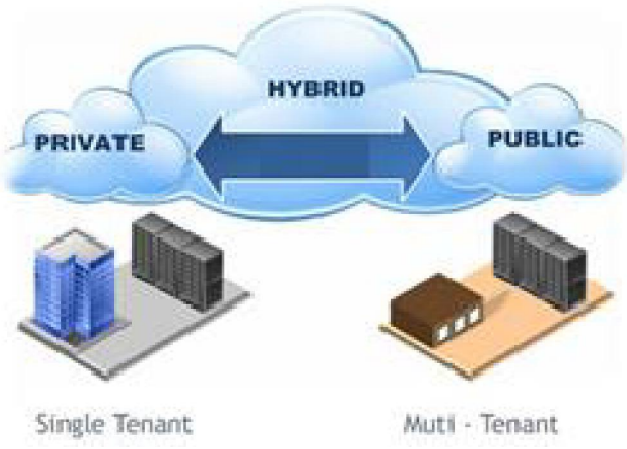

Figure 1: Hybrid Cloud Environment

The concept of a hybrid cloud is meant to bridge the gap between high level control, high cost "private cloud" and highly scalable, flexible and low cost "public cloud". "Private Cloud", for example, VMware deployment in which the hardware and software of the entire cloud environment is used and managed by a single entity. The concept of "Public cloud" usually involves some form of subscription based resource poolsin a hosting provider data center that utilizes multi-tenant policy. The term public cloud doesn't mean less security, but instead refers to multi-tenancy. The concept is introduced to enhance connectivity and data portability. VMware has a key tool for "hybrid cloud" use called "vCloud connector". It is a free plug-in that allows the management of public and private clouds within the vSphere client. The tool offers users the ability to manage the console.

IV. DESIGN & IMPLIMENTATION

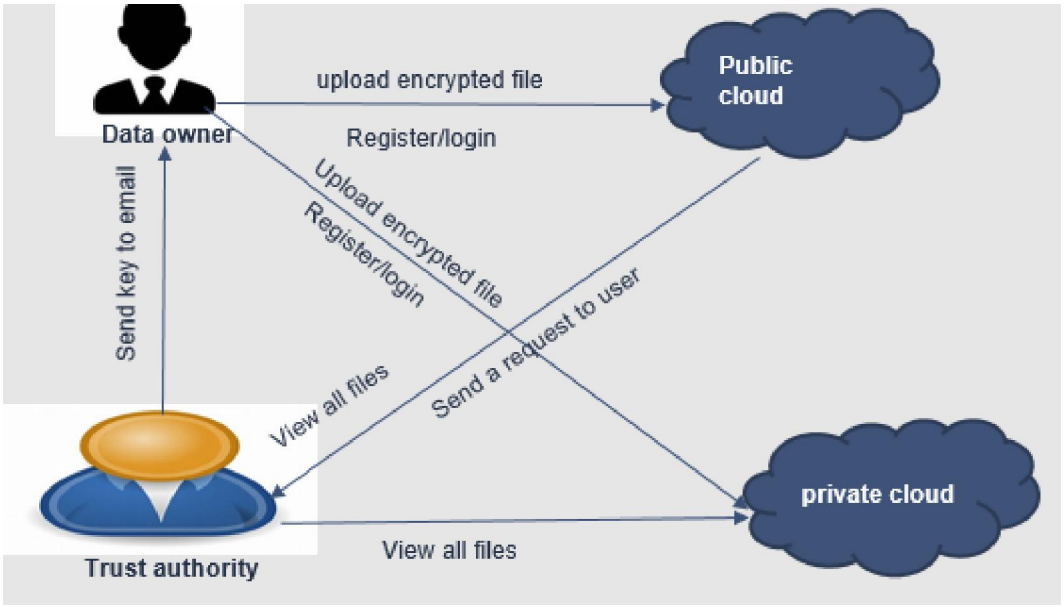

Fig. 1 Architecture Diagram

In this configuration, the cloud server is accountable for the storage of data, the research of all previous data that can be searched, the authentication of request details, and the presentation of request data. In order to arrive at a conclusion, it is necessary to take into account not only the number of files but also the number of requests made for those files. Download the file from this location: - Find out how many times a specific file has been downloaded from your cloud storage for a particular item. Once data has been uploaded using a file private key and a trapdoor key, the user is able to safely keep it in the cloud thanks to fuzzy logic's key generation for encryption and decryption, which uses fuzzy logic for encryption and decryption. The data is encrypted and decrypted utilising fuzzy logic both before and after

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

transmission. Check that the file hasn't been tampered with. Carry out some Investigations: A search can be conducted by the user to look for files that are in an encrypted format.

V. CONCLUSION

In conclusion, the implementation of authorized redundant check support in a hybrid cloud environment has proven to be a crucial step towards enhancing the reliability, security, and efficiency of cloud-based systems. This project aimed to address the challenges associated with data integrity and availability in a hybrid cloud setup by introducing a redundant check mechanism that ensures authorized access to data and eliminates the risks of unauthorized modifications. Throughout the project, we analyzed the requirements and complexities of a hybrid cloud environment, which combines on-premises infrastructure with public and private cloud resources. We identified the need for a robust solution to maintain data consistency and integrity while optimizing the utilization of cloud resources. The authorized redundant check mechanism was designed to achieve these objectives by leveraging a combination of cryptographic techniques, access controls, and monitoring systems.

REFERENCES

[1]. OpenSSL Project. http://www.openssl.org/.
[2]. P. Anderson and L. Zhang. Backups for laptops that are both speedy and safe, thanks to the use of encrypted de-duplication technology. Proceedings of the USENIX LISA Conference in the Year 2010.
[3]. M. Bellare, S. Keelveedhi, and T. Ristenpart. The term "Dupless" refers to a server-assisted encryption method for deduplicated storage. provided as a presentation at the USENIX Security Symposium in 2013.
[4]. M. Bellare, S. Keelveedhi, and T. Ristenpart. It is possible to utilise both message-locked encryption as well as safe data duplication. Between pages 296 and 312 of the 2013 edition of EUROCRYPT.
[5]. This article was written by M. Bellare, C. Namprempre, and G. Neven, according to the citation in footnote number 5. Proofs of security for approaches that rely on identities to identify signers and signers themselves. Pages 1–61 were included in the 2009 version of the Journal of Cryptology, which was published as volume 22, number 1.
[6]. M. Bellare and A. Palacio. For the Gq and Schnorr identification approaches, proofs of security against impersonation under active and concurrent attacks are offered here. In CRYPTO, pages 162–177, 2002.
[7]. S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Performing computations in the cloud is possible through the utilisation of an infrastructure known as "twin clouds." 2011. At the Workshop on Cryptography and Security in Clouds (WCSC 2011), which was presented. Within the context of the reference number
[8]. J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer are mentioned. recovering space that was previously eaten up by duplicate files in a serverless distributed file system. In ICDCS, pages 617–624, 2002.