Improving Audit Service in Cloud for Outsourced Storage Dynamically

[1]N.Praveen kumar, [2]S.Bavaji
[1]*M.Tech Student,*[2]*Assistant Professor,*
Dept. of CSE.,Sree Vidyanikethan Engineering College, Tirupati, Andhra Pradesh, India.

Abstract**: In this paper, we discuss cloud computing is a dreamed of computing as a fifth type of utility, In this type of utility users can remotely store their data into the cloud environment such that to enjoy the on-demand required high quality applications and services from a shared pool of configurable computing resources. In such a way that cloud based outsourced storage relieves the client`s load for storage management and preservation by providing an equivalently scalable, low cost, location independent platform. The main part in the paper is Data integrity and storage efficiency are the two important requirements for cloud storages Authorized users access the data and shares the files in secure manner. Such as fragment structures, random sampling, index hash table and Advanced Cryptographic Techniques to avoid the data loss and corrupt the Meta data.**

Keywords**: Storage security, provable data possession, audit service, cloud storage, RSA.**

I. INTRODUCTION

Cloud computing may provides a flexible environment for improving amounts of data and that that work are processes in all applications and the services are on demand self-services. The outsourced storage capable in clouds containing a new profit growth point, this may provides a comparably scalable, maintain low-cost location-independent platform for client managing users (client's) data. The Cloud Storage Services (CSS) improves the burden for maintain the storage management [2]. However the some important service is dangerous to attacks or failures, it would takes irretrievable irretrievable Losses to the clients because their data or archives are stored in an uncertain storage pool outside the enterprises or platforms . These Security risks are rising from the following reasons: Firstly, the cloud infrastructures are very powerful and authentic than personal computing devices too, but they are still capable to internal threats (e.g., via virtual machine) and external threats (e.g., via system holes) that can damage data integrity and cost maintains cost; secondly, for the benefits of possession, there exist various motivations for cloud service providers to behave unbelievable toward the cloud customers; it disputes occasionally suffer from lack of trust on CSP because the data change may not be timely known by the cloud users, even if these disputes may result from the users' own indefinite operations.

II. RELATED WORK

Security audit is a important solution to enabling trace-back and understanding of any performances including data accesses, security reaches, and application activities, and so on. And it compared to the common audit, the audit services for cloud storages should provide to clients with a more efficient proof that can verifies the integrity of stored data. Unfortunately, the traditional cryptographic technology depends on hash functions and signature schemes thus cannot be support for data integrity on without a local copy of data. In addition, it is obviously impractical for audit services to download all data for checking data validation due to the communication cost, particularly for large-size files[1].

Therefore, security and performance methods should be mapped to achieve an effective audit for outsourced storages in clouds:

- *Public audit ability*: This allows for a Third Party Auditor or clients with the help of TPA to checks the correctness of cloud data on demand without recovering a copy data or introducing additional online burden to cloud services.
- *Dynamic operations*: To ensure there is no attack to compromise the security of verification protocol.
- Timely detection. To identify the data errors or losses in outsourced storage, as well as behaviors of data operations in a timely manner.
- *Effective forensic*: To allow TPA for strict audit and supervision for outsourced data, and offer Efficient evidences for anomalies.
- *Light weight:* By this to find and perform the audit tasks with minimum storage and low communication cost and less computation.
- Email Authentication. By using Email to verify the clients are performed the right operations are not.

Cloud data storage service involving three type of entities, as shown in Fig.1

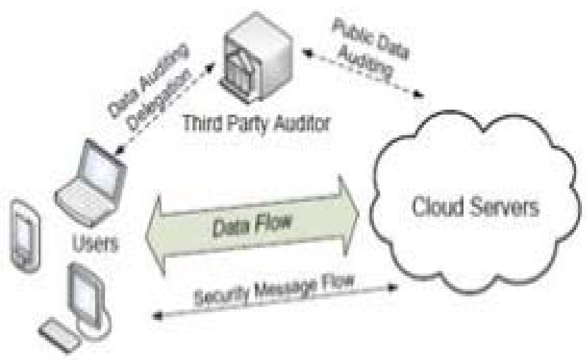


Fig 1: Architecture of Cloud Storage Service

1. The cloud user (U), which contains huge amount of data files that can stored in the cloud.
2. 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.
3. The 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.

