International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 02 | Feb -2017 www.irjet.net p-ISSN: 2395-0072

A Survey on Provable Multi-copy Dynamic Data Possession in Cloud Computing Systems

Ms. Supriya Harishchandra Lokhande [1] , Asst.Prof.S.V.Todkari[2]
Department of Computer Engineering ,Jayawantrao Sawant College Of Engineering, Pune Maharashtra,India
Department of Information Technology Jayawantrao Sawant College Of Engineering, Pune Maharashtra,India

---

Abstract -*Progressively more associations are picking outsourcing information to remote cloud service providers (CSPs). Clients can lease the CSPs stockpiling framework to store and recover practically boundless measure of information by paying expenses metered in gigabyte/month. For an expanded level of versatility, accessibility, and solidness, a few clients may need their information to be imitated on different servers over various server farms. The more duplicates the CSP is requested that store, the more expenses the clients are charged. Hence, clients require to have a solid certification that the CSP is putting away all information duplicates that are settled upon in the administration contract, and every one of these duplicates are predictable with the latest changes issued by the clients. In this paper, we propose a map-based provable multi-copy dynamic data possession (MB-PMDDP) conspire that has the accompanying components: 1) it gives a proof to the clients that the CSP is not deceiving by putting away less duplicates; 2) it underpins outsourcing of element information, i.e., it underpins piece level operations, for example, square adjustment, addition, erasure, and affix; what's more, 3) it permits approved clients to consistently get to the record duplicates put away by the CSP. We give a near examination of the proposed MB-PMDDP conspire with a reference show acquired by augmenting existing provable ownership of element single-duplicate plans. The hypothetical investigation is approved through test comes about on a business cloud stage. Furthermore, we appear the security against intriguing servers, and examine how to recognize defiled duplicates by marginally changing the proposed conspire.*

***Key Words*: Cloud Computing, Data Replication, Outsourcing, Data Storage, Dynamic Environment.**

1. INTRODUCTION

OUTSOURCING information to a remote cloud service provider (CSP) permits associations to store more information on the CSP than on private PC frameworks. Such outsourcing of information stockpiling empowers associations to focus on developments and assuages the weight of steady server overhauls what's more, other registering issues. In addition, many approved clients can get to the remotely put away information from various geographic areas making it more helpful for them. Once the information has been outsourced to a remote CSP which may not be dependable, the information proprietors lose the coordinate control over their touchy information. This absence of control raises new imposing and testing errands identified with information classification and honesty security in distributed computing.

The classification issue can be taken care of by scrambling touchy information before outsourcing to remote servers. In that capacity, it is a significant request of clients to have a solid proof that the cloud servers still have their information and it is not being messed with or incompletely erased after some time. Therefore, numerous scientists have concentrated on the issue of provable data possession (PDP) and proposed distinctive plans to review the information put away on remote servers. PDP is a method for approving information honesty over remote servers. In a run of the mill PDP demonstrate, the information proprietor produces some metadata/data for an information record to be utilized later for check purposes through a test reaction convention with the remote/cloud server. The proprietor sends the record to be put away on a remote server which might be un-trusted, what's more, erases the nearby duplicate of the record. As a proof that the server is as yet having the information record in its unique frame, it needs to effectively figure a reaction to a test vector sent from a verifier — who can be the first information proprietor or a trusted substance that shares some data with the proprietor. Specialists have proposed distinctive varieties of PDP conspires under various cryptographic suppositions; for case, see [1]–[9].

One of the center plan standards of outsourcing information is to give dynamic conduct of information to different applications. This implies the remotely put away information can be definitely not just got to by the approved clients, additionally upgraded and scaled (through piece level operations) by the information proprietor. PDP plans exhibited in [1]–[9] concentrate on just static or warehoused information, where the outsourced information is kept unaltered over remote servers. Cases of PDP developments that manage dynamic information are [10]–[14]. The last are in any case for a solitary duplicate of the information record. Despite the fact that PDP plans have been exhibited for different duplicates of static information, see [15]–[17], to the best of our insight, this work is the main PDP conspire

specifically managing different duplicates of element information. In Appendix A, we give an outline of related work. While confirming different information duplicates, the general framework respectability check falls flat if there is at least one tainted duplicates. To address this issue and perceive which duplicates have been ruined.

Proof of retrievability (POR) is a correlative way to deal with PDP, and is more grounded than PDP in the sense that the verifier can remake the whole record from reactions that are dependably transmitted from the server. This is expected to encoding of the information document, for instance utilizing eradication codes, before outsourcing to remote servers. Different POR plans can be found in the writing, for instance [18]–[23], which concentrate on static information.

