Privacy-Preserving and Public Auditing for Cloud Storage Applying Regeneration-Code-based using RSA Algorithm

Pooja K. Patil
Professor, Dr. D. Y. P. C. O. E Ambi, Pune

Reshma Anil Bhailume
BE Computer (SEM VII). Dr. D. Y. P. C. O. E Ambi, Pune

Dipali Arun Ware
BE Computer (SEM VII). Dr. D. Y. P. C. O. E Ambi, Pune

Sayali Avinash Inamdar
BE Computer (SEM VII). Dr. D. Y. P. C. O. E Ambi, Pune

Sushma Bhagwat Waghmare
BE Computer (SEM VII). Dr. D. Y. P. C. O. E Ambi, Pune

ABSTRACT
The cloud has measure issues of bulk data storage, outsourced data corruptions, fault tolerance together with data integrity check and failure reparation. Another problem is that user need to always stay online for the purpose of continuous auditing of his own data which is not practically possible, especially for long-term archival storage. This might result in data owner's loss of ultimate control over the fate of their outsourced data [1]. Thus, the correctness, accessibility and reliability of the data are being put at risk.

To solve the above problem of failed auditing in the absence of data owners, system introduce a proxy server, which is privileged to regenerate the authenticators, into the traditional public auditing system. This arrangement helps to outsource the burden of continuous online availability of user for auditing purpose to proxy server. In addition to this systems introduce regenerating-code-based cloud storage to handle the problem of data integrity check and failure reparation.

Keywords
Cloud storage, regenerating codes, public audit, privacy preserving, authenticator regeneration, proxy, privileged, provable secure.

1. INTRODUCTION
Cloud storage offers an on-demand data outsourcing service model, and is fast popularity due to its flexibility and low maintenance cost. However, security concerns arise when data storage is stored to TPA storage providers. It is desirable to enable cloud clients to verify the integrity of their stored data, in case their data have been accidentally corrupted or unkindly compromised by insider/outsider attacks. One major use of cloud storage is continuing retrieval, which represents a workload that is written once and hardly read [1][3].While the stored data are hardly read, it remains necessary to ensure its integrity for failure recovery or fulfillment with legal requirements . Since it is normally to have a large size archived data, whole-file checking becomes unaffordable. POR [2] and PDP [3][4]have thus been proposed to verify the integrity of a large file by point by point checking only a portion of the file via various cryptographic primitives.

Storage of a data on to a server, which could be a CSP. If user detect corruptions in users stored data (e.g., when a server crashes or is attacks), then user should repair the corrupted and deleted data and restore the original data of a user. However, putting all data in a single server is vulnerable and also it is very risky to the single point-of-failure problem. Thus, to repair and reconstruct a failed server, user can 1) Read data from the other available servers2) Reconstruct the corrupted and reconstruct data of the failed server, and3)Write reconstructed data to new server.

Proofs of Retrievability and PDP this concept are originally proposed for the single-server. MR-PDP and HAIL [4][5]provides integrity checks to more than one servers setting using duplication and erasure coding, respectively. In particular, erasure coding (e.g. R-S codes) has a lower storage operating cost than replication under the same fault tolerance level. Field measurements describes that huge-scale storage systems commonly experience disk/sector failures. Some of which can result in permanently data loss. For example, the Annualized Replacement Rate for disks in production storage systems. Data loss is also found in commercial in CSS.

2. LITERATURE SURVEY
Fox, R. Griffithet al [1] proposed that developers with advanced ideas for new Internet services no longer require the large capital expenditures in hardware to deploy their service or the human expense to operate it. They need not be concerned about provisioning for a service whose popularity does not meet their prospects, thus the costly resources are getting waste or under- provisioning for one that becomes uncontrollably popular ,thus missing possible customers and income .**Juels, B. S. KaliskiJr et al [3]**They define and explore proofs of Retrievability. A POR system enable an back-up service to produce a brief proof that a user which is also called verifier can retrieve a target file f, that is, that the archive retains and dependably transmits file data sufficient for the user to recover and reconstruct f in its entirety.

