ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Distributed Provable Data Possession in Multi-Cloud Storage through Client Authentication

N.A Gayatri
M.Tech(CSE)
Sankethika Vidya Parishad Engineering College

G.Kalyan Chakravarthi, M.Tech
Assistant Professor
Sankethika Vidya Parishad Engineering College

Reshma Sultana
Assistant Professor
Sankethika Vidya Parishad Engineering College

Abstract:
Identity-Based Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing construction of an efficient scheme for distributed cloud storage to support the scalability of service and data migration, in which of multiple cloud service providers to cooperatively store and maintain the clients' data. Cloud computing has become an important thing in computer field. Cloud computing takes information processing as a service, such as storage and computing. Data integrity is important thing in cloud storage. In certain situations, clients should store their data such as image or text in multi cloud. When the client stores his/her data on multicloud servers, the distributed storage and integrity checking is very important. Here we propose an Identity Based Distributed Provable Data Possession (ID-DPDP) protocol for multi-cloud storage. Remote data integrity checking is important in cloud storage. It can make the clients verify whether their data is kept as it is without downloading the entire data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost.

Keywords: ***Cloud computing, integrity, multicloud, data possession, IDPDP.***

Introduction:

Provable Data Possession (PDP) is one such scheme proposed in this scheme ensures that the data integrity is not lost. However, this scheme needs the users to download data for verification which causes security problem again. Therefore it is essential to have a scheme where data downloading is not required for verification. Towards this end PDP scheme such as Scalable PDP and Dynamic PDP came into existence. These schemes focused on single cloud storage providers. There are schemes like SPDP, DPDP and Merkle Hash Tree (MHT) make use of authenticated skip list in order to verify the adjacent blocks for integrity. These schemes do not work in multi-cloud environments as they can't construct MHT for such environment. The other schemes such as CPOR and PDP make use of homomorphic verification tags where downloading data for verification is not required.

Multi cloud storage :

Distributed computing is used to refer to any large collaboration in which many individual personal computer owners allow 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 constructed based on open architectures and interfaces; it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud .A multi-cloud allows clients to easily access his/her resources remotely through interfaces.

Data Integrity :

Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Related Work

RDP permits a customer that has put away information at a Public cloud server (PCS) to check that the server has the first information without recovering it. The model produces probabilistic confirmations of ownership by examining irregular sets of pieces from the server, which definitely lessens I/O costs. The customer keeps up a steady measure of metadata to check the verification.

The test/reaction convention transmits a little, steady measure of information, which minimizes system correspondence. Keeping in mind the end goal to accomplish secure RDPC usage, Ateniese et al. proposed a provable information ownership (PDP) standard [1] and planned two provably-secure PDP. Plans focused around the trouble of extensive whole number considering. They refined the first standard also proposed an element PDP plot in [2] yet their proposal does not help the supplement operation.

So as to tackle this issue, Erway et al. proposed a full-dynamic PDP conspire by utilizing a confirmed flip table [3]. Taking after Ateniese et al's. Spearheading work, analysts gave incredible exertions to RDPC with augmented models and new conventions [4], [5], [6], [7], [8], [9], [10]. One of the varieties is the verification of retrievability (POR), in which an information stockpiling server can't just demonstrate to a verifier that he is really putting away the greater part of a customer's information, additionally it can demonstrate that the clients can recover them whenever. This is stronger than the consistent PDP thought.

Sachem exhibited the first POR plans [15] with provable security. The condition of the craftsmanship can be found in [16], [17], [18], [19] in any case few POR conventions are more productive than their PDP partners. The test is to assemble POR frameworks that are both productive and provably secure [14]. Note that one of profits of cloud capacity is to empower general information access with autonomous topographical areas. This suggests that the end gadgets may be versatile and restricted in processing and stockpiling. General RDP conventions are more suitable for cloud clients outfitted with portable end gadgets. Our ID-RDP structural planning and convention are focused around the PDP model.

Existing System:

In cloud computing, remote data integrity checking is an important security problem. The clients' massive data is outside his control. The malicious cloud server may corrupt the clients' data in order to gain more benefits. The formal system model and security model are existing models.

In the PDP model, the verifier can check remote data integrity with a high probability. Based on the RSA, they designed two provably secure PDP schemes. PDP allows a verifier to verify the remote data integrity without retrieving or downloading the whole data. It is a probabilistic proof of possession by sampling random set of blocks from the server, which drastically reduces I/O costs. The verifier only maintains small metadata to perform the integrity checking. PDP is an interesting remote data integrity checking model.

In POR, the verifier can check the remote data integrity and retrieve the remote data at any time. On some cases, the client may delegate the remote data integrity checking task to the third party. It results in the third party auditing in cloud computing

Disadvantages of Existing System:

- Does not provide efficiency in remote data integrity checking.
- More expensive.
- The existing system provides less flexibility.
- Less efficient.

Proposed System:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Remote data integrity checking is of crucial importance in cloud storage. In multi-cloud environment, distributed provable data possession is an important element to secure the remote data. we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffi Hellman) problem. The proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

Advantages of Proposed System:

- The distributed cloud storage is indispensable.
- Efficient and Flexible.
- Elimination of the certificate management.

System Architecture:

The ID-PDP framework model and security definition are given in this area. AN ID-PDP convention contains four very surprising substances. We have a tendency to depict them beneath:

Client: AN element, that has expansive information to be put away on the multi-cloud for upkeep and processing, may be either singular customer or partnership.

CS (Cloud Server): AN element that is overseen by cloud administration supplier has imperative space for putting away and processing asset to deal with the customers' data.

