

Using Indirect Mutual Trust and Enabling Dynamic Data in Cloud Computing Storage Systems

Rohit H. Patil¹, Nitin S. Pawar², Dhiraj B. Chaudhari³, Mayur D. Pandav⁴, Prof.P.P.Waghralkar⁵

Department of Computer Engineering
1, 2, 3, 4, 5 P.V.P. Institute of Technology, Bavdhan, Pune

Abstract-Cloud service providers (CSP) are the services that provide storage space as a service for the organizations to store their important data on a server of the system. A cloud based storage scheme that permit the data owner to service from the facilities CSP and enables indirect mutual trust between them. The important feature of this scheme: First one it permits the owner to outsource sensitive data to a CSP, and perform full block level dynamic operations on the external data (i.e. append, deletion, insertion and modification). Second one it ensures that approved users (i.e. those that have the right to access the owner's file) receive the most recent version of the outsourced data. Third one it allows indirect mutual trust between the owner and also the cloud service providers. And fourth one it permits the owner to grant or revoke access to the external data. That justifies its performance through hypothetical analysis, model implementation and evaluation of communication, computation and storage overheads towards the cloud computing environment.

Keywords-Cloud computing, Data security, Data outsourcing, Cloud service provider, Mutual trust.

I. INTRODUCTION

In the current time of digital world, many organizations produce an oversized measure of sensitive data together with personal information, electronic health records, and financial data. The native management of such large quantity of data is problematic and expensive attributable to the wants of high storage capability and qualified personnel. Therefore, SaaS offered by cloud service providers (CSPs) emerged as an answer to mitigate the burden of large native data storage and cut back the upkeep price by means that of outsourcing data storage. The data proprietor physically discharges delicate information to a remote CSP; there are a few concerns in regards to access control, integrity and confidentiality of the data. The privacy highlight is secured by the owner by means of encoding the information before outsourcing to remote servers. For supportive data integrity over cloud servers, researchers have projected demonstrable data possession technique to validate the intactness of information hold on remote locales. Confirmation of irretrievability [10]-[13] was presented as a more grounded

system than PDP as in the whole information record can be remade from bits of the data that are dependably put away on the servers.[1]

Normally, customary get to control strategies accept the presence of the data owner and the storage servers in the same trust domain. This presumption, be that as it may, no more holds when the information is outsourced to a remote CSP, which takes the complete charge of the outsourced data management and dwells outside the trust domain of the data owner. A plausible arrangement can be introduced to empower the owner to authorize get to control of the data put away on a remote untrusted CSP. Which is imparted just to the approved clients. The unapproved clients, including the CSP, can't get to the data since they don't have the decryption key. This general arrangement has been broadly fused into existing plans [14]-[11], which go for giving data storage security on untrusted remote servers. Another class of solution uses attributes based encryption to accomplish fine-grained get to control [18], [19].

Diverse methodologies have been explored that energize the owner to outsource the information, and offer a few kind of sort of guarantee identified with the integrity, access control and confidentiality control of the outsourced data. These approaches can stop and find malicious actions from the CSP aspect. Then again, the CSP should be defended from an untrustworthy owner, who endeavors to get unlawful remunerations by dishonestly asserting data debasement over cloud servers. This worry, if not appropriately taken care of, can bring about the CSP to leave business [19].

In this work, a service that locations vital issues identified with outsourcing the storage of data, access control, newness, namely dynamic data and mutual trust. The remotely keep data will be not solely accessed by authorized users, however additionally updated and scaled by the owner. After change, authorized users should receive the most recent version of the data (newness property), i.e., a method is needed to observe whether or not the received data is stale. Mutual trust between the data owner and therefore the CSP is another imperative issue, which is addressed within the projected scheme. A mechanism is introduced to work out the dishonest party, i.e., misbehavior from any aspect is detected and therefore the responsible. [1]

