RSA Based CPDP with Adaptive Indexed Cluster for Distributed Cloud Storage Services

S.Abinaya[1] M.Kumaresan[2]
[1]M.E. [2]Assistant Professor
[1,2]Department of Computer Science and Engineering,
[1,2]PGP College of Engineering and Technology, Namakkal

Abstract—Provable data possession is a probabilistic technique for storage providers has proven integrity and ownership of client's data (without downloading) the essential for large files and folders. To check data is tampered with or deleted without downloading latest version of data. It provides replacement for hash and signature function in storage outsourcing. Most PDP schemes address scalability and dynamics of PDP Un-trusted servers in single cloud storage provider unsuitable for multi-cloud storages. Integrity of data storage outsourcing is done with provable data possession.

The existing work presented Cooperative Provable Data Possession (CPDP) scheme for distributed cloud storage. The multiple cloud service providers cooperatively store and maintain client's data. Operation of CPDP is based on Homo-morphic verifiable response and hash index hierarchy. The security of CPDP is arrived with multi-prover zero knowledge proof system. The performance optimization selects optimal metrics for clients and storage providers to minimize computation complexity and Communication overhead. IT present an RSA based CPDP with adaptive indexed cluster network for distributed cloud storage services. RSA encryption is associated with CPDP group user's data possession for multiple cloud storage locations of the client's data. The indexed clustered network is constructed to match the index structure of hash hierarchies of distributed cloud services. The indexed clustered network operations are based on adoptive parent tree hierarchy.

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

I. INTRODUCTION

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 internet 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.

Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing. In this paper, we address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. We present a cooperative PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy. We prove the security of our scheme based on multiprover zero-knowledge proof system, which can satisfy completeness, knowledge soundness, and zero-knowledge properties. In addition, we articulate performance optimization mechanisms for our scheme, and in particular present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers. Our experiments show that our solution introduces lower computation and communication overheads in comparison with noncooperative approaches.

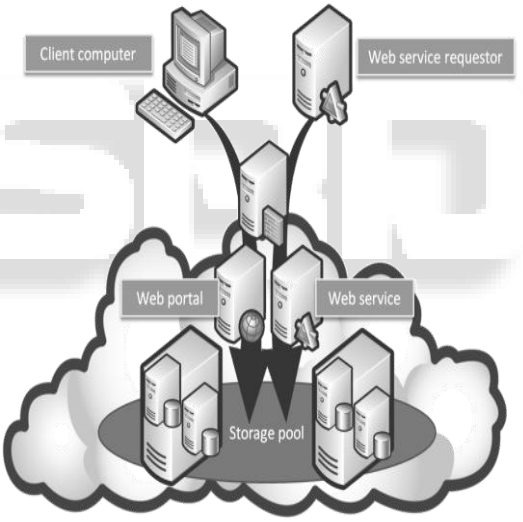

Fig. 1: Cloud storage systems

Cloud storage service has arrived greater demand due to its low cost, scalability and position independent platform. Open architecture interface of cloud environment provide highly interoperable multiple internal/external cloud services ensure clients to access data remotely through web service (interfaces). Multi-cloud help cloud providers to build distributed cloud storage for client's data but susceptible to security attacks Illegal access of confidential data. Tampering or loss of relevant data and achieves. Security attacks leads to provide security models for managing storage services.

II. LITERATURE SURVEY

More often than not, a cloud refers to an Infrastructure-as-a-Service (IaaS) cloud, such as Amazon EC2, where IT infrastructure is deployed in a cloud provider's datacenter in the form of virtual machines. With the growing popularity

of IaaS clouds, an ecosystem of tools and technologies is emerging that can transform an organization's existing infrastructure into a private cloud or a hybrid cloud [1]. Provable data possession (PDP) model is introduced that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof [2].

PORs are an important tool for semi-trusted online archives. Cryptographic techniques help users ensure the privacy and integrity of files they retrieve. It is also natural, however, for users to want to verify that archives do not delete or modify files prior to retrieval. The goal of a POR is to accomplish these checks without users having to download the files themselves. A POR can also provide quality-of-service guarantees [3]. The storage server is assumed to be untrusted in terms of both security and reliability. (In other words, it might maliciously or accidentally erase hosted data; it might also relegate it to slow or off-line storage.) The problem is exacerbated by the client being a small computing device with limited resources. Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form [4].

DPDP solution is based on a new variant of authenticated dictionaries, where we use rank information to organize dictionary entries. DPDP is able to support efficient authenticated operations on files at the block level, such as authenticated insert and delete. DPDP enables efficient proofs of a whole file system, enabling verification at different levels for different users (e.g., every user can verify her own home directory) and at the same time not having to download the whole data [5].

This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, it considered the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing [6]. HAIL cryptographically verifies and reactively reallocates file shares. It is robust against an active, mobile adversary, i.e., one that may progressively corrupt the full set of servers. This work proposes a strong, formal adversarial model for HAIL, and rigorous analysis and parameter choices. HAIL improves on the security and efficiency of existing tools, like Proofs of Retrievability (PORs) deployed on individual servers [7].

