ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
DIIF 0.876

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 9, SEPTEMBER 2015, PP 580-584

Efficient PDP Scheme for Distributed Cloud Storage Framework.

[1]Mummadi Sravana Sandhya,[2] N.Parashuram, [3]Dr S.Prem Kumar
[1](M.Tech), CSE,
[2]Assistant Professor, Department of Computer Science and Engineering
[3]Professor & HOD, Department of computer science and engineering,
G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract: In cloud computing systems, data owner more often than not store immense volume information on the cloud servers hence customers may get to the information from Cloud servers without knowing their region in this association outsourcing customer information among untrusted cloud servers, reliable verify, effective information outsourcing and framework execution is a testing issue .keeping in mind the end goal to address the above issues we utilize Centralized Cloud Service Provider to enhance the System Performance by decreasing the time many-sided quality .Therefore, every Client solicitation is overseen by incorporated Cloud Service Provider. In order to provide the reliable verification during uploading and downloading User has to answer the Security Question. Security Questions and Answers are provided by user during the registration phase. So during Uploading/Downloading operation If user is normal then he can answer that security questions if he/she is intruder then he/she cannot answer that questions. Thus, utilizing this we can give more Security. Additionally, we can give the Security to transferred information and the summary by utilizing the encryption algorithm in this manner we can accomplish proficient information out sourcing with information respectability. Moreover, the respectability test convention must be proficient keeping in mind the end goal to spare the verifier's expense.

Keywords: Provable data possession, MultiCloud, Centralized distribution.

– – – – – – – – – – ◆ – – – – – – – – – –

1 INTRODUCTION

Information storage on cloud is one of the surely understood administrations offered by cloud computing. On account of this administration endorsers don't need to store their own information on neighborhood servers, where rather their information will be put away on the cloud administration supplier's servers. Cloud storage makes it feasible for clients to remotely store their information and appreciate the on interest astounding cloud applications without the any weight of neighborhood equipment and programming administration, while making customers free from information storage weights, cloud brings new and extreme security dangers in client's outsourced information. The discriminating issue of information trustworthiness comes at whatever point customer transfers information on un-dependable servers. In such situations, customers need to actualize techniques to demonstrate inventiveness of information. The customer may need to get to entire document to guarantee information trustworthiness, which is time and space devouring [4]. Considering the gigantic size of the outsourced information and the clients compelled asset it is not generally conceivable to get to finish information. Which brag a variety of points of interest like boundless storage capacity, anyplace openness and so forth. Since Cloud computing environment is developed on open architectures and interfaces; it can possibly fuse numerous interior and/or outer cloud benefits together to give high interoperability. This sort of circulated cloud environment is called as a multi-Cloud. The saying of not putting all your investments tied up on one place applies in Multi-cloud as well. A multi-cloud approach is one where an enterprise uses two or more cloud services, therefore reducing the risk of widespread data loss or outage due to a component failure in a single cloud computing environment. Frequently, by using virtual infrastructure management (VIM) [1], a multi-cloud allows clients to easily access his/her resources remotely through interfaces such as Web services provided by Amazon EC2. There exist various tools and technologies for multi-cloud, such as VMware

vSphere, Platform VM Orchestrator and Ovirt. These tools help cloud providers to create a distributed cloud storage platform (DCSP) for managing clients' data. But, if such an important platform is vulnerable to security attacks, it would bring irrevocable losses to the clients. For example, the secret data in an enterprise may be illegally accessed by using remote interfaces, or organization relevant data and archives are lost or tampered with when they are stored into an uncertain storage pool outside the enterprise.

One of the biggest issues with cloud data storage is that of data integrity verification at untrusted servers. Also, there exist various motivations like maintaining reputation for cloud service providers (CSP) to behave unfaithfully towards the cloud users. For example, the cloud service provider(CSP), which experiences Byzantine failures infrequently, may decide to hide the data errors from the clients for the benefit of their own like for maintaining their reputation or for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client Therefore, it is crucial for cloud service providers (CSPs) to provide security techniques for managing their storage services. Provable data possession (PDP) [2] (or proofs of retrievability (POR) [3]) is such a probabilistic proof technique for a storage provider to prove the integrity and ownership of clients' data without downloading data. Checking proof without downloading makes it especially important for large-size files and folders (typically including many clients' files) to check whether these data have been tampered with or deleted without downloading the latest version of data. Consequently, it is able to replace traditional hash and signature functions in storage outsourcing. Different PDP schemes have been recently proposed, such as Scalable PDP [4] and Dynamic PDP [5]. However, these schemes mainly focus on PDP issues at untrusted servers in a single cloud storage provider and are not suitable for a multi-cloud environment.

II. LEVELS OF SECURITY RISK IN MULTICLOUD

From different cloud service models, the security responsibility between cloud users and cloud service providers is different. In different cloud environment addresses security control in relation to physical, environmental, and virtualization security, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data According to Tabakiet al. [9], the way the responsibility for privacy and security in a cloud computing environment is shared between cloud users and cloud service providers differs between delivery models. In SaaS, cloud service providers are more responsible for the security and privacy of application services than the cloud users. This responsibility is more relevant to the public than the private cloud environment because the clients need stricter security requirements in the public cloud. With PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud service providers are responsible for protecting one user's applications from others.

