International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 543-546 1 May 2014

Privacy Preserving Public Auditing for Secure Cloud Storage-Replica

[1]V. Deepa, [2]K.Rajakumari
Department of Computer Science, Baharath University, Chennai, India
[1]intimatetodeepa@gmail.com , [2] mail2rajkumari@gmail.com

Abstract—***Using cloud computing user will be able to store and secure their data without burden of local computer. Additionally, users should be able to just use the cloud storage as if it is local, without distressing about the need to verify its integrity. By enabling and using public audit for cloud storage, it can check the integrity of the data. Finding data that are corrupted using this is difficult. To have original data integrity for our cloud user by cloud server provider (CSP) replica should be taken. We propose a secure cloud storage system supporting privacy preserving public auditing and having replica of the data which supports to retrieve the lost data. We further extend our result to have more efficient cryptographic algorithm to maintain the replica of data. Shown the performance and security analysis of the proposed schemes are provably secure and highly efficient.***

Index Terms—Third-party auditor (TPA), replica, cloud service provider (CSP)

I. INTRODUCTION

Cloud computing is that the delivery of computing services over the web. Cloud services permit people and businesses to use package and hardware that are managed by third parties at remote locations. Samples of cloud services embrace on-line file storage, social networking sites, webmail and on-line business applications. The cloud computing model allows access to data and pc resources from anyplace that a network affiliation is on the market. Cloud computing gives a shared pool of resources, as well as knowledge cupboard space, networks, pc process power and specialized company and user applications. Services can be scaled bigger or minor and use of a service is measured and customers are billed accordingly. The cloud computing service models SaaS (software package as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). During a software package as a Service model, a pre-made application, in conjunction with any needed software package, package, hardware and network square measure provided. In PaaS, Associate in Nursing package, hardware, and network square measure provided and therefore the client installs or develops its own software package and applications. The IaaS model provides simply the hardware and network; the client installs or develops its own operative systems, software package and applications. Cloud computing has been developed by the [5]U.S. National Institute of Standards and Technology (NIST).

Using cloud storage, users will remotely store their knowledge and luxuriate in the on-demand high-quality applications and services from a shared pool of configurable computing resources, while not the burden of native knowledge storage and maintenance. Moreover, users ought to be able to simply use the cloud storage as if it's native, without concern regarding the requirement to verify its integrity. [3] Thus, enabling public audit ability for cloud storage is of important so users will resort to a third-party auditor (TPA) to examine the integrity of outsourced knowledge and be concern free. To firmly introduce a good TPA, the auditing method mustn't bring new vulnerabilities toward user knowledge privacy and introduce no extra on-line burden to user. Cloud computing provides flexibility to users and Users pay the maximum amount as they use Users don't ought to originated the massive computers however the operation is managed by the Cloud Service supplier (CSP) the user offer their knowledge to CSP; CSP has management on (the knowledge the information) the user has to confirm the information is correct on the cloud Internal (some worker at CSP) and external (hackers) threats for data integrity CSP would possibly behave unreliably.

As enabling public audit ability for cloud storage, using storage that we can check the integrity of the data. In this auditing it's difficult to find the data. So before it auditing has to take the replica of our original data integrity for our cloud user by cloud server provider. We propose a secure cloud storage system supporting privacy-preserving public auditing and taking replica of the data which supports to retrieve the lost data. Section-II introduces the related work of the paper. Then Section-III introduces for what are the demerits consider in the previews paper, then what going proposed in Section-IV, Experimental setup & Result discussed in Section-V, Conclusion of the paper in Section-VI, References in Section-VII.

II. RELATED WORKS

Multiple-Replica Provable Data Possession

Most storage systems trust replication to extend the provision and sturdiness of knowledge on non trustworthy storage systems. At present, such storage systems give no robust proof that multiple copies of the information are literally hold on. Storage servers will to form it appear as if they're storing several copies of the information, whereas actually they solely store one copy. We tend to address this disadvantage through [7]multiple-replica obvious knowledge possession (MR-PDP).

A provably-secure theme that permits a consumer that stores t duplicates of a go in a storage system to verify through a challenge-response protocol that (a) every distinctive duplicate may be created at the time of the challenge which (b) the storage system uses t times the storage needed to store one replica. MR-PDP extends previous work on knowledge possession proofs for one copy of a go in a client/server storage system. Victimization MR-PDP to store t replicas is computationally way more economical than employing a single-replica PDP theme to store t separate, unrelated files (e.g., by encrypting every file one by one before storing it).