A POR may be viewed as a type of cryptographic POK, but one specially designed to handle a large file f. **R. Curtmola, O. Khan, R. Burns et al [4]**Many storage systems trust on replication to increase the availability and durability of data on not trusty storage systems. At in attendance, such storage systems does not provides strong and correct evidence that number of copies of the data are actually stored. Storage servers can plan to make it look like a original copies in many forms they are storing of the data, whereas in reality they only store a single copy **K. D. Bowers, A. Juels et al [5]**They introduce HAIL (High-Availability and Integrity Layer), a scattered cryptographic system that permit a number of servers to show to a client that a stored file is in-tact and retrievable. HAIL strengthens, formally unifies, and

streamlines separate approaches from the cryptographic and distributed-systems communities. Proofs in HAIL are efficiently calculable by servers and highly compact typically tens or hundreds of bytes, irrespective of file size. [2][3]

2.1 Cloud storage

Cloud storage is now gaining popularity because it offers a flexible and on-demand data storing service with appeals benefit: relief of the burden for storage management, universal data access with not dependant on location, and avoid of capital cost on hardware, software, and personal maintenances etc.[14][15] Nevertheless, this new part of data hosts service also brings new security threats toward users data, thus making enterprisers still feel hesitant. It is noted that data owners lose his power on data.

2.2 Proposed system

In this paper, system concentrate on the honesty verification issue in recovering code-based distributed storage, particularly with the effective repair method. Considering the unreserved size of the outsourced information and the client's obliged asset capacity, the undertakings of evaluating and reparation in the cloud can be imposing and costly for the clients. The overhead of utilizing distributed storage have to be minimized however much as could be expected such that a client does not have toper form an excess of operations to their outsourced information.[3][5][11]

3. OBJECTIVE

1 System focus on the integrity verification problem in regenerating-code-based cloud storage, especially with the practical restore strategy.

2 Only the data owner is allowed to verify the integrity and repair the faulty servers. Considering the huge size of the stored data and the user's constrained resource capability.

3 To allow Third Party Auditor to verify the intactness of the data in the cloud on demand without introducing additional online burden to the data owner.

4 To ensure that the cloud server can never pass the auditing procedure except when it to be sure manages the owner's data undamaged.

4. SYSTEM DESIGN

4.1 Modules

1. Setup Module:

The data owner maintains this procedure to initialize the auditing scheme.

2.Audit Module:

The cloud servers and TPA interact with one another to take a random sample on the blocks and check the data intactness in this method.

3. Repair Module:

In the absence of the data owner, the proxy interacts with the cloud servers for the period of this procedure to repair the wrong server detected by the auditing process.

5. ALGORITHMS

RSA Algorithm:

RSA stands for Rivest-shamir-Adleman. It is one of cryptosystem for public key encryption and is generally used for securing responsive data. Which uses two different keys one is public and another is private. The public key can be shared by everyone and private key must be kept secret. It provides method of assuring the confidentiality, integrity, authenticity.[13][15]

Key Generation: key Gen(p,q)
Input: p,q €P
Compute: n=p.q Choose e such that Ø(n)=(p-1)(q-1) Gcd(e, Ø(n))=1 Determine d such that e.d mod Ø(n))=1
Output: (pk,sk) Public key=(e,n) Secret key=(d,n)

Encryption: Enc(m,pk)
Input: $m \in Z_n$
Compute: $C=m^e \bmod n$
Output: $C \in Z_n$

Decryption:Dec(C,sk)
Input: $e \in Z_n$
Compute: $m=C^d \bmod n$
Output: $m \in Z_n$

6. SYSTEM ARCHITECTURE

Distributed storage is presently picking up prevalence in light of the fact that it offers a flexible on-interest information outsourcing administration with engaging benefits: help of the weight for capacity administration, widespread information access with area freedom, and shirking of capital consumption on equipment, programming, and individual maintenances etc., Nevertheless, this new worldview of information facilitating administration additionally brings new security dangers toward clients information, accordingly making people or enter presser still feel reluctant.[6][7][14]

It is noticed that information proprietor lose extreme control over the destiny of their outsourced information; subsequently, the rightness, accessibility and honesty of the information are being put at danger.[9] From one viewpoint, the cloud administration is typically confronted with a wide scope of inside/outer enemies, who might noxiously erase or degenerate clients' information; then again, the cloud service providers may act untrustworthily, endeavoring to conceal information misfortune or defilement and asserting .[12][10]

Accordingly it bodes well for clients to actualize an efficient convention to perform periodical verification of their stored information to guarantee that the cloud for sure keeps up their information correctly. Cloud storage is now getting popularity because it offers a flexible on-demand data storing service with appealing different benefits: relief of the load for storage management, overall data access with different from location, and opposing of money cost on hardware, software, and personal maintenance, etc.[8] Nevertheless, this new paradigm of data hosting service also brings new security errors to the user's data, thus making individuals still feel headache. It is noted that data owners loss ultimate control their stored data; thus, the accuracy, available and intactness of the data are being put at risk. [9][10][11]