In IaaS, users are responsible for protecting operating systems and applications, whereas cloud service providers must provide protection for the users' data [9]. Ristenpartet al. [10] claims that the levels of security issues in IaaS are different. The impact of security issues in the public cloud is greater than the impact of the private cloud. For instance, any damage which occurs to the security of the physical infrastructure or any failure in relation to the management of the security of the infrastructure will cause many problems. In the cloud environment, the physical infrastructure that is responsible for data processing and data storage can be affected by a security risk. Confidentiality: confidential is term in which cloud service provider also unknown to cloud users data which is uploaded on his own cloud, the cloud storage provider does not learn any information about customer data. Integrity: any unauthorized or illegal modification and updating the contents of client data from the cloud storage provider can be detected by the customer while retaining the main benefits of a public storage service: Availability: data of cloud user are available to the user at anytime, anywhere, anyplace from the cloud server. Customer data is accessible from any machine and at all-time reliability: customer data is reliably backed up Efficient retrieval: data retrieval times are comparable to a public cloud storage service data sharing: customers can share their data with trusted parties. Data sharing: cloud users can share data securely with trusted parties.

III.ID-DPDP SYSTEM MODEL AND SECURITY DEFINITION PRESENTED SYSTEM:

COOPERTIVE PROVABLE DATA POSSESSION SHCEME

This work addresses the construction of an efficient PDP scheme for distributed cloud storage to support data migration and scalability of service, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. It presents a cooperative PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy. Multi-prover zeroknowledge proof system is used to prove the security of this scheme, which can satisfy knowledge soundness, completeness and zero-knowledge properties.

A. Hash Index Hierarchy: To support distributed cloud storage, architecture used in cooperative PDP scheme as shown in fig. 2. Our structure has a hierarchy structure which resembles a natural representation of file storage. This structure consists of three layers to represent relationships among all blocks for stored resources. This hierarchy structure and layers are described as follows: 1) Express Layer: This layer offers an abstract representation of the stored resources; 2) Service Layer: This layer offers and manages cloud storage services; and 3) Storage Layer: This layer represents data storage on many physical devices.

This hierarchy used to organize data blocks from multiple CSP services into a large size file by shading their differences among these cloud storage systems. In Figure the resource in Express Layer are split and stored into three CSPs that are indicated by different colors are shown in Service Layer. After that each CSP fragments and stores the assigned data into the storage servers in Storage Layer. It also makes use of colors to distinguish different CSPs. Moreover, it follows the logical order of the data blocks to organize the Storage Layer.

B. Homomorphic Verifiable Response: Homomorphic Verifiable Responses (HVR), which is used to integrate multiple responses from the different CSPs in CPDP scheme. If given two responses φi and φj for two challenges Qi and Qj from two CSPs, there exist an efficient algorithm to combine them into a response corresponding to the sum of the challenges Qi ∪Qj then a response is called homomorphic verifiable response in a PDP protocol. Homomorphic verifiable response is the key technique of CPDP because it not only reduces the communication bandwidth, but also hides the location of outsourced data in the distributed cloud storage environment.

C. Security Analysis:

Multi-prover zero-knowledge proof system is directly used for security, which satisfies following properties:

1) Collision resistant for index-hash hierarchy: The indexhash hierarchy in CPDP scheme is collision resistant, even if the client generates files with the same file name and cloud name collision doesn't occur there.

2) Completeness property of verification: In this scheme, the completeness property implies public verifiability property. Due to this property allows client as well as anyone other than client (data owner) can challenge the cloud server for data integrity and data ownership without the need for any secret information.

3) Zero-knowledge property of verification: This paper makes use of the zero-knowledge property to preserve the privacy of data blocks and signature tags. Initially, randomness is adopted into the CSPs' responses in order to resist the data leakage attacks.

4) Knowledge soundness of verification: The soundness means that it is infeasible to fool the verifier to accept false statements. Often, the soundness can also be considered as a stricter notion of unforge ability for file tags to avoid cheating the ownership. This denotes that the CSPs, even if collusion is tried, cannot be tampered with the data or forge the data tags if the soundness property holds. Thus CPDP scheme can resist the tag forgery attacks to avoid cheating the CSPs' ownership.

3.1 Presented System

The ID-DPDP system model and security definition are presented in this section. An IDDPDP protocol comprises four different entities which are illustrated in Figure 1. We describe them below:

1) Client: an entity, which has massive data to be stored on the multi-cloud for maintenance and computation, can be either individual consumer or corporation.

2) CS (Cloud Server): an entity, which is managed by cloud service provider, has significant storage space and computation resource to maintain the clients' data.

3) Combiner: an entity, which receives the storage request and distributes the block-tag pairs to the corres-

ISSN (Online): 2349-7084

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 9, SEPTEMBER 2015, PP 580-584

ponding cloud servers. When receiving the challenge, it splits the challenge and distributes them to the different cloud servers. When receiving the responses from the cloud servers, it combines them and sends the combined response to the verifier.