We mainly introduce audit system architecture for outsourced data in clouds. To realize these functions, our proposed audit service is comprised of three processes:

I. *Tag generation:* The client (DO) uses a secret key to preprocess a file, which consists of a group of n blocks, produce a set of public verification parameters (PVPs) and IHT that are stored in TPA, transmits the file and some verification tags to CSP, and may delete its local copy.

II. *Periodic sampling audit:* By using an interactive proof protocol for repeatability, TPA issues a "random sampling" challenge to audit the integrity and availability of the outsourced data in terms of verification information stored in TPA.

III. *Audit for dynamic operations:* An AA, who holds a DO's secret key, holds can treats as the outsourced data and update the associated IHT stored in TPA[1]. The privacy of security key and the checking algorithm ensure that the storage server cannot cheat the AAs and forge the valid audit records.

III. PROPOSED ALGORITHMS

We define a cryptographic in audit scheme to our audit system in clouds. This scheme is constructed on the standard model of interactive proof system, which can ensure the confidentiality of secret data (zero-knowledge property) and un decidability of invalid tags (soundness property).

3.1. Algorithm for key generation:

keyGen(1^k): Given a bilinear map group system=(p,G,G_T,e) and a collosion resistant hash function $H_k(.)$,chooses a random $\alpha,\beta \in_R Z_P$ and computes $H_1=h^\alpha$ and $H_2=h^\beta \in G$. Thus, the secret key is $s^k=(\alpha,\beta)$ and the public key is pK=(g,h,H1,H2).

TagGen(sK,F): Splits the file F into n x s sectors $F=\{m_{i,j}\} \in Z_p^{n \times s}$,chooses s random $T_{1,\ldots}{}^{Ts} \in Z_p$ as the secret of this file and computes $u_i=g^{ri} \in G$ for $i \in [1,s]$ and$\xi^{(1)}=H_\xi$("Fn"),where $\xi=\sum_{i=1}^{s}$ Ti and Fn is the filename. Builds an index Hash table $\chi=\{x^i\}^n{}_{i=1}$ and fills the item $\chi^i=(B_i=I,V_i=1,R_i \in_R \{0,1\}^*)$ in χ for $i \in [1,n]$,then calculates its tag as $ð^i$<- $(\xi_i^{(2)})^\alpha,g^{\sum_{j=i}^{s}} T_j.m_{i,j}.\beta \in G$. Where $\xi_i^{(2)}= H_\xi^{(1)}(\chi_i)$ and $i \in [1,n]$. Finally, sets $u=(\xi^{\{1\}},u_1,\ldots.u_s)$ and outputs $\psi=(u,\chi)$ to TPA, and $ð=(ð_1,\ldots,ðn)$ to CSP.

Proof(CSP,TPA): This is a 3-move protocol between prover (CSP) and Verifier(TPA), as follows:

- Commitment(CSP-→TPA):CSP chooses a random $\gamma \in Z_p$and s random $\lambda_j \in_R Z_p$ for $j \in [1,s]$,and sends its commitment $C=(H_1{}',\Pi)$ to TPA, where $H_1{}'=H_1{}^\gamma$ and $\Pi \leftarrow e(\Pi_{j=1}^{s} u_j^{\lambda}{}_{j,H2});$
- Challenge(CSP←TPA): TPA chooses a random challenge set I of t indexes along with t random coefficients $v_i \in Z_p$. Let Q be the set of challenge index coefficient pairs$\{(i,v_i)\}_i \in$ I. TPA sends Q to CSP;
- Response(CSP→TPA): CSP calculates the response 0,μ as $ð' \leftarrow \Pi_{(I,vi) \in Q} \, {}^{ð}{}_{i}{}^{\gamma vi},\mu_j \leftarrow \lambda_j+\gamma.\sum_{(I,vi) \in Q} v_i.m_{i,j}$,where $\mu=\{\mu_j\}j \in [1,s]$. P sends $0=(ð',\mu)$ to TPA ; and
- Check: The verifier TPA checks whether the response is correct by

$$\Pi .e(ð^1.h)=e(\Pi_{(i,vi) \in Q}(\xi_i^{(2)v}{}_i,H_1{}').e(\Pi_{j=1}u_j^{\mu}{}_j,H_{2)}.$$

IV. PSEUDO CODE

4.1. Dynamic Operations Services

For updating records: Client Side

1. Client request to access a file from CSP.
2. CSP ask client for authentication just like login page.
3. Client authenticates CSP by his password
4. Verify password if correct send a file that he wants to access. Else move to step 2.
5. Client decrypts the file by applying decryption algorithm [12].
6. If client modify the file he will send file to CSP and TTP with a message like *Md* as (*F*',$,*M*) and *F* ' here M denotes for modification F ' for encrypted file, *Md* for message digest file [12] and $ for signature.