II. RELATED WORK

We need to investigate the cloud based storage Outline Survey: Cloud system give significantly more compelling figuring by centralized memory processing, bandwidth and storage. The issue in distributed computing is that they are confronting a conceivably imposing danger for corrupted data or missing. Third person auditor ought to be ready to expeditiously audit the cloud based data storage while not difficult the native copy of data. DES method can use for encryption in CSP. A number of PDP protocols are given to expeditiously validate the integrity of data,[2]-[9] e.g., Proof of irretrievability was introduced as a strong technique than PDP within the sense that the whole record are often reconstructed from parts of the data that are dependably keep on the servers[10]. We introduce a model for demonstrable data possession (PDP) that permits a client that has keep data at an un-trusted server to verify that the server possesses the original data while not retrieving it. [1]

III. METHODOLOGY

The cloud computing storage model during this work consists of four main parts a data owner that may be a corporation generating sensitive data to be keep within the cloud and made out there for controlled external use. A CSP who manages cloud servers and provides paid space for storing on its infrastructure to store the owner's files and build them available for authorized users. Authorized users is a set of owner's purchasers who have the right to access the remote data and a trusted third party (TTP), an entity who is sure by all alternative system elements, and has capabilities to detect/specify dishonest parties.

Fig. 1 shows the relations between completely different system parts are denoted by double-sided arrows, where dotted and solid arrows represent trust and distrust relations, severally. as an example, the data owner, the authorized users, and also the CSP trust the TTP. On the opposite hand, the data owner and also the authorized users have mutual distrust relations with the CSP. Thus, the TTP is used to modify indirect mutual trust between these 3 components. There's a right away trust relation between the data owner and also the authorized users.

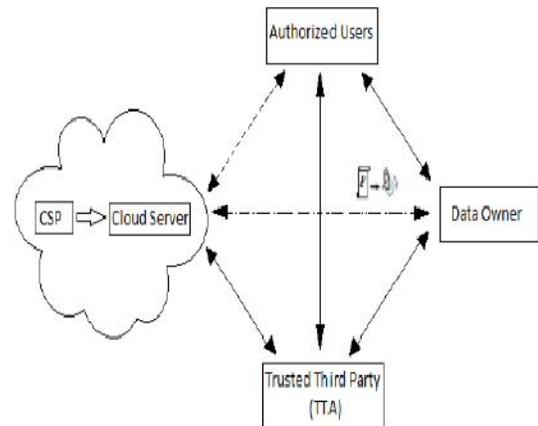


Fig.1 System Architecture

In this work, the auditing method of the data received from the CSP is completed by authorized users and we resort to the TTP only to resolve disputes that may arise relating to data integrity or age. Reducing the storage overhead on the CSP aspect is economically a key feature to lower the fees paid by the purchasers. Moreover, decreasing the computation value within the system is another crucial side. To realize these goals, a small part of the owner's work is delegated to the TTP. [1]

The owner encrypts before sending data to cloud servers. When data outsourcing, the owner will act with the CSP to perform block level operations on the file which included data. Additionally, the owner enforces access control by granting access rights to the outsourced data. To access the data, the authorized user sends a data access request to the CSP and receives the data file in an encrypted kind which will be decrypted using a secret key generated by the authorized user. [1]

Security Requirements

Confidentiality

Outsourced data must be protected from the TTP, the CSP and users that don't seem to be granted access.

Integrity

Outsourced data is needed to stay intact on cloud servers. The data owner and authorized users should be enabled to acknowledge data corruption over the CSP aspect.

Newness

Receiving the foremost recent version of the outsourced data file is an essential demand of cloud-based

storagesystems. There should be an identification system if the CSP disregards any data overhaul demands issued by the owner.

Access control

Only authorized users are allowed to access the outsourced data. Revoked users will read unmodified data; however, they need to not be able to read updated/new blocks.

Defense

The CSP should be safeguarded against false accusations which will be claimed by dishonest owner/users and such a malicious conduct is required to be uncovered. [1]

IV. RESULT ANALYSIS

To evaluate the computation overhead on the owner side due to dynamic operations, we perform 100 different block operations from which 50% are executed following revocations (this percent is higher than an average value in practical applications). For different number of system users, Fig. 2 shows the owner's average computation overhead per operation.