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 543-546 1 May 2014

Another advantage of MR-PDP is that it will generate additional replicas on demand, at very little expense, once a number of the prevailing replicas fail.

Dynamic Provable Data Possession

In order to form positive that integrity of the info within the Cloud, [2] particularly the dynamic files which might be updated on-line, we have a tendency to propose Associate in Nursing improved dynamic obvious knowledge possession model: It divides file into blocks, generates a tag for every block, computes a hash price for every tag, uses tags to make sure the integrity of the file blocks, and uses hash values to make sure the integrity of the tags. Having concern with Compare with previous works, it reduces the procedure and communication quality from login to constant. Though consumer has to store some secret values which can produce some extra storage expense, it solely takes up concerning zero.02% of the initial file size.

Towards Publicly Auditable Secure Cloud Data Storage Services

Cloud computing is that the long unreal vision of computing as a utility, wherever knowledge data owners will remotely store their knowledge within the cloud to fancy on-demand high-quality applications and services from a shared pool of configurable computing resources. Whereas knowledge outsourcing relieves the data owners of the burden of native knowledge storage and maintenance, it additionally eliminates their physical management of storage responsibleness and security, that historically has been expected by each enterprises and people with high service-level necessities. So as to facilitate fast preparation of cloud knowledge storage service and regain security assurances with outsourced knowledge responsibleness, economical ways that change on-demand knowledge correctness verification on behalf of cloud knowledge data owners got to be designed. During this article we tend to propose that in public auditable cloud knowledge storage is ready to assist this emerging cloud economy become totally established. With public auditability, a sure entity expertly expert and capabilities knowledge data owners don't possess may be delegated as an external audit party to assess the danger of outsourced knowledge once required. Such associate degree auditing service not solely helps save knowledge computation resources however additionally provides a clear however cost-efficient technique for knowledge owners to realize trust within the cloud. We tend to describe approaches and system necessities that ought to be brought into thought, and description challenges that require to be resolved for such a in public auditable secure cloud storage service to become a reality.

Above the Clouds: A Berkeley View of Cloud Computing

[6]Cloud Computing, the awaiting dream of computing as a utility, has the potential to transform a huge part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for fresh Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus lost potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is extraordinary in the history of IT

III. PROBLEM STATEMENTS

When we consider a cloud data storage service involving three different entities, the *cloud user* (U), who has large amount of data files to be stored in the cloud; the *cloud server* (CS), which is managed by the *cloud service provider* (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter); the [4] *third party auditor* (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request.

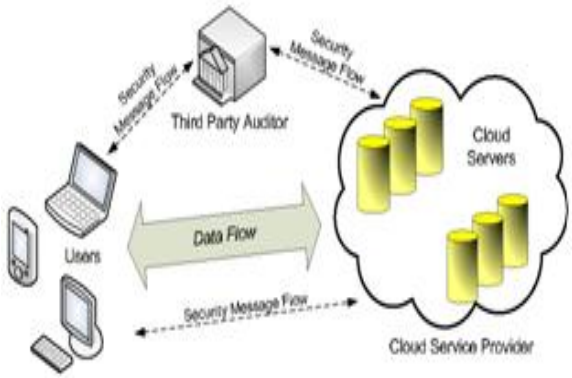
- As security threat is very high, which restrict user to use cloud computing
- Existing mechanism for audit is not sufficient enough to handle audit
- loss of control over data
- [1] Dependence on the Cloud Computing provider.

IV. PROPOSED SCHEMES

In the Proposed System, we are implementing the secure system namely Privacy preserving auditing with replica of data. In this system, first the Data Owner will register with the Cloud Service Providers. During the registration phase the Public and Private will be generated for the Data Owner. The Data Owner has to provide their Private Key while updating their data in the Cloud Server. Using Merkle Hash Tree Algorithm the Cloud Server Split the in to batches. The Cloud Server will allow the Trusted Party Auditor (TPA) to audit the data that was Stored in the Cloud Server as requested by the User. The TPA will also audit multiple Files also.

