IJEEE

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Secure and Efficient Public Auditing Scheme for Privacy Preservation in Cloud Storage

Manjunath C[1], Asha R N[2]

[1]Student, Computer Science and Engineering, Don Bosco Institute of Technology, Karnataka, India
[2] Asst. prof, Computer Science and Engineering, Don Bosco Institute of Technology, Karnataka, India

Abstract: **Cloud storage enables user to remotely stores their data in cloud and enjoy the on-demand self-services and applications from a shared storage of configurable computing resources without creating online burden of local data storage and maintenance users should be able to use the cloud storage as if it is local without worrying about the integrity of the data. Thus enabling public auditability for cloud storage is very important so that user can request to third-party auditor TPA) to check and verify the integrity of the data. Privacy Stabilizing Public Auditing for Secure Cloud Storage a secure cloud storage system supporting privacy-preserving public auditing and enabling the TPA to perform audits for multiple users simultaneously and efficiently also support data dynamic operation. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.**

Key Words: **Data storage, public auditability, cloud computing, batch verification, Third party auditor**

1. INTROUCTION

Cloud computing has been envisioned as the next generation information technology (IT) architecture for enterprises due to its long list of unprecedented advantages like on-demand self-service network access location independent resource pooling rapid resource elasticity usage-based pricing and transference of risk [2]. As a disruptive technology with profound implications cloud computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data are being centralized or outsourced to the cloud. From users perspective including both individuals and IT enterprises storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits relief of the burden for storage management universal data access with location independence and avoidance of capital expenditure on hardware software and personnel maintenances [3].

While cloud computing makes these advantages more appealing than ever it also brings new and challenging Security threats toward users outsourced data. Since cloud service providers (CSP) are separate administrative entities data outsourcing is actually relinquishing user's ultimate control over the fate of their data.As a result the Correctness of the data in the cloud is being put at risk due to the following reasons.

- ➢ First is although the infrastructures under the cloud are more power full and reliable than the personal computing but still facing broad range of both internal and external threats for data integrity [4].
- ➢ Second there do exist various motivations for Cloud service provider to behave unfaithfully toward the cloud users regarding their outsourced data status.

To fully ensure the data integrity and save the cloud users computation resources as well as online burden it is of critical importance to enable public auditing service for cloud data storage so that users may resort to an independent third-party auditor (TPA) to audit the outsourced data when needed. The TPA who has expertise and capabilities that users do not can periodically check the integrity of all the data stored in the cloud on behalf of the users which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Public auditability allows an external party in addition to the user himself to verify the correctness of remotely stored data. However most of these schemes do not consider the privacy protection of users data against external auditors. TPA will performs the auditing process without demanding the local copy of the data thus reduces the computation and communication as compared to the straightforward data auditing approaches. By integrating the Holomorphic linear authentication with random masking our protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server (CS) during the efficient auditing process.

2. CLOUD STORAGE ARCHITECTURE

To enable privacy-preserving public auditing for cloud data storage the protocol design should achieve the following security and performance guarantees.

1. Public auditability: Public auditability allows third-party auditor to verify the correctness of the data without demanding for local copy of the data or additional online burden to the cloud users.
2. Storage correctness: Storage correctness ensures there is no cheating cloud server or fake servers exist that can pass third-party auditor audit process.

3. Privacy preserving: Privacy preserving ensures the leakage of the data to external and internal auditor while auditing process.

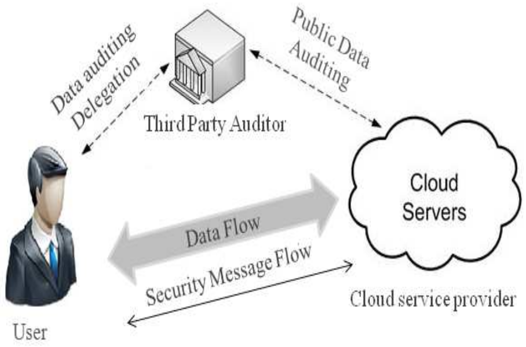


Fig 1: Cloud Data Storage service Architecture

4. Batch auditing: Batch auditing will ensure the auditing of multiple users simultaneously and efficiently.
5. Lightweight: Light weight allows TPA to perform auditing with minimum communication and computation overhead.

A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, and Verify Proof). KeyGen is a key generation algorithm that is run by the user to setup the scheme. SigGen is used by the user to generate verification metadata, which may consist of digital signatures. GenProof is run by the cloud server to generate a proof of data storage correctness, while VerifyProof is run by the TPA to audit the proof. Running a public auditing system consists of two phases.

