IJSEAT International Journal of Science Engineering and Advance Technology

An Efficient Pdp Scheme For Distributed Cloud Storage To Support Dynamic Scalability On Multiple Storage Servers

[1]Ch.Rajeshwari,[2] S.Suresh
[1]choppararaji@gmail.com,
Balaji Institute of Technology & Science Narsampet warangal

Abstract:

The confirmation examination without downloading makes it particularly important for large-size files and folders typically including many clients' files to make sure whether these data have been tampered with or deleted without downloading the latest version of data. Provable data possession is such a probabilistic proof technique for a storage provider to establish the integrity and ownership of clients' data without downloading data. Consequently it is able to put back traditional hash and signature functions in storage outsourcing. Various PDP schemes have been recently proposed such as Scalable PDP and Dynamic PDP. Though these schemes mainly focus on PDP issues at untrusted servers in a single cloud storage provider and are not appropriate for a multi-cloud environment. Furthermore clients need to know the exact position of each file block in a multi-cloud environment. The confirmation process in such a case will lead to high communication overheads and calculation costs at client sides as well. Consequently it is of utmost necessary to design a cooperative PDP model to decrease the storage and network overheads and improve the transparency of verification activities in cluster-based cloud storage systems. A cooperative PDP scheme should give features for timely detecting abnormality and renewing multiple copies of data.

Keywords: Storage Security, Provable Data Possession, Interactive Protocol, Zero-knowledge, Multiple Cloud, Cooperative.

Introduction:

To perk up the system performance with respect to the method we analyze the performance of probabilistic queries for detecting abnormal situations. This probabilistic method also has an intrinsic benefit in reducing computation and communication overheads. Then we present a competent method for the selection of optimal parameter values to minimize the computation overheads of CSPs and the clients' operations. In addition we analyze that our scheme is appropriate for existing distributed cloud storage systems. Finally the experiments show that our solution brings in very limited computation and communication overheads. Cloud storage service has become a faster income growth point by providing a comparably low-cost, scalable, position-independent platform for clients' data. As cloud computing environment is constructed based on open architectures and interfaces it has the ability to slot in multiple internal and/or external cloud services jointly to provide high interoperability. This property greatly extended application areas of PDP protocol due to the separation of data owners and the users. However these schemes are insecure against replay attacks in dynamic situations because of the dependence on the index of blocks. Moreover they do not fit for multi-cloud storage due to the loss of homomorphism property in the confirmation process.

Related Work:

In order to support dynamic data operations Ateniese et al. developed a dynamic PDP solution called Scalable PDP. They proposed a frivolous PDP scheme based on cryptographic hash function and symmetric key encryption other than the servers can mislead the owners by using previous metadata or replies due to the lack of chance in the challenges. The numbers of updates and challenges are limited and fixed in advance and users cannot perform block insertions anywhere. Erway et al. introduced two Dynamic PDP schemes with a hash function tree to understand (log n) communication and computational costs for a n-block file. The basic scheme called DPDP-I keep hold of the drawback of Scalable PDP and in the block less scheme called DPDPII, Juels and Kaliski presented a POR scheme which relies mainly on pre-processing steps that the client conducts before sending a file to a CSP. Regrettably these operations stop any efficient extension for updating data. Shacham and Waters proposed an enhanced version of this protocol called Compact POR which uses homomorphic property to aggregate a proof into (1) authenticator value and $O(t)$ computation cost for t challenge blocks but their answer is also still and could not avoid the leakage of data blocks in the verification process.

Existing System:

There exist various tools and technologies for multicoloud such as Platform VM Orchestrator, VMwarev Sphere and Ovirt. These tools assist cloud providers build a distributed cloud storage platform for managing clients' data. On the other hand if such an important platform is susceptible to security attacks it would bring irreparable losses to the clients. For illustration the confidential data in an enterprise may be unlawfully accessed through a remote interface provided by a multi-cloud or pertinent data and archives may be lost or tampered with when they are stored into an unsure storage pool outside the enterprise. Therefore it is crucial for cloud service providers to provide security methods for managing their storage services.

Disadvantages:

Even though various security models have been proposed for existing PDP schemes these models still cannot cover all security requirements particularly for provable secure privacy preservation and ownership verification. To found a highly effective security model it is compulsory to analyze the PDP scheme within the framework of zero-knowledge proof system (ZKPS) due to the cause that PDP system is essentially an interactive proof system.

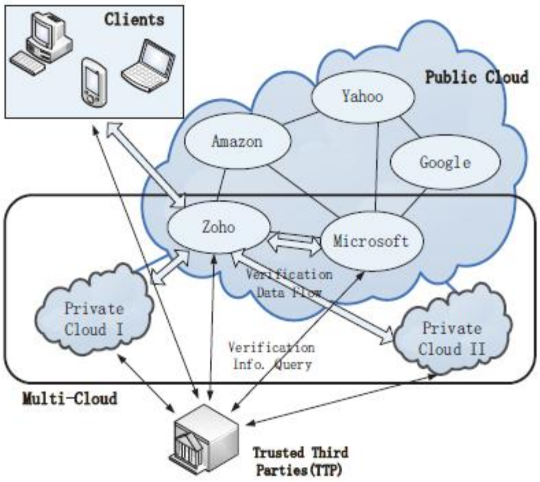
Proposed System:

To make sure the accessibility and reliability of outsourced data in cloud storages researchers have proposed two basic approaches called Provable Data Possession and Proofs of Retrievability .Ateniese et al. first proposed the PDP model for make sure control of files on untrusted storages and provided an RSA-based scheme for a static case that attains the communication cost. They also proposed a publicly verifiable version which allows anyone not just the owner to confront the server for data possession..They proposed a lightweight PDP scheme based on cryptographic hash function and symmetric key encryption but the servers can take in the owners by using previous metadata or responses due to the lack of randomness in the challenges. The numbers of updates and challenges are limited and fixed in advance and users cannot perform block insertions anywhere.