- The user is allowed to access the data only by providing the Public and Private key components By allowing the Trusted party Auditor to audit the data will increase the Trustworthiness between the User and Cloud Service Providers.
- By using (MHT) Merkle Hash Tree Algorithm the data will be audited via multiple level of batch auditing Process
- As Business Point of view, the Company's Customers will be increased due to the Security and Auditing Process.
- Uses homomorphic authenticator (HA)
- Pseudo Random Function (PRF) provide a random mask that we can use

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 543-546 1 May 2014



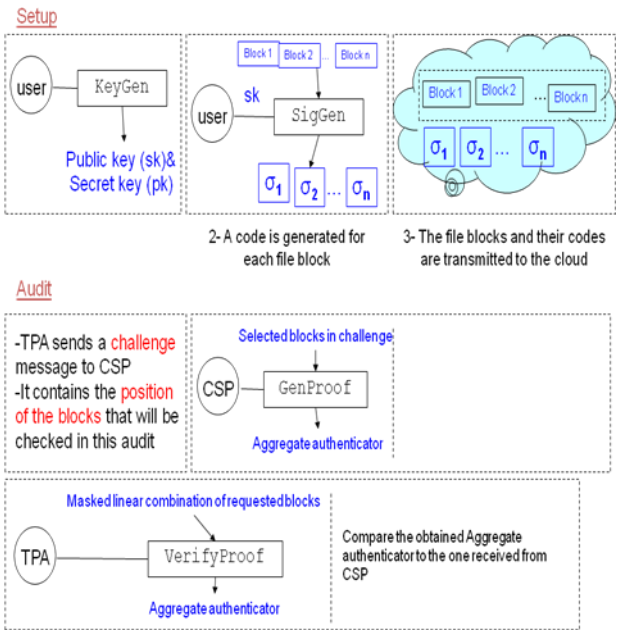
"Fig" The architecture of cloud data storage service

Algorithm

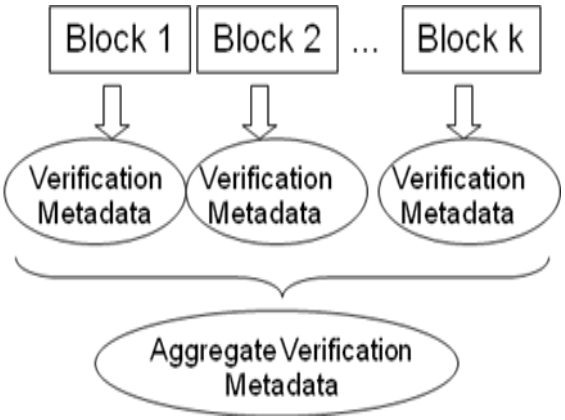
These algorithm are (KeyGen, SigGen, GenProof, VerifyProof, MHT)

- KeyGen: A algorithm for key generation that is run by the user to setup the scheme
- SigGen: Verification metadata that are generated by the user, that consist of signatures, MAC or Other information used for doing auditing
- GenProof: Cloud server runs to generate a proof of data storage correctness
- VerifyProof: TPA runs to audit the proof of data from the cloud server
- MHT: (Merkle hash tree) It is used to divide the data as a block.

V. EXPERIMENTAL SETUP & RESULTS



- User generates public and secret parameters
- A code is generated for each file block
- The file blocks and their codes are transmitted to the cloud
- TPA sends a challenge message to CSP
- It contains the position of the blocks that will be checked in this audit
- CSP also makes a linear combination of selected blocks and applies a mask. Separate PRF key for each auditing.



"Fig" Homomorphic authendicator

Block – It splits as blocks n based on file size
Verification Metadata – Verify the meta data of the file
In addition to Aggregate Authenticator, a linear combination of file blocks re received by TPA

$$\mu' = \sum_{i \in I} \nu_i m_i$$

v_i are random number
m_i are file blocks

- TPA might be able to infer the file blocks, if it has many linear combinations of the same block
- Pseudo Random Function (PRF) provide a random mask that we can use

V. CONCLUSION

In this paper we propose a Replica of Public Auditing for Secure Cloud Storage We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process. And also provide the replica of the user's data during the auditing process, which supports to retrieve the lost data.

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 543-546 1 May 2014

VI. REFERENCES

i. *Derrick Harris "Watch Out, World: IBM Finally Offers a Real Cloud". Giga Om. Retrieved 5 January 2012.*

ii. *Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.*

iii. *C. Wang, Q. Wang, K. Ren, & W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.*

iv. *Cloud Security Alliance, "Top Threats to Cloud Computing, "http://www.cloudsecurityalliance.org, 2010.*

v. *P. Mell and T. Grance, "Draft NIST Working Definition ofCloud Computing,"http://csrc.nist.gov/groups/SNS/cloudcomputing/ index.html, June 2009.*

vi. *M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.*

vii. *G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.*