CSP Side

7. CSP check the signature for authenticity and compute the message digest to find encrypted file which is com-pare with encrypted file of another message.
8. If correct it will change previous file with this one and move to step12.
9. Else ask the client to follow the step 8.
10. CSP sends a same message to client after addition of his signature.
11. If file is same as previous one, drop this packet and move to step 1 or step 13.
12. Else ask CSP to follow step 11 again.
13. Exit ' F

4.2. RSA Coding

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.

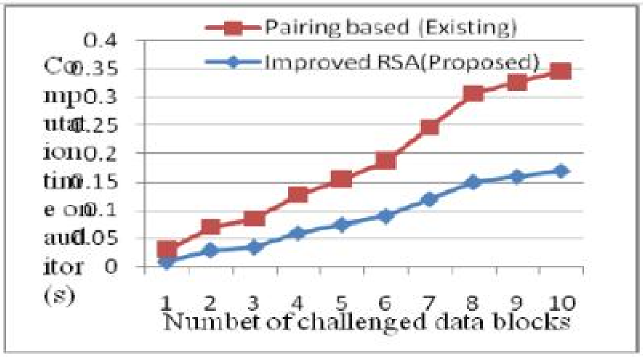
5. Now determine d as follows: d = e-1(mod Ø(n)) i.e., d is multiplicate inverse of e mod Ø(n).
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n). Encryption is the process of converting original plain text (data) into cipher text (data).
Steps:
1. Cloud service provider should give or transmit the Public-Key (n, e) to the user who want to store the data with him or her.
2. User data is now mapped to an integer by using an agreedUpon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text(data) C isC = me (mod n).
4. This cipher text or encrypted data is now stored with the CSP.

Decryption:
Decryption is the process of converting the cipher text (data) to the original plain text(data).
Steps:
1. The cloud user requests the Cloud service provider for the Data.
2. Cloud service provider verifies the authenticity of the user And gives the encrypted data i.e., C.
3. The Cloud user then decrypts the data by computing, m = Cd (mod n).
4. Once m is obtained, the user can get back the original data By reversing the padding scheme.

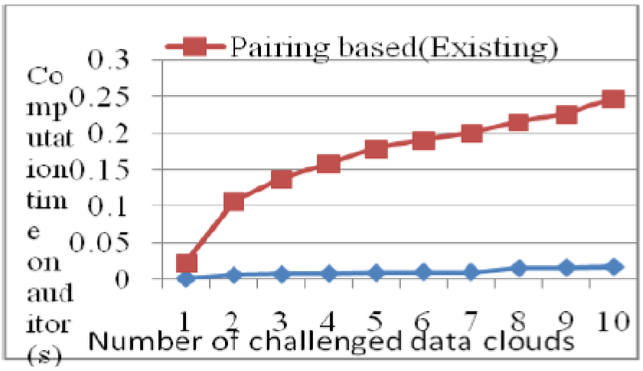
V. Implementation Results

The computation time of the auditor versus the number of data blocks, and the number of clouds, and the number of owners are calculated or compared as shown in Fig.4.a. shows the computation time of the auditor versus the number of challenged data blocks in the single cloud and single owner case. In this figure, the number of data blocks goes to, but it can illustrate the linear relationship between the computation cost of the auditor versus the challenged data size. From Fig. 4a, it is shown that the proposed scheme incurs less computation cost of the auditor than Zhu's IPDP scheme[4], when coping with large number of challenged data blocks. In real cloud storage systems, the data size is very large. The propoed scheme can apply the sampling auditing method to ensure the integrity of such large data

The sample size and the frequency are determined by the service-level agreement. From the simulation results, it is estimated that it requires 800 seconds to audit for 1-GByte data. However, the procedure abilities of the cloud server and the auditor are much more powerful than proposed simulation PC, so the computation time can be relatively small. Therefore, proposed auditing scheme is practical in large-scale cloud storage systems. Fig5.b. Define the cost computation of the auditor of the various cloud batches auditing scheme versus the number of challenged cloud storages.