I. Setup: The user initially initializes the public and secret parameters of the system by executing the key generation and preprocesses the data file using sig generation to generate the metadata. The user than stores the generated metadata and data file to cloud server and delete the local copy, user may alter the data file by expanding it or including additional metadata to be stored at server.

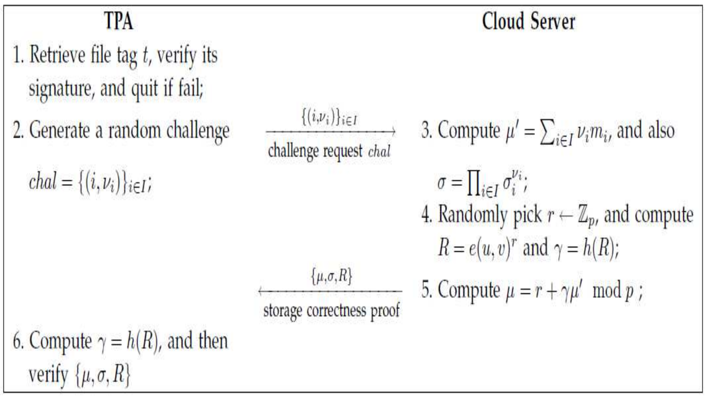
II. Audit: The third-party auditor issues an audit message or challenge to the cloud serer to make sure that the cloud retained the data file F properly at the time of audit process. The cloud server will response by executing Gen proof algorithm using data file f and metadata as input later TPA will verifies the response via Verify proof.

Our framework assumes that the TPA is stateless TPA does not need to maintain and update state between audits which is a desirable property especially in the public auditing system [7]. Note that it is easy to extend the framework above to capture a stateful auditing system essentially by splitting the verification metadata into two parts which are stored by the TPA and the cloud server respectively. Our design does not assume any additional property on the data file. If the user wants to have more error resilience he can first redundantly encodes the data file and then uses our system with the data that has error correcting codes integrated

3. THIRD PARTY AUDITOR

To achieve privacy-preserving public auditing we propose to uniquely integrate the homomorphic linear authenticator with random masking technique. In our protocol the linear combination of sampled blocks in the Servers response is masked with randomness generated by the server. With random masking the TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the users data content no matter how many linear combinations of the same set of file blocks can be collected. On the other hand the correctness validation of the block-authenticator pairs can still be carried out in a new way which will be shown shortly even with the presence of the randomness. Our design makes use of a public key-based HLA to equip the auditing protocol with public auditability. Specifically we use the HLA proposed [7] which is based on the short signature scheme proposed by Boneh Lynn and Shacham (hereinafter referred as BLS signature) [8]. There is no secret keying material or states for the TPA to keep or maintain between audits and the auditing protocol does not pose any potential online burden on users. This approach will ensures the privacy of the data contents during auditing process using holomorphic linear authentication with random masking technique to hide the data in linear combination of the data blocks.

TABLE 1
Privacy Preservation Auditing Protocol



TPA		Cloud Server
1. Retrieve file tag t, verify its signature, and quit if fail;		
2. Generate a random challenge $chal = \{(i,\nu_i)\}_{i\in I}$;	$\xrightarrow[\text{challenge request } chal]{\{(i,\nu_i)\}_{i\in I}}$	3. Compute $\mu' = \sum_{i\in I}\nu_i m_i$, and also $\sigma = \prod_{i\in I}\sigma_i^{\nu_i}$;
		4. Randomly pick $r \leftarrow \mathbb{Z}_p$, and compute $R = e(u,v)^r$ and $\gamma = h(R)$;
	$\xleftarrow[\text{storage correctness proof}]{\{\mu,\sigma,R\}}$	5. Compute $\mu = r + \gamma\mu' \mod p$;
6. Compute $\gamma = h(R)$, and then verify $\{\mu,\sigma,R\}$		

3.1 Challenge Token Creation

The main idea of challenge token creation is to verify the data integrity in cloud server when user store the data to the cloud server the data should not be modified during auditing process for that purpose the user will pre-computes certain number of short verification tokens on individual vector each token covering a random subset of data blocks that would be distributed to the different cloud servers. Later, when the user wants to make sure the storage correctness for the data in the cloud, he challenges the cloud servers with a set of randomly generated block indices. Upon receiving challenge each cloud server computes a short signature over the specified blocks and returns them to the user. The values of these signatures should match the corresponding tokens pre-computed by the user. Suppose if the user wants to challenge the cloud server t times to ensure the correctness of data storage, the user must pre-compute x verification tokens for indusial a challenge key kchal and a master permutation key K_{PRP}. To generate the ith token for server j, the user acts as follows:

A. Random challenge is generated and forwarded to TPA and precompiled key based on the data.
B. On receiving the request from the user TPA will forward challenge to the cloud server.
C. The cloud server will calculate the key for the requested data and forward to the TPA
D. TPA will compare the precompiled key and key from server if both the keys are same than data not modified and verify the data integrity.