Combiner: AN element, that gets the capacity ask for and disseminates the piece label sets to the comparing cloud servers. When getting the test, it parts the test and disseminates them to the different cloud servers. When accepting the reactions from the cloud servers, it joins them and sends the joined reaction to the hero.

PKG (Private Key Generator): A substance, once getting the character, it yields the relating non-open key.

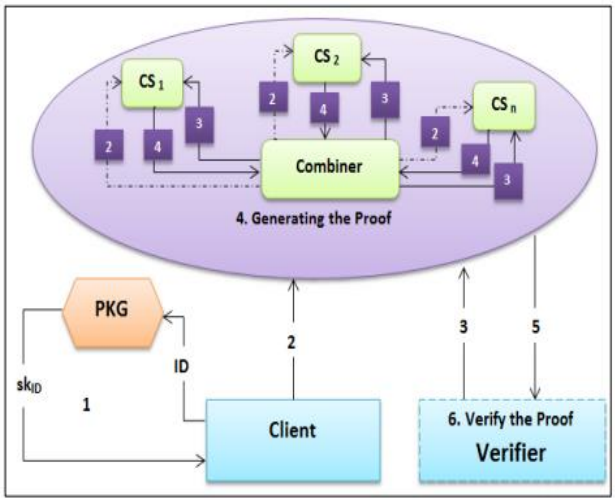

Fig: IDPDP protocol

In identity-based public key cryptography, this paper focuses on distributed provable data possession in multi-cloud storage. The protocol can be made efficient by eliminating the certificate management. We propose the new remote data integrity checking model: IDDPDP. The system model and security model are formally proposed. Then, based on the bilinear pairings, the concrete ID-DPDP protocol is designed. In the random oracle model, our ID-DPDP protocol is provably secure. On the other hand, our protocol is more flexible besides the high efficiency. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

Conclusion:

We presented the construction of an efficient PDP scheme for distributed cloud storage. Based on homomorphic verifiable response and hash Index hierarchy, we have proposed 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 resist various attacks even if it is deployed as a public audit service in clouds. Further more, Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

be treated as a new candidate for data integrity verification in outsourcing data storage systems.

References:

[1] Huaqun Wang, Identity-Based Distributed Provable Data Possession in Multicloud Storage, IEEE Transactions on Services Computing, (Volume:8 , Issue: 2)

[2] G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik. Scalable and Efficient Provable Data Possession.SecureComm 2008, article9, 2008.

[3] C. C. Erway, A. Kupcu, C. Papamanthou, R. Tamassia. Dynamic Provable Data Possession.CCS'09, 213-222, 2009.

[4] F. Seb ´ e, J. Domingo-Ferrer, A. Mart´ ınez-Ballest ´ e, Y. Deswarte, J. Quisquater. Efficient Remote Data Integrity checking inCritical Information Infrastructures. IEEE Transactions on Knowledge and Data Engineering, 20(8):1034-1038, 2008.

[5] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, S. S. Yau. Efficient Provable Data Possession for Hybrid Clouds.CCS'10, 756-758,2010.

[6] Y. Zhu, H. Hu, G.J. Ahn, M. Yu. Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage.IEEE Transactions on Parallel and Distributed Systems, 23(12):2231-224, 2012.

[7] R. Curtmola, O. Khan, R. Burns, G. Ateniese. MR-PDP: Multiple-Replica Provable Data Possession. ICDCS'08, 411-420,2008.

[8] A. F. Barsoum, M. A. Hasan. Provable Possession and Replication of Data over Cloud Servers. CACR, University of Waterloo,Report2010/32,2010.

[9] H. Wang. Proxy Provable Data Possession in Public Clouds.IEEE Transactions on Services Computing. To appear, availableon-line at http://doi.ieeecomputersociety.org/10.1109/TSC.2012.35

[10] Z. Hao, N. Yu. A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability. 2010 SecondInternational Symposium on Data, Privacy, and E-Commerce, 84-89, 2010.

[11] A. F. Barsoum, M. A. Hasan, On Verifying Dynamic Multiple Data Copies over Cloud Servers. IACR eprint report 447, 2011.Available at http://eprint.iacr.org/2011/447.pdf

[12] H. Wang, Y. Zhang. On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage.IEEE Transactions on Parallel and Distributed Systems. To appear, available on-line at http://doi.ieeecomputersociety.org/10.1109/TPDS.2013. 16

[13] Q. Wang, C. Wang, K. Ren, W. Lou, J. Li. Enabling Public Auditability and Data Dynamics for Storage Security in CloudComputing. IEEE Transactions on Parallel And Distributed Systems, 22(5):847-859, 2011.

[14] A. Juels, B. S. Kaliski Jr. PORs: Proofs of Retrievability for Large Files. CCS'07, 584-597, 2007.

[15] H. Shacham, B. Waters. Compact Proofs of Retrievability.ASIACRYPT 2008, LNCS 5350, 90-107, 2008.

[16] K. D. Bowers, A. Juels, A. Oprea. Proofs of Retrievability: Theory and Implementation. CCSW'09, 43-54, 2009.

[17] Q. Zheng, S. Xu. Fair and Dynamic Proofs of Retrievability.CODASPY'11, 237-248, 2011.

[18] Y. Dodis, S. Vadhan, D. Wichs1, Proofs of Retrievability via Hardness Amplification, TCC 2009, LNCS 5444, 109-127, 2009.

[19] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu. ZeroKnowledge Proofs of Retrievability.Sci China InfSci, 54(8):1608-1617, 2011.

[20] D. Boneh, M. Franklin. Identity-based Encryption from the Weil Pairing.CRYPTO 2001, LNCS 2139, 213-229, 2001