4) PKG (Private Key Generator): an entity, when receiving the identity, it outputs the corresponding private key

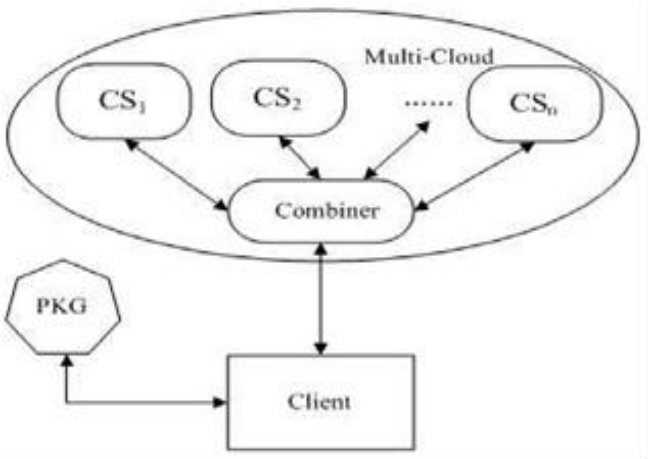

Fig 1. Presented ID-DPDP system model

3.2. Proposed System:

System Functions:

1) PKG (Private Key Generator). Entity, trusted by the clients and the PCSs, that generates the public parameters Params, the master public key mpk, the master secret key msk and the private key of the Client which helps to protect user privacy as well provide data integrity .

2) Client. Entity which has massive data to be stored on the public cloud for maintenance and computation. Clients can be either individual consumers or group consumers, e.g., the departments of the company in the motivated scenario.

3) Cloud Server. Entity, managed by the cloud service provider that has significant storage space and computational resources to maintain the clients' data. In the cloud paradigm, by putting the large data files on the remote cloud servers, the clients can be relieved of the burden of storage and computation. As the clients no longer possess their data locally, it is of critical importance for them to ensure that their data are being correctly stored and maintained. That is, clients should be equipped with certain security means so that they can periodically verify the correctness of the remote data even without the existence of local copies.

4. Centralized CSP: to reduce the complexity we can use the Centralized Cloud Service Provider. Therefore, every request is managed by centralized Cloud Service Provider in order to reduce the time complexity thus to improve the system performance. Here every client outsource data will managed by Centralized CSP in secured manner data will not reviled at Centralized CSP Level. It will distribute Encrypted data over Multiple Cloud severs as Network code based (spitted data among servers) manner. Hence it helps data availability and security.

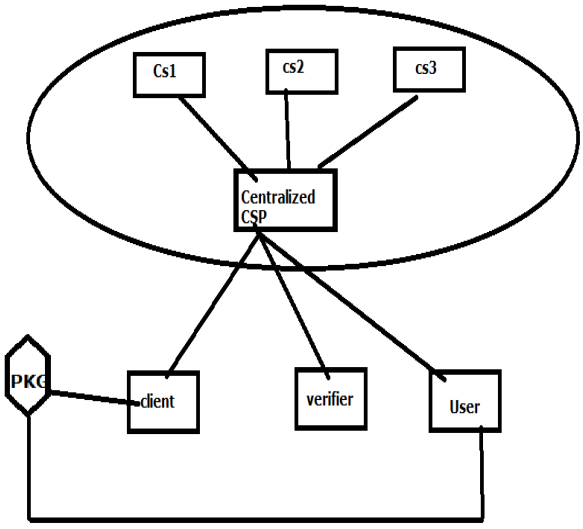

Fig 2. Proposed System

IV. CONCLUSION AND FUTURE WORK

This paper address different difficult issues which are identified with access controlling, information honesty, information accessibility, security of information and framework execution regarding multicloud information storage and sharing by the customers .These are the significant worries in a disseminated domain. As we are utilizing multi cloud so there are different cloud administration suppliers for various clouds. As we need to store hinder in every cloud so the solicitation needs to go from every Cloud Administration Supplier so to decrease the multifaceted nature we can utilize the

Brought together Cloud Administration Supplier. Subsequently, every solicitation is overseen by concentrated Cloud Administration Supplier. This exploration can be dealt with as another strategy for information trustworthiness check in information ownership. As a component of future improvement, I would like extend my work for better security data need to encrypt before to upload into cloud as ASCII code and convert into binary formatted as double layser encryption on multicloud.

REFERENCES

[1] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster, Virtual infrastructure management in private and hybrid clouds," IEEE Internet Computing, vol. 13, no. 5, pp. 14–22,2009.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609.

[3] A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, SecureComm, 2008, pp. 1–10.

[5] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213–222.

[6] H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90–107.

[7] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in ESORICS, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355–370.

[8] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, "Enabling public Verifiability and data dynamics for storage security in cloud Computing," in ESORICS, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355–370.

[9] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced Storages in clouds," in SAC, W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550–1557.

[10] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D.Keromytis, Eds. ACM, 2009, pp. 187–198.

[11] Y. Dodis, S. P. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109–127.

[12]L. Fortnow, J. Rompel, and M. Sipser, "On the power of multiprover Interactive protocols," in Theoretical Computer Science, 1988, pp.156–161.