Table 1. Computation overhead per user

System Users	Computation Overhead (in Sec)
20000	0.19
40000	0.28
60000	0.42
80000	0.53
100000	0.61

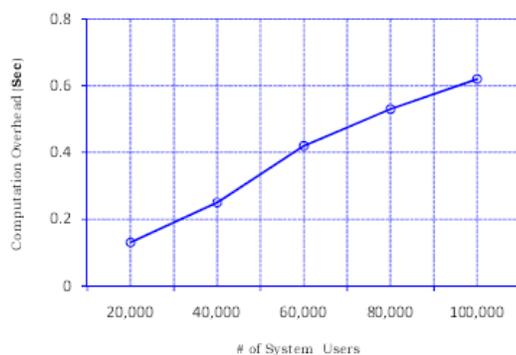


Fig. 2. Average computation overhead per operation.

V. CONCLUSION

In this paper, we have present a cloud-based storage scheme which support outsourcing of dynamic data, where the

owner is fit for not just filing and getting to the data put away by the CSP, additionally scaling and updating this data on the remote servers. The presented system enables the authorized users to guarantee that they are getting the latest adaptation of the outsourced data. Also, in case of dispute about data newness/integrity, a TTP can decide the exploitative party. The data owner implements get to control for the outsourced data by joining three cryptographic systems: lazy revocation, key rotation and broadcast encryption. We have concentrated on the security components of the present's scheme.

REFERENCES

- [1] Rohit H. Patil , Dhiraj B. Chaudhari and et. al. "Cloud Computing Storage System Using Enabling Dynamic Data and Indirect Mutual Trust : A Survey" in IERJ vol. 2, issue 8 ,pp 2775-2777.
- [2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, —Provable data possession at untrusted stores, in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.
- [3] F. Seb' e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, —Efficient remote data possession checking in critical information infrastructures, IEEE Trans. on Knowl. And Data Eng., vol. 20, no. 8, 2008.
- [4] 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 Networks, 2008, pp. 1–10.
- [5] C. Erway, A. K'upc, " u, C. Papamanthou, and R. Tamassia, —Dynamic provable data possession, in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 213–222.
- [6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing, in Proceedings of the 14th European Conference on Research in Computer Security, 2009, pp. 355–370.
- [7] A. F. Barsoum and M. A. Hasan, Provable possession and replication of data over cloud servers, Centre For Applied Cryptographic Research, Report 2010/32, 2010, <http://www.cacr.math.uwaterloo.ca/techreports/2010/cacr2010-32.pdf>.
- [8] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, MR PDP: multiple-replica provable data possession, in 28th IEEE ICDCS, 2008, pp. 411–420.
- [9] A. F. Barsoum and M. A. Hasan, On verifying dynamic multiple data copies over cloud servers, Cryptology

- ePrint Archive, Report 2011/447, 2011, 2011, <http://eprint.iacr.org/>.
- [10] K. D. Bowers, A. Juels, and A. Oprea, HAIL: a high-availability and integrity layer for cloud storage, in *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2009, pp. 187–198.
- [11] Y. Dodis, S. Vadhan, and D. Wichs, Proofs of retrievability via hardness amplification, in *Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography*, 2009.
- [12] A. Juels and B. S. Kaliski, PORs: Proofs of Retrievability for large files, in *CCS'07: Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 584–597.
- [13] H. Shacham and B. Waters, Compact proofs of retrievability, in *ASIACRYPT '08*, 2008, pp. 90–107.
- [14] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, —Plutus: Scalable secure file sharing on untrusted storage, in *Proceedings of the FAST 03: File and Storage Technologies*, 2003.
- [15] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, Sirius: Securing remote untrusted storage, in *Proceedings of the Network and Distributed System Security Symposium, NDSS*, 2003.
- [16] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage, in *NDSS*, 2005.
- [17] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, —Over-encryption: Management of access control evolution on outsourced data, in *Proceedings of the 33rd International Conference on Very Large Data Bases*. ACM, 2007, pp. 123–134.
- [18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in *CCS '06*, 2006, pp. 89–98.
- [19] S. Yu, C. Wang, K. Ren, and W. Lou, —Achieving secure, scalable, and fine-grained data access control in cloud computing, in *INFOCOM'10*, 2010, pp. 534–542