It build the first unbounded-use PoR scheme where the communication complexity is linear in the security parameter and which does not rely on Random Oracles, resolving an open question of Shacham and Waters. Also it builds the first bounded-use scheme with information-theoretic security [8]. On this basis of high security, verification transparency, and high performance, a verification framework for hybrid clouds along with the main techniques adopted: (1) fragment structure, (2) hash index hierarchy (HIH), and (3) homomorphic verifiable response (HVR). It is possible to construct a collaborative PDP (CPDP) scheme without compromising data privacy based on modern cryptographic techniques, such as multiprover zero-knowledge proof system (MPZKP) [9].
A general technique for the efficient computation of pairings is presented on super singular Abelian varieties. This formulation, which called the eta pairing, generalizes results of Duursma and Lee for computing the Tate pairing on super singular elliptic curves in characteristic three. It leads to a new algorithm which is about twice as fast as the Duursma-Lee method [10].
The phases involved in the proposed schemes are

1. Distributed Cloud Data Storage
2. Hash Index hierarchy (HIH) and Homo-morphic verifiable response (HVR)
3. Cooperative Provable Data Possessions
4. Adaptive Indexed Cluster
5. RSA based CPDP

A. Distributed Cloud Data Storage

The framework of Distributed cloud data storage comprises of entities such as Clients, Cloud Service Providers, and Trusted Third Party. The clients have large amount of data to be stored in multiple clouds and they have permissions to access and manipulate stored data. Cloud Service Providers (CSPs) work together to provide data storage services and have enough storages and computation resources. Trusted Third Party (TTP) used to trust to store verification parameters offer public query services for these parameters.

B. Hash Index hierarchy (HIH) and Homo-morphic verifiable response (HVR)

The Hash Index Hierarchy is a structure of index hash table is similar to structure of file block allocation table in file systems. It is used to utilize hash function in PDPs. Hash hierarchical structure consists of three layers. They are express layer, service layer, and storage layer. It represents relationships among all blocks for stored resources. It provides simple index-hash table to record the changes of file blocks and also generate the hash value of each block in the verification process. Index-hash table consists of serial number, block number, version number, and Random integer. All records in index table differ from one another to prevent forgery of data blocks and tags. Homo-morphic Verifiable Response is a map between two groups with Homomorphic Verifiable Tags (HVTs). It integrates multiple responses from the different CSPs in CPDP scheme. It's also used to reduce communication bandwidth and conceals location of outsourced data in distributed cloud storage environment.

C. Cooperative Provable Data Possessions

The index hash table records CPDP scheme support dynamic data operations. The CPDP scheme for multi-cloud system is constructed on collision-resistant hash, bilinear map group, aggregation algorithm, and homomorphic responses. CPDP process used for the organizer initiates the protocol and sends a commitment to the verifier. Verifier returns a challenge set of random index-coefficient pairs to the organizer. The organizer relays them into each cloud

storage provider according to the exact position of each data block. Each cloud storage provider returns its response of challenge to the organizer. The organizer synthesizes a final response from received responses and sends it to the verifier. The above process guarantees that the verifier accesses files without knowing on which CSPs or in what geographical locations their files reside.

D. Adaptive Indexed Cluster

The indexed clusters of the cloud storages are formed in the cloud service provider scenario. Index structure of hash hierarchies of distributed cloud services are matched with cluster ids of cloud data owners. Indexed clustered cloud storage operations are based on adoptive parent tree hierarchy. The adoptive parent supports cloud storage providers lacking parental cloud service node in its hierarchy. Null cloud data storage child are adopted by next nearest hop hierarchy parent. The adaptive ability of cloud data storage to support anonymous nodes is improved.

E. RSA based CPDP

RSA encryption is made into CPDP cloud data storage communication for cloud data owners and consumers. The cloud data user's data possession is provable secured with efficient cryptology adopted. The RSA public-key cryptography based on factoring large integers along with CPDP mode, The cloud data owners creates RSA publishes product of two large prime numbers along with an auxiliary value, as their public key. A prime factor was kept secret by trusted third party of cloud storage provider. Data owners or consumers use the public key to encrypt cloud data with currently published methods of cloud storage data owners. Public key is large enough to make hackers more difficult to decode original cloud data storages.

III. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section we evaluate performance of RSA based CPDP with Adaptive Indexed Cluster for Distributed Cloud Storage Services through cloudsim simulation. One of the major contributions of this work is the indexed cluster distributed based on the cloud storage services. To confirm the analytical results, we implemented RSA based CPDP with Adaptive Indexed Cluster for Distributed Cloud Storage Services in the implementation cloudsim and evaluated the performance of algorithm.

In order to construct performance evaluations, we have implemented Resource Efficient Position using the NS2 simulator which simulates several RSA based CPDP with Adaptive Indexed Cluster for Distributed Cloud Storage Services. The performance of RSA based CPDP with Adaptive Indexed Cluster for Distributed Cloud Storage Services is evaluated by the following metrics.