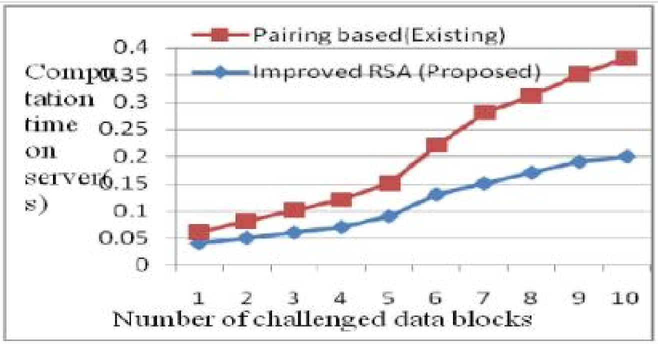
5.a: Single owner single cloud



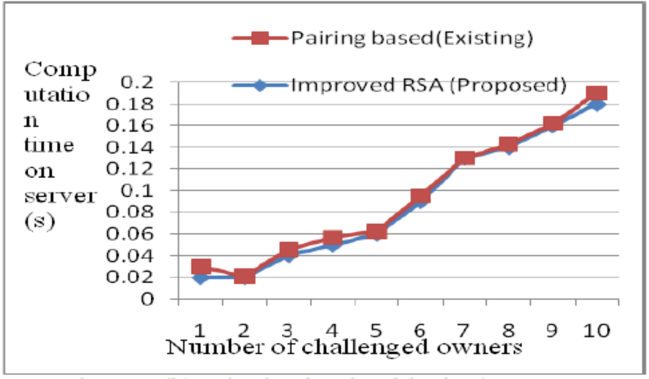
5.b: Single user 5block/cloud

Computation Cost of the Server

The computation cost of the server versus the number of data blocks in Fig. 5.2.a, and the number of data owners in Fig. 5.2.b, is compared. The Proposed scheme moves the computing loads of the auditing from the auditor to the server, such that it can greatly reduce the computation cost of the auditor.



4.2.a: Single owner single cloud



4.2.b:Single cloud, 5 blocks/cloud

VI. CONCLUSION AND FUTURE WORK

Finally in this paper, we presented a construction of Improving dynamic audit services for untrusted and outsourced storages. And also presented efficient methodologies for periodic sampling audit and E-mail verification to enhance the performance of TPAs and storage service providers. Our experiments have been shows the, our solution has a small, constant amount of overhead, which reduce the computation and communication costs.

REFERENCES.

1. Yan Zhu, Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, "Dynamic Audit Services For Outsourced Storages In Clouds" Hongxin Hu, Member, IEEE, Stephen S. Yau, Fellow, IEEE,Ho G. An, And Chang-Jun Ieee Transactions On Services Computing, Vol. 6, No. 2, April-June 2013.
2. Amazon Web Services, "Amazon S3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.
3. A. Juels And B.S. Kaliski Jr., "Pors: Proofs Of Retrievability For Large Files," Proc. Acm Conf. Computer And Communications Security (Ccs '07), Pp. 584-597, 2007.
4. Shingare Vidya Marshal "Secure Audit Service By Using Tpa For Data Integrity In Cloud System" International Jproposednal Of Innovative Technology And Exploring Engineering (Ijitee) Issn: 2278-3075, Volume-3, Issue-4, September
5. M. Mowbray, "The Fog Over The Grimpen Mire: Cloud Computing And The Law," Technical Report Hpl-2009-99, Hp Lab., 2009.
6. A.A. Yavuz And P. Ning, "Baf: An Efficient Publicly Verifiable Secure Audit Logging Scheme For Distributed Systems," Proc. Ann. Computer Security Applications Conf. (Acsac), Pp. 219-228, 2009.
7. 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," Proc. 14th Acm Conf. Computer And Comm. Security, Pp. 598-609, 2007.
8. G. Ateniese, R.D. Pietro, L.V. Mancini, And G. Tsudik, "Scalable And Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security And Privacy In Comm. Netowrks (Securecomm), Pp. 1-10, 2008.
9. C.C. Erway, A. Ku¨ Pc¸U¨ , C. Papamanthou, And R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th Acm Conf. Computer And Comm. Security, Pp. 213-222, 2009.