2. REMOTE INTEGRITY CHECKING

This section dissects the issue of checking the uprightness of records put away on remote servers. Since servers are inclined to fruitful assaults by pernicious programmers, the consequence of straightforward uprightness checks keep running on the servers can't be trusted. On the other hand, downloading the records from the server to the confirming host is unfeasible. Two arrangements are proposed, in view of test reaction conventions.

3. PROOFS OF RETRIEVABILITY FOR LARGE FILES

In this section, we characterize and investigate verifications of retrievability (PORs). A POR plot empowers a chronicle or go down administration (prover) to create a succinct evidence that a client (verifier) can recover an objective document F, that will be, that the file holds and dependably transmits record information adequate for the client to recuperate F completely. A POR might be seen as a sort of cryptographic confirmation of information (POK), however one exceptionally intended to handle a huge document (or bitstring) F. We investigate POR conventions here in which the correspondence costs, number of memory gets to for the prover, and capacity necessities of the client (verifier) are little parameters basically autonomous of the length of F. Notwithstanding proposing new, pragmatic POR developments, we investigate usage contemplations and advancements that bear on beforehand investigated, related plans. In a POR, dissimilar to a POK, neither the prover nor the verifier require really know about F. PORs offer ascent to another and uncommon security definition whose plan is another commitment of our work. We see PORs as a critical apparatus for semi-trusted online files. Existing cryptographic methods help clients guarantee the protection and honesty of records they recover. It is likewise normal, in any case, for clients to need to check that documents don't erase or adjust records preceding recovery. The objective of a POR is to finish these checks without clients downloading the documents themselves. A POR can likewise give nature of-administration certifications, i.e., demonstrate that a document is retrievable inside a specific time bound.

4 .PROVABLE DATA POSSESSION

We present a model for provable information ownership (PDP) that permits a customer that has put away information at an un-trusted server to confirm that the server has the first information without recovering it. The model produces probabilistic confirmations of ownership by examining irregular arrangements of squares from the server, which radically lessens I/O costs. The customer keeps up a steady measure of metadata to check the evidence. The test/reaction convention transmits a little, consistent measure of information, which minimizes arrange correspondence. Hence, the PDP display for remote information checking bolsters substantial information sets in generally disseminated capacity framework. We display two provably-secure PDP plans that are more proficient than past arrangements, notwithstanding when contrasted and plots that accomplish weaker certifications. Specifically, the overhead at the server is low (or even steady), rather than straight in the extent of the information. Tests utilizing our usage check the reasonableness of PDP and uncover that the execution of PDP is limited by plate I/O and not by cryptographic calculation.

5 . SMALLER PROOFS OF RETRIEVABILITY

In a proof-of-retrievability framework, an information stockpiling focus persuades a verifier that he is really putting away the greater part of a customer's information. The focal test is to assemble frameworks that are both proficient and provably secure- - that is, it ought to be conceivable to remove the customer's information from any prover that passes a confirmation check. In this paper, we give the main evidence of-retrievability plans with full verifications of security against arbitrary enemies in the most grounded model, that of Juels and Kaliski. Our first plan, worked from BLS marks and secure in the arbitrary prophet demonstrate, has the shortest inquiry and response of any evidence of-retrievability with open unquestionable status. Our second plan, which constructs richly on pseudorandom capacities (PRFs) and is secure in the standard model, has the shortest response of any evidence of-retrievability plan with private undeniable nature (yet a more drawn out_question). Both plans depend on homomorphic properties to total a proof into one little authenticator esteem.

6. MB-PMDDP SCHEME

Creating novel differentiable duplicates of the information record is the center to plan a provable multi-duplicate information ownership conspire. Indistinguishable duplicates empower the CSP to just betray the proprietor by putting away just a single duplicate and imagining that it stores numerous duplicates. Utilizing a straightforward yet effective way, the proposed conspire produces unmistakable duplicates using the dispersion property of any secure encryption conspire. The dissemination property guarantees

that the yield bits of the cipher text rely on upon the info bits of the plaintext in an extremely complex manner, i.e., there will be an erratic finish change in the cipher text, if there is a single piece change in the plaintext [24]. The collaboration between the approved clients and the CSP is considered through this system of creating unmistakable duplicates, where the previous can unscramble/get to a document duplicate got from the CSP. In the proposed plot, the approved clients require just to keep a single mystery key (imparted to the information proprietor) to decode the record duplicate, and it is not really to perceive the list of the got duplicate. In this work, we propose a MB-PMDDP conspire permitting the information proprietor to upgrade and scale the pieces of document duplicates outsourced to cloud servers which might be un-trusted. Approving such duplicates of element information requires the learning of the square forms to guarantee that the information hinders in all duplicates are predictable with the latest adjustments issued by the proprietor. Also, the verifier ought to know about the square files to ensure that the CSP has embedded or included the new squares at the asked for positions in all duplicates. To this end, the proposed plan depends on utilizing a little information structure (metadata), which we call a MAP Version table.