1. Computation Overhead
2. Communication Overhead
3. Data Integrity Rate

Figure 2 demonstrates the computation overhead. X axis represents user density whereas Y axis denotes the computation overhead using both the Cooperative Provable Data Possession Scheme and our proposed RSA based CPDP with Adaptive Indexed Cluster Network. When the number of user density increased computation overhead also gets increased.

User Density	Existing Cooperative Provable Data Possession (CPDP) Scheme	Proposed RSA based CPDP with Adaptive Indexed Cluster Network
10	200	100
20	240	130
30	340	210
40	430	235
50	520	300

Table 1: Computation Overhead

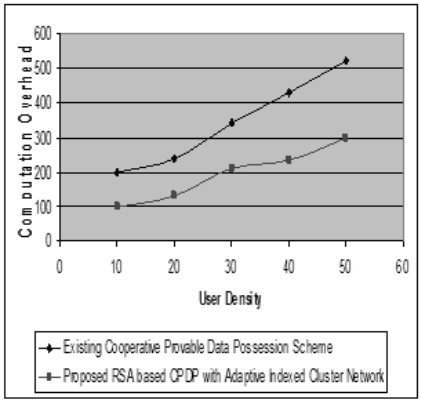

Fig. 2: Computation Overhead

Figure 2 shows the effectiveness of computation overhead over different number of user density than existing Cooperative Provable Data Possession Scheme and our proposed RSA based CPDP with Adaptive Indexed Cluster Network. RSA based CPDP with Adaptive Indexed Cluster Network achieves 15% to 23% more computation overhead when compared with existing schemes.

User Density	Existing Cooperative Provable Data Possession (CPDP) Scheme	Proposed RSA based CPDP with Adaptive Indexed Cluster Network
10	3.4	1.4
20	3.9	1.9
30	4.5	2.3
40	5.3	2.7
50	6.7	3.1

Table 2: Communication Overhead

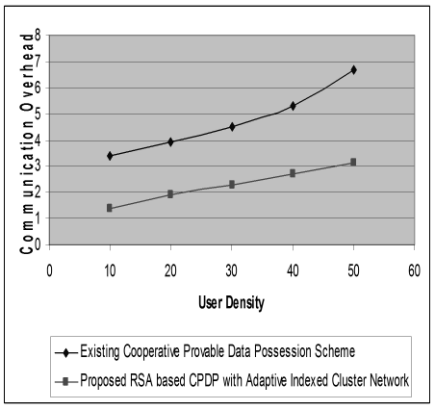

Fig. 3: Communication Overhead

Figure 3 demonstrates the communication overhead. X axis represents user density whereas Y axis denotes the communication overhead using both the Cooperative Provable Data Possession Scheme and our proposed RSA based CPDP with Adaptive Indexed Cluster Network. When the number of user density increased communication overhead also gets increased. RSA based CPDP with Adaptive Indexed Cluster Network achieves 25% to 35% more computation overhead when compared with existing schemes.

File Size	Existing Cooperative Provable Data Possession (CPDP) Scheme	Proposed RSA based CPDP with Adaptive Indexed Cluster Network
200	40	20
400	67	36
600	98	50
800	120	75
1000	175	100

Table 3: Delay Integrity Rate

Figure 4 demonstrates the delay integrity rate. X axis represents the file size whereas Y axis denotes the delay integrity rate using both the Cooperative Provable Data Possession Scheme and our proposed RSA based CPDP with Adaptive Indexed Cluster Network. When the number of file size increased, delay integrity rate also gets increases accordingly. The rate of delay integrity is illustrated using the existing Cooperative Provable Data Possession Scheme and proposed RSA based CPDP with Adaptive Indexed Cluster Network. Figure 4 shows better performance of Proposed RSA based CPDP with Adaptive Indexed Cluster Network in terms of delay integrity rate than existing Cooperative Provable Data Possession Scheme and Proposed RSA based CPDP with Adaptive Indexed Cluster Network. RSA based CPDP with Adaptive Indexed Cluster Network achieves 40 to 50% more delay integrity rate variation when compared with existing system.

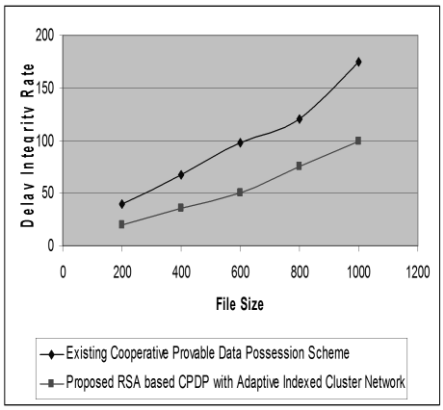

Fig. 4: Delay Integrity Rate

IV. CONCLUSION

In this paper, we presented the construction of an efficient PDP scheme for distributed cloud storage. Based on homomorphic verifiable response and hash index hierarchy, we have experiment 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. We have proposed RSA based CPDP with adaptive indexed cluster network for data possession is a probabilistic technique for storage providers.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609.

[9] 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.

[10] P. S. L. M. Barreto, S. D. Galbraith, C. O'Eigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties," Des. Codes Cryptography, vol. 42, no. 3, pp. 239–271, 2007.

