A Evidence Multicopy Dynamic Data Possession in Multi Cloud Computing System

G. VENKATA TEJASWI
PG Scholar
Dept of CSE
Krishna Chaitanya Institute of Technology & Sciences
Markapur, Prakasam Dist, AP, India.

B. SUBBA REDDY
Associate Professor
Dept of CSE
Krishna Chaitanya Institute of Technology & Sciences
Markapur, Prakasam Dist, AP, India.

Abstract: **Now a day more and more organizations increasing and are opting for outsource data to remote cloud services provider .the customers can rent the CSPs storage infrastructures to stores and retrieves almost unlimited amount of data by paying fees metered in gigabyte/month. In this paper, proposes a map-based provable multicopy dynamic data possession (MB-PMDDP) scheme that's has to follows features: 1) its provide an evidences to customer that the CSPs is not going to cheat by storing the copy of data; 2) its support outsourcing of dynamic data and its support block levels operation, such as block modifications, insertion, deletion, and append; and 3) it allows authorized users to seamlessly access the file copies stored by the CSP. It gives a comparative analysis of the proposed MB-PMDDP scheme with a reference model obtained by extends existing provable possessions of dynamics single copies scheme.**

Index Terms—**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, its crucial demands of customer to have strong evidence that the cloud servers still possess their data & its 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.

Hypothesis of a Paper:

PDP is a technique for validating data integrity over remote servers. In a typical PDP model, the data owner generates some MD/information's for a data files to be used later for verifications purposes through a *challenges response* protocols with the remotes cloud servers. The owner sends the file to be stored on a remote server which may have been untrusts, and deletes the local copy of the files. One can be the original data owner or a trusted entity that shares some information with the owner [1]–[9]. One of the core design principles of outsourcing data is to provide dynamic behavior of data for different application.

PDP schemes presented [1]–[9] focus on only *static* or warehoused data that outsource data's is kept unchanged over remote servers and PDP constructions that deal with *dynamic* data are [10]–[14]. PDP schemes have been presented for *multiple* copies of *static* data [15]–[17], to the best of knowledge; this works is the first PDPs schemes directly dealing with *multiples* copies of *dynamic* data. When verifying multiple data copies and the overall systems integrity checks fails if there are one or more corrupted copies. To address this issue and recognize which copies have been corrupted, in this paper discusses a slight modification to be applied to the proposed scheme.

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 single-copy data.
- The paper shows the security of scheme against colluding servers, and discusses proposed scheme to identify corrupted copies.

System Architecture:

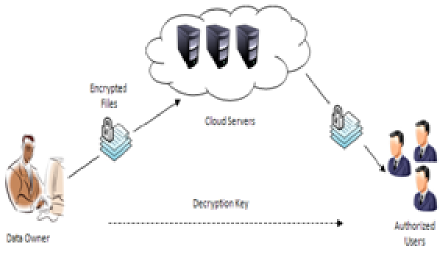
The cloud computing storage model considered in this work consists of three main components as illustrated in Fig.

1. A data owner that can be an organization originally possessing sensitive data to be stored in the cloud;
2. CSP who manages cloud servers (CSs) and provides paid storage space on its infrastructure to store the owner's files;

3. Authorized users — a set of owner's clients who have the right to access the remotes data.

The storages models used in this works can be adopts by many practical's applications. The numbers of copies depend on the natures of data's; more copies are needed for critical data that cannot easily be reproduced, and to achieve a higher level of scalability. This critical data should be replicated on multiple servers across multiple data centers.

The CSP pricing model is related to the number of data copies.



An authorized user of the outsourced data sends a data access request to the CSP and receives a file copy in an encrypted form that can be decrypted using a secret keys share with the owners. According to the loads balancing mechanism used by the CSP to organize the work of the servers, the data access requests is direct to the server with the lowest congestion, and thus the user is not aware of which copy has been received.

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.

2nd , a 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.

II. 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.

MB PMDDPs schemes allows the data owners to updates and scales the block of files copies outsource to cloud servers which may be untrusteds. Validating such copies of dynamics data required the knowledge of the blocked of versions to ensures that the data's block in all copy are consistent with the most recent modification issue by the owners. Moreover, the verified should be aware of the blocks indices to guarantees that the CSPs has inserts or added the news blocks at the requests position in all copies. To this ends, the propose schemes is based on using a small data's structures, which we call a map-versions tables.

Implementation The paper implemented the proposed MB-PMDDP scheme and the TB-PMDDP reference model on top of Amazon S3 is a web storages services to stores and retrieves almost unlimited amounts of data's. Moreover, it enable customer to specify geographies location for storing theirs data's. It present schemes consist of 3 modules:

OModules (owners modules), CModules (CSPs modules), and VModules (verifiers modules). OModules, which are running on the owner's sides, is a library that includes Key Gens, Copy Gens, Tag Gens, and Prepares Updates of algorithm. CModules is a library that runs on Amazons EC2 and includes Executes Updates and Proves algorithm. VModules is a library to be run at the verifiers sides and its include the algorithms and propose a new PDPs schemes, which its support outsourcing of multiple copies and dynamic data, the data owners is capable of not only archiving and accessing the data's copies stores by CSPs, and also updates and scaling these copies on the remotes servers.

III. CONCLUSION

The propose MB PMDDPs schemes outperform the TB-PMDDPs approaches derives from a classes of dynamics single-copies PDPs model. The TB-PMDDPs leads to high storages overheads on the remotes server & high computation on both the CSPs and the verifier's side. The MB-PMDDPs schemes significant reduce the computations times during the challenges responses phases which make it more practical's for application, for a larger numbers of verifier are connects to the CSPs causing a huge computations over heads on the server. Besides, it has lower storages over heads on the CSPs, and thus reduces the fee paid by the cloud customer. A light modifications can be done on the propose schemes to supports the features of identifying the indices of corrupts copies. The corrupts data copies can be reconstruct even from a completes damages using duplicate copies on others server. It has show throw security analysis, that the proposed scheme is provably secure.

IV. REFERENCES

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

[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.

AUTHOR’s PROFILE

G. Venkata Tejaswi is pursuing her M-Tech in Dept of CSE, Krishna Chaitanya Institute of Technology and Sciences, Markapur, Prakasam Dist, Affiliated to JNTUK University.

B.SUBBAREDDY Pursuing Ph.D from JNTU Hyderabad. He has 15 years of experience in Teaching. Currently working as Associate Professor & Head of the Department for CSE in Krishna Chaitanya Institute of Technology & Sciences, Markapur, Prakasam Dist, Affiliated by JNTUK University.