The map-version table (MVT) is a little element information structure put away on the verifier side to approve the uprightness also, consistency of all document duplicates outsourced to the CSP. The MVT comprises of three sections: serial number (SN), block number (BN), and block version (BV). The SN is an ordering to the document pieces. It demonstrates the physical position of a piece in an information document. The BN is a counter used to make a consistent numbering/ordering to the document squares. Along these lines, the connection amongst BN and SN can be seen as a mapping between the consistent number BN and the physical position SN. The BV demonstrates the present adaptation of record squares. Whenever a information record is at first made the BV of every piece is 1. On the off chance that a particular square is being redesigned, its BV is augmented by 1.

Comment 1: It is vital to note that the verifier keeps just a single table for boundless number of document duplicates, i.e., the capacity prerequisite on the verifier side does not rely on upon the quantity of record duplicates on cloud servers. For n duplicates of a information record of size |F|, the capacity prerequisite on the CSP side is O(n|F|), while the verifier's overhead is O(m) for all document duplicates (m is the quantity of document squares).

Comment 2: The MVT is actualized as a connected rundown to disentangle the inclusion cancellation of table passages. For real execution, the SN is not should have been put away in the table; SN is thought to be the section/table record, i.e., every table section contains only two whole numbers BN and BV (8 bytes). In this way, the aggregate table size is 8m bytes for all document duplicates. We facilitate take note of that despite the fact that the table size is straight to the document estimate, in rehearse the previous would be littler by a few requests of greatness.

7. CONCLUSIONS

Outsourcing data to remote servers has become a growing drift for some associations to ease the weight of nearby information stockpiling and support. In this work we have considered the issue of making different duplicates of element information document and confirming those duplicates put away on untrusted cloud servers. We have proposed another PDP plot (alluded to as MB-PMDDP), which underpins outsourcing of multi-duplicate dynamic information, where the information proprietor is equipped for not just documenting and getting to the information duplicates put away by the CSP, however likewise upgrading and scaling these duplicates on the remote servers. To the best of our insight, the proposed plan is the first to address numerous duplicates of element information. The communication between the approved clients and the CSP is considered in our plan, where the approved clients can flawlessly get to an information duplicate got from the CSP utilizing a solitary mystery key imparted to the information proprietor. Also, the proposed conspire underpins open undeniable nature, empowers discretionary number of evaluating, and permits ownership free check where the verifier can confirm the information respectability despite the fact that he neither has nor recovers the document hinders from the server. Through execution examination and test comes about, we have shown that the proposed MB-PMDDP plot beats the TB-PMDDP approach got from a class of element single-duplicate PDP models. The TB-PMDDP leads to high stockpiling overhead on the remote servers and high calculations on both the CSP and the verifier sides. The MB-PMDDP conspire altogether diminishes the calculation time amid the test reaction stage which makes it more pragmatic for applications where a substantial number of verifiers are associated with the CSP creating a colossal calculation overhead on the servers. Plus, it has bring down capacity overhead on the CSP, and in this way diminishes the charges paid by the cloud clients. The dynamic piece operations of the guide based approach are finished with less correspondence cost than that of the tree-based approach. A slight adjustment should be possible on the proposed conspire to bolster the component of distinguishing the files of ruined duplicates. The ruined information duplicate can be reproduced even from a total harm utilizing copied duplicates on other servers. Through security examination, we have demonstrated that the proposed plan is provably secure.

ACKNOWLEDGEMENT

The authors can acknowledge any person/authorities in this section. This is not mandatory.

REFRENCES:

[1] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 598–609.

[2] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[3] Y. Deswarte, J.-J. Quisquater, and A. Saïdane, "Remote integrity checking," in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst. (IICIS), 2003, pp. 1–11.

[4] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer," IACR (International Association for Cryptologic Research) ePrint Archive, Tech. Rep. 2006/150, 2006.

[5] F. Sebé, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034–1038, Aug. 2008

[6]] P. Golle, S. Jarecki, and I. Mironov, "Cryptographic primitives enforcing communication and storage complexity," in Proc. 6th Int. Conf. Financial Cryptograph. (FC), Berlin, Germany, 2003, pp. 120–135.