After token generation, the user has the choice of either keeping the pre-computed tokens locally or storing them in encrypted form on the cloud servers.

3.2 Correctness Verification

The response values from the cloud serve for each challenge not only determines the correctness of the distributed data but also contains information regarding the data error. The procedure of the ith challenge-response for verification over the d servers is described as follows:

A. The user will forwards permutation key to each server.
B. The server will aggregate those k rows specified by permutation key into a linear combination.
C. Upon receiving linear combination from all the servers the user choose the random value.
D. Then the user verifies whether the received values remain a valid codeword determined by secret matrix P.

4. BATCH AUDITING

With the establishment of privacy preserving public auditing the TPA may concurrently handle multiple auditing upon different users delegation. The individual auditing of these tasks for the TPA can be tedious and very inefficient. Given K auditing delegations on K distinct data files from K different users it is more advantageous for the TPA to batch these multiple tasks together and audit at one time. Keeping this natural demand in mind we slightly modify the protocol in a single user case and achieve the aggregation of K verification equations into a single one

.

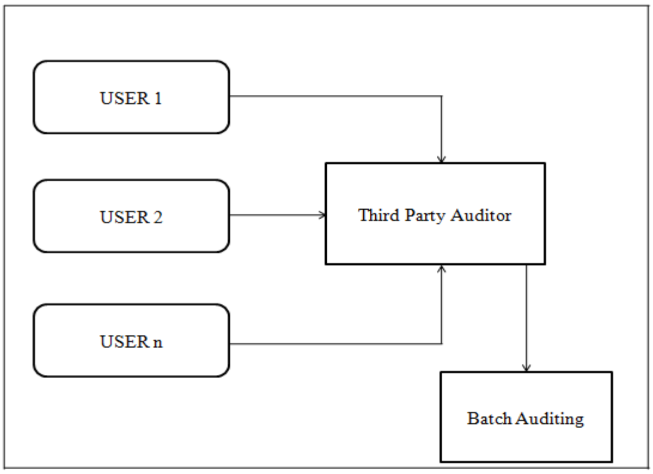
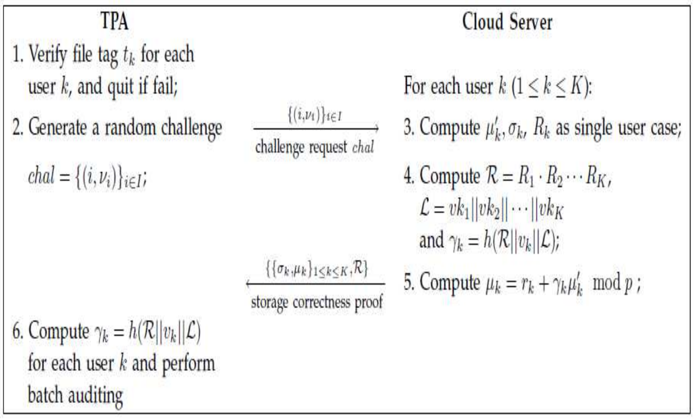


Fig 2: Batch Auditing

As a result a secure batch auditing protocol for simultaneous auditing of multiple tasks is obtained. As a result a secure batch auditing protocol for simultaneous auditing of multiple tasks is obtained.

Table 2
Batching Auditing Protocol



TPA		Cloud Server
1. Verify file tag t_k for each user k, and quit if fail;		For each user k ($1 \leq k \leq K$):
2. Generate a random challenge $chal = \{(i,\nu_i)\}_{i \in I}$;	$\xrightarrow[\text{challenge request } chal]{\{(i,\nu_i)\}_{i\in I}}$	3. Compute μ'_k, σ_k, R_k as single user case;
		4. Compute $\mathcal{R} = R_1 \cdot R_2 \cdots R_K$, $\mathcal{L} = vk_1 \| vk_2 \| \cdots \| vk_K$ and $\gamma_k = h(\mathcal{R} \| v_k \| \mathcal{L})$;
	$\xleftarrow[\text{storage correctness proof}]{\{\{\sigma_k,\mu_k\}_{1\leq k\leq K},\mathcal{R}\}}$	5. Compute $\mu_k = r_k + \gamma_k \mu'_k \mod p$;
6. Compute $\gamma_k = h(\mathcal{R} \| v_k \| \mathcal{L})$ for each user k and perform batch auditing		