Advantages:

To provide a low-cost, scalable, location independent platform for managing clients' data current cloud storage systems take on several new distributed file systems it is vital to propose an efficient verification on the integrity and ease of use of stored data for detecting faults and automatic recovery. Moreover this verification is essential to provide dependability by automatically maintaining multiple copies of data and automatically redeploying processing logic in the event of failures.

System Architecture:



We believe the survival of multiple CSPs to together store and maintain the clients' data. Moreover a cooperative PDP is used to confirm the integrity and availability of their stored data in all CSPs. The confirmation process is described as firstly a client data owner uses the secret key to pre-process a file which consists of a collection of n blocks produces a set of public verification information that is stored in TTP transmits the file and some verification tags to CSPs and may remove its local copy. Then by using a authentication protocol the clients can issue a challenge for one CSP to check the integrity and availability of outsourced data with respect to public information stored in TTP. A TTP server is built as a core trust base on the cloud for the sake of security. We suppose the TTP is dependable and independent to setup and uphold the CPDP cryptosystem and to produce, store data owner's public key and to store the public parameters used to carry out the verification protocol in the CPDP scheme.

Multi Cloud Storage:

Distributed computing is used to refer to any large association in which many individual personal computer owners permit some of their computer's processing time to be put at the service of a large problem. In our system the each cloud admin consist of data blocks. The cloud user uploads the data into multi cloud. Cloud computing environment is built based on open architectures and interfaces. It has the ability to slot in multiple internal and/or external cloud services jointly to provide high interoperability. We call such a distributed cloud environment as a multi-cloud .A multi-cloud allows clients to simply access his/her resources distantly through interfaces.

Cooperative Pdp:

Cooperative PDP (CPDP) plans assume zero-knowledge property and three-layered index hierarchy respectively. In particular competent method for selecting the most favourable number of sectors in each block to reduce the computation costs of clients and storage service providers. Cooperative PDP (CPDP) scheme without compromising data privacy based on modern cryptographic techniques**.**

Data Integrity:

Data Integrity is extremely significant in database process in particular and Data warehousing and Business intelligence in general. Because Data Integrity make sure that data is of high quality, correct, consistent and accessible.

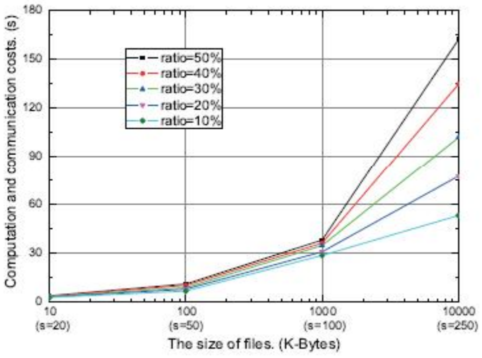
THIRD PARTY AUDITOR:

Trusted Third Party (TTP) who is confidential to store confirmation parameters and offer public query services for these parameters. Trusted Third Party outlook the user data blocks and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data blocks. If any alteration tried by cloud owner an alert is send to the Trusted Third Party.

Cloud User:

The Cloud User who has a large amount of data to be stored in manifold clouds and have the permissions to access and influence stored data. The User's Data is rehabilitated into data blocks. The data blocks are uploaded to the cloud. The TPA views the data blocks and Uploaded in multi cloud. The user can update the uploaded data. If the user wants to download their files the data's in multi cloud is integrated and downloaded.

Experimental Results:



The experimental results demonstrate that the computation and communication costs of commitment and challenge are somewhat changed along with the sampling ratio but those for response and verification produce with the increase of the sampling ratio. Here challenge and response can be divided into two sub-processes as challenge1 and challenge2 as well as response1 and response2 respectively. Also the proportions of data blocks in each CSP have better influence on the computation costs of challenge and response processes. The scheme has better performance than non-cooperative approach.

Conclusion:

We have projected a cooperative PDP scheme to support dynamic scalability on multiple storage servers. We also showed that our scheme provided all security properties required by zero knowledge interactive proof system so that it can oppose various attacks even if it is deployed as a public audit service in clouds. Also we optimized the probabilistic query and periodic verification to perk up the audit performance. Our experiments clearly established that our approaches only introduce a small amount of computation and communication overheads. Therefore the solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems. As part of future work we would make bigger our work to explore more effective CPDP constructions. First from our experiments we found that the performance of CPDP scheme especially for large files is affected by the bilinear mapping operations due to its high complexity.

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, andP. 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] 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.

[9] 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.

[10] 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.

[11] L. Fortnow, J. Rompel, and M. Sipser, “On the power of multiprover interactive protocols,” in *Theoretical Computer Science*, 1988, pp. 156–161.

[12] Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, “Collaborative integrity verification in hybrid clouds,” in *IEEE Conference on the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom, Orlando, Florida, USA, October 15-18*, 2011, pp. 197–206.

[13] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” EECS Department, University of California, Berkeley, Tech. Rep., Feb 2009.

[14] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in *Advances in Cryptology (CRYPTO’2001)*, vol. 2139 of LNCS, 2001, pp. 213–229.

[15] O. Goldreich, *Foundations of Cryptography: Basic Tools*. Cambridge University Press, 2001.