[7] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. 11th USENIX Workshop Hot Topics Oper. Syst. (HOTOS), Berkeley, CA, USA, 2007, pp. 1–6.

[8]] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," IACR Cryptology ePrint Archive, Tech. Rep. 2008/186, 2008.

[9] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," ACM Trans. Storage, vol. 2, no. 2, pp. 107–138, 2006.

[10] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw. (SecureComm), New York, NY, USA, 2008, Art. ID 9.

[11] C. Wang, Q. Wang, K. Ren, and W. Lou. (2009). "Ensuring data storage security in cloud computing," IACR Cryptology ePrint Archive, Tech. Rep. 2009/081. [Online]. Available: http://eprint.iacr.org/.

[12] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2009, pp. 213–222.

[13] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. 14th Eur. Symp. Res. Comput. Secur. (ESORICS), Berlin, Germany, 2009, pp. 355–370.

[14] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Trans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432–1437, Sep. 2011.

[15] A. F. Barsoum and M. A. Hasan. (2010). "Provable possession and replication of data over cloud servers," Centre Appl. Cryptograph. Res., Univ. Waterloo, Waterloo, ON, USA, Tech. Rep. 2010/32. [Online]. Available: http://www.cacr.math.uwaterloo.ca/techreports/2010/cacr2010-32.pdf.

[16] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiplereplica provable data possession," in Proc. 28th IEEE ICDCS, Jun. 2008 ,pp. 411–420.

[17] Z. Hao and N. Yu, "A multiple-replica remote data possession checking protocol with public verifiability," in Proc. 2nd Int. Symp. Data, Privacy, E-Commerce, Sep. 2010, pp. 84–89.

[18] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. 14th Int. Conf. Theory Appl. Cryptol. Inf. Secur., 2008, pp. 90–107.

[19] A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 584–597.

[20] R. Curtmola, O. Khan, and R. Burns, "Robust remote data checking," in Proc. 4th ACM Int. Workshop Storage Secur. Survivability, 2008, pp. 63–68.

[21] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in Proc. ACM Workshop Cloud Comput. Secur. (CCSW), 2009, pp. 43–54.

[22] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in Proc. 6th Theory Cryptograph. Conf. (TCC), 2009, pp. 109–127.

[23] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2009, pp. 187–198.

[24] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

[25] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT), London, U.K., 2001, pp. 514–532.

[26] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. 15th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT), Berlin, Germany, 2009, pp. 319–333.

[27] R. C. Merkle, "Protocols for public key cryptosystems," in Proc. IEEE Symp. Secur. Privacy, Apr. 1980, p. 122.

[28] C. Martel, G. Nuckolls, P. Devanbu, M. Gertz, A. Kwong, and S. G. Stubblebine, "A general model for authenticated data structures," Algorithmica, vol. 39, no. 1, pp. 21–41, Jan. 2004.

[29] P. S. L. M. Barreto and M. Naehrig, Pairing-Friendly Elliptic Curves of Prime Order With Embedding Degree 12, IEEE Standard P1363.3, 2006.

[30] Amazon Elastic Compute Cloud (Amazon EC2). [Online]. Available: http://aws.amazon.com/ec2/, accessed Aug. 2013.

[31] Amazon Simple Storage Service (Amazon S3). [Online]. Available: http://aws.amazon.com/s3/, accessed Aug. 2013.

[32] Amazon EC2 Instance Types. [Online]. Available: http://aws.amazon.com/ec2/, accessed Aug. 2013.

[33] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in Proc. 12th Int. Workshop SAC, 2005, pp. 319–331.

[34] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, "Practical short signature batch verification," in Proc. Cryptograph. Track RSA Conf., 2009, pp. 309–324.

[35] A. F. Barsoum and M. A. Hasan. (2011). "On verifying dynamic multiple data copies over cloud servers," IACR Cryptology ePrint Archive, Tech. Rep. 2011/447. [Online]. Available: http://eprint.iacr.org/.

[36] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Efficient provable data possession for hybrid clouds," in Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS), 2010, pp. 756–758.

BIOGRAPHIES :

Ms.Lokhande Supriya Harishchandra is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. She received her B.E (Computer) Degree from K.B.P College of Engineering , Satara , Maharashtra, India 411007.

Asst .Prof.S.V.Todkari .He is currently working as H.O.D. and Asst. Prof. at Department of Information technology, Jayawantrao Sawant College of Engineering, Pune, India.