5. DATA DYNAMIC OPERATION

In cloud computing outsourced data might not only be accessed but also updated frequently by users for various Applications purpose [9],[10],[11].supporting data dynamics for privacy-preserving public auditing is also of paramount importance. Now we show how to build upon the existing work [5] and adapt our main scheme to support data dynamics including block level operations of modification, deletion, and insertion. Since data do not reside at users local site but at cloud service providers address domain supporting dynamic data operation can be quite challenging. On the one hand cloud service provider needs to process the data dynamics request without knowing the secret keying material. On the other hand users need to ensure that the dynamic data operation request has been faithfully processed by cloud service provider.

A. Update Operation: In cloud storage sometimes the user need to alter the data blocks stored in the cloud data storage, user can modify the data file without downloading the file, Modifying directly in loud server itself by eliminating the online burden ttis process is called as the update operation.

B. Delete Operation: The data stored in cloud server sometimes need to delete. The delete operation we are considering is a general one in which user replaces the data block with zero or some special reserved data symbol. From this point of view the delete operation is actually a special case of the data update operation where the original data blocks can be replaced with zeros or some predetermined special blocks.

C. Append Operation: User may want to increase the size of the data stored in cloud server by adding data blocks at the end of the data file which we refer as data append operation, most frequent append operation in cloud data storage is bulk append in which the user needs to upload a large number of blocks (not a single block) at one time.

We create a cloud environment where user TPA and cloud server are connected each other. In public auditing system the correctness of the data is checked by keyGen, sigGen, Gen proof and verify proof algorithms Homomorphism authenticator with random masking is used to achieve privacy preserving auditing scheme. The technique of bi-linear aggregate signature is used to achieve batch auditing. In cloud the data does not remain Static. We enhance the system with explicit dynamic operations in data blocks

6. ALGORITHMS

1. Key Generation: Run by client
Input: None
Output: public key rpk, secrete key rsk, generator g.

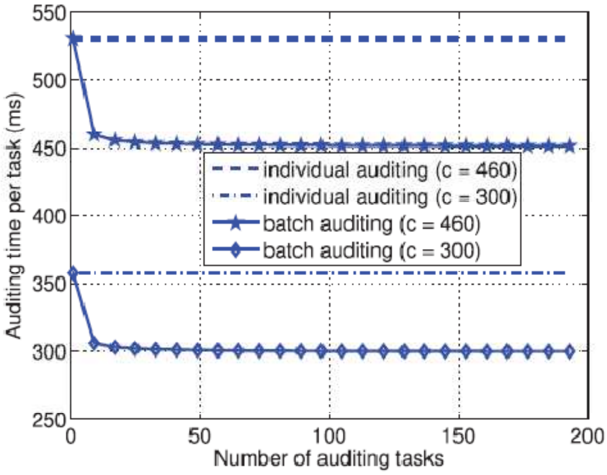
2. SignatureGeneration: Run by client
Input: File Blocks F, secret key rsk, generator g.
Output: set of signature Φ.

3. GenerateProof: Run by cloud storage server
Input: Subset of file blocks mi, coefficient i
Output: Proof P

4. VerifyProof: Run by TPA
Input: Proof P Output:
Boolean value {TRUE, FALSE}

7. RESULTS

Comparison on auditing time between individual and batch auditing: Per task auditing time denotes the total auditing time divided by the number of tasks.



8. CONCLUSION

A privacy-preserving public auditing system for data storage security in cloud computing utilize the holomorphic linear authenticator and random masking to guarantee that the Third-party auditor would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Analysis shows that our schemes are provably secure and highly efficient.

REFERENCES

[1] C.Wang, Q.Wang, K.Ren, and W.Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Feb 2013.

[2] P.Mell and T.Grance "Draft NIST working Definition of Cloud Computing" June 2009.

[3] 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.

[4] Cloud Security Alliance, "Top Threats to Cloud Comp-uting "http://www.cloudsecurityalliance.org,2010.

[5] 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.

[6] 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.

[7] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008.

[8] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.

[9] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10, 2008.

[10] C. Wang, Q. Wang, K. Ren and W. Lou "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Service Computing vol. 5 no. 2, 220-232, Apr.-June 2012.

[11] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.