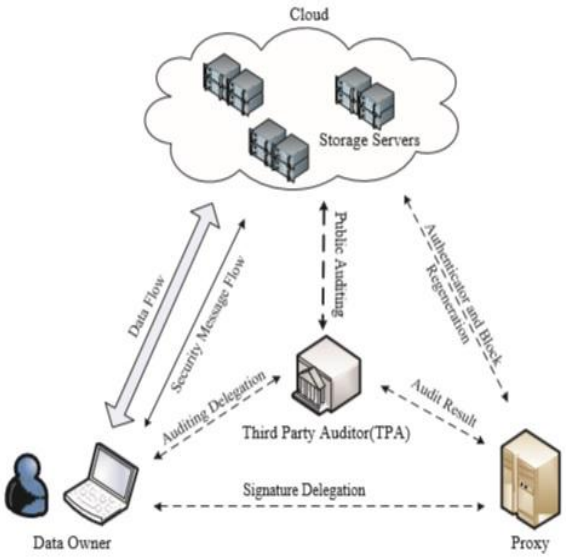

Fig 1:-System Architecture

The cloud service is usually interacting with a large range of internal/external equipments, which would dangerous delete users' data.

Uultimate control over the fate of their saved data; the accuracy, available and intactness of the data are on the very danger condition. The cloud service is usually faced with a large range of internal/external equipments, who would fraud delete users' data; oppositely , the CSPs may act not honestly, attempting to hide data loss or corruption surly says that the files are still correctly stored in the cloud for reputation reasons. Thus it makes great sense for users to implement an effective protocol to perform periodical verification of their stored data to ensure that the cloud maintains their data.

7. CONCLUSION

The public auditing scheme for the regenerating-code-based cloud storage system, where the data owners are privileged to assign TPA for their data validity checking. To protect the original data privacy against the TPA, the System randomizes the coefficients in the beginning rather than applying the blind method during the auditing process. Considering that the data owner cannot always stay online in practice, in order to keep the storage accessible and verify after a malicious corruption, the system introduce a semi-trusted proxy into the system model and provide a freedom for the proxy to handle the reparation of the coded blocks and authenticator. To better appropriate for the regenerating-code, system design the authenticator based on the BLS signature. This authenticator can be efficiently generated by the data owner simultaneously with the encoding procedure.

This system has a future scope that it will secure the data which is stored on cloud. If any data will loosed it will automatically regenerate this properly.

8. REFERENCES

[1] Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, Dept. Electrical Eng. and Comput. Sciences, Above the clouds: A berkeley view of cloud computing.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598– 609, Provable data possession at untrusted stores.

[3] Juels and B. S. KaliskiJr, in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597. Pors: Proofs of retrievability for large files.

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, in Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on. IEEE, 2008, pp. 411–420. Mr-pdp: Multiple- replica provable data possession.

[5] K. D. Bowers, A. Juels, and A. Oprea, in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 187–198.Hail: a high-availability and integrity layer for cloud storage.

[6] Bo Chen, Reza Curtmola, Giuseppe Ateniese, Randal Burns, Remote Data Checking for Network Coding-basedDistributed Storage Systems.

[7] Henry C. H. Chen and Patrick P. C. Lee, Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage.

[8] Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE, An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing.

[9] Yunghsiang S. Han, Fellow, IEEE, Hung-Ta Pai, Senior Member, IEEE, Efficient Exact Regenerating Codes for Byzantine Fault Tolerance in Distributed Networked Storage.

[10] Boyang Wang, Student Member, IEEE, Baochun Li, Oruta: Privacy-Preserving Public Auditing For Shared Data in the Cloud.

[11] Chao Tian, Senior Member, IEEE, Characterizing the Rate Region of the (4, 3, 3) Exact-Repair Regenerating Codes.

[12] S. Nancy Priya1, D. Elavarasi, Remote resource maintenance with data integrity based on code regeneration scheme.

[13] Jing He a, Yanchun Zhang a, Guangyan Huang a, Yong Shib, c, Distributed data possession checking for securing multiple replicas in geographically-dispersed clouds.

[14] Henry C.H. Chen and Patrick P.C. Lee, Enabling Data Integrity Protection in Regenerating- Coding- Based Cloud Storage: Theory and Implementation.

[15] Onur Ozan Koyluoglu, Member, IEEE, Ankit Singh RawatSecure Cooperative Regenerating Codes for Distributed StorageSystems.