International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

A Study on Provable Multicopy Dynamic Data Possession in Cloud Computing Systems

[1]Sampanna Laxmi, [2]T.Ravindhar Reddy

[1]M.Tech Student, Dept of CSE, Brilliant grammar school educational institutions group of institutions integrated campus, T.S, India

[2]Professor, Dept of CSE, Brilliant grammar school educational institutions group of institutions integrated campus, T.S, India

Abstract: *Gradually more and more organizations are opting for outsourcing data to remote cloud service providers (CSPs). clients can rent the CSPs storage infrastructure to store and get back almost infinite amount of data by paying amount per month. On behalf of an improved level of scalability, availability, and durability, some clients may want their data to be virtual on multiple servers across multiple data centers. The more copies the CSP is asked to store, the more amount the clients are charged. As a result, clients need to have a strong assurance that the CSP is storing all data copies that are decided upon in the service contract, and all these copies are reliable with the most recent modifications issued by the clients. Map-based provable multicopy dynamic data possession (MB-PMDDP) method is being proposed in this paper and consists of the following features: 1) it affords an proof to the clients that the CSP is not corrupt by storing less copies; 2) it supports outsourcing of dynamic data, i.e., it supports block-level functions, such as block alteration, addition, deletion, and append; and 3) it permits official users to effortlessly access the file copies stored by the CSP. In addition, we discuss the security against colluding servers, and discuss how to recognize corrupted copies by a little revising the projected scheme.*

Keywords: Cloud Computing, Data Replications, Outsourcing Data Storages, Dynamic Environments.

I. INTRODUCTION

Now a day's Outsourcing data to a remote cloud service providers allows organization to stores more data on the CSP than on private computer systems. Such outsourcing of data storages enable organizations to concentrates on innovation and relieve the burden of constant server updates and other computing issues. The confidentiality issue can be handled by encrypting sensitive data before outsourcing to remote server. As such, it's crucial demands of customer to have strong evidence that the cloud servers still possess their data & it's being tamp

rated with or partially delete over times. Consequently, many researchers have focused on the problem of *provable data possessions (PDP)* and we propose different methods to audit the data stored on remote servers.

Main Contributions:

Our contributions can be summarized as follows:

It proposes of a map-based provable multicopy dynamics data possessions (MB-PMDDP) schemes, provides an adequate guarantee that the CSP stores all copies that are agreed upon in the service contract and the scheme supports outsourcing of dynamic data. It gives a thorough comparison of MB-PMDDP with a reference scheme, which one can obtain by extending existing PDP models for dynamic singlecopy data. The paper shows the security of scheme against colluding servers, and discusses proposed scheme to identify corrupted copies.

The Threat Model:

The integrity of customers' data in the cloud may be at risks due to the following reasons. 1st The csp whose goals is like to make profit and maintain a reputations has an increasing, and its has an incentives to hides data losses storages by discarding data's that has not been or is rarely accessed. Dishonesties CSP may stores fewer copies

than what has been agrees upon in the services contacts with are correctly stored intact. 3rd to save the computational resource, the CSP may totally ignore the data-update requests issued by the owners, or not executes them on all copies leading to inconsistency between the file copies. The goal of the proposed scheme is to detect the CSP misbehavior by validating the number and integrity of file copies.

PROPOSED MB-PMDDP SCHEME

Generating unique differentiable copies of the data file is the core to design a provable multi copy data possessions schemes. Identically copy enables the CSPs to simply deceive the owners by storing only one copy and pretends that it stores multiples copies. Using a simple yet *efficient* ways, the propose scheme generate distinctness copy utilize the *diffusions* property of any Secures encryptions schemes. The interactions between the authorize user and the CSPs is consider through this methodologies of generate distinct copies, where the formers can decrypts/access a files copies receives from the CSPs. In the propose schemes, the authorized user needs only to keep a singles

secrets key to decrypts the files copies, and it is not necessarily to recognizes the indexes of the receives copies.

Our implementation of the presented schemes consists of three modules: OModule (owner module), CModule (CSP module), and VModule (verifier module). OModule, which runs on the owner side, is a library that includes KeyGen,CopyGen,TagGen,algorithms.

CModule is a library that runs on Amazon EC2

and includes ExecuteUpdate and Prove algorithms. VModule is a library to be run at the verifier side and includes the Verify algorithm.

CONCLUSION:

Outsourcing data to remote servers has turn into a growing trend for many organizations to ease the burden of local data storage and protection. In this work we have considered the difficulty of creating multiple copies of dynamic data file and confirm those copies stored on untrusted cloud servers. We have proposed a new PDP scheme (referred to as MBPMDDP), which supports outsourcing of multi-copy dynamic data, where the data owner is skilled of not only archiving and accessing the data copies stored by the CSP, but also updating and scaling these copies on the remote servers. The proposed scheme is the first to address multiple copies of dynamic data. The communication between the authorized users and the CSP is measured in our system, where the authorized users can effortlessly access a data copy received from the CSP using a single secret key shared with the data owner. Furthermore, the proposed scheme supports public verifiability, allows arbitrary number of auditing, and allows possession-free verification where the verifier has the capability to verify the data integrity even though they neither possesses nor retrieves the file blocks from the server.

REFERENCES :

[1] Ayad F. Barsoum and M. Anwar Hasan, " Provable Multicopy Dynamic Data Possession in Cloud computing systems", in IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015

[2] 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.

[3]K. Zeng, "Publicly verifiable remote data integrity," in Proc. 10th Int. Conf. Inf. Commun. Secur. (ICICS), 2008, pp. 419–434.

[4] 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.

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

[12]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.

[13]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.

[14]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/