www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12368-12373

Privacy Preserving Public Auditing Mechanism For Shared Data In Cloud Computing Environment With Dynamic Groups

Mrs. Suvarna L. kattimani[1], Mr. Aniruddha A. Atwadkar[2], Dr Suvarna Nandyal[3]

[1]Assistant Professor, Dept of CSE, BLDEA'S Dr Halkatti College of Engineering & Technology, vijayapur, karnataka,(India)
[2]PG Scholar, Dept of CSE, BLDEA'S Dr Halkatti College of Engineering & Technology, vijayapur, karnataka,(India)
[3]Professor, HOD Dept of CSE, P.D.A College Of Engineering, Gulbarga,karnataka, (India)

Abstract

In Cloud environment, clients can remotely store their information and appreciate the on-interest high caliber applications and administrations. The respectability of cloud information is liable to distrust because of the presence of equipment/programming disappointments and human lapses. A few components have been intended to permit both information proprietors and open verifiers to proficiently review cloud information uprightness without recovering the whole information from the cloud server. Nonetheless, open reviewing on the uprightness of imparted information to these current instruments will open evaluating on shared information put away in the cloud that endeavour ring signature to figure confirmation metadata expected to review the rightness of shared data.so that an outsider evaluator (TPA) has the capacity check the honesty of shared information for clients without recovering the whole information. In the interim, the character of the user on every block of data in shared information is kept private from the TPA likewise ready to perform numerous examining undertakings at the same time as opposed to checking them one by one.

Keywords: Cloud environment, shared data, public auditing, privacy preserving, TPA.

1. INTRODUCTION

Cloud administration supplier's deal with a venture class foundation that offers an adaptable, secure and dependable environment for clients, at a much lower minimal cost because of the sharing way of assets. It is schedule for clients to utilize distributed storage administrations to share information with others in a group, as information sharing turns into a standard element in most distributed storage offerings.

The honesty of information in distributed storage, notwithstanding, is subject to distrust and investigation, as information put away in an untrusted cloud can without much of a stretch be lost or defiled, due to equipment disappointments and human mistakes. To ensure the honesty of cloud information, it is best to perform open inspecting by presenting an outsider examiner (TPA), who offers its inspecting administration with all the more capable communication and correspondence capacities than general clients.

As of late, numerous components have been proposed to permit an information proprietor itself as well as an open verifier to effectively perform respectability checking without downloading the whole information from the cloud, which is alluded to as open examining. In these instruments, information is isolated into numerous little blocks of data, where every piece is autonomously signed by the proprietor and an irregular blend of the considerable number of pieces rather than the entire information is recovered for trustworthiness checking .An open verifier could be an information client (e.g. researcher)who might want to use the proprietor's information by means of the cloud or an outsider evaluator (TPA) who can give master uprightness checking administrations. Existing open examining instruments can really be reached out to confirm shared information integrity on dynamic groups.

However, the new significant mechanism addresses the security for safeguarding the protection of proprietor from the outside verifier (TPA), this is only done on the static groups. The verifier has prior information about the groups to be verified. Having prior knowledge about groups to be audited to the untrusted auditor may cause lead security break of information.

Also, extend this mechanism to support dynamic groups and batch auditing of dynamic groups, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks. Auditing on dynamic groups is necessary to secure the identity of user and information as the auditor has no prior information of groups to be audited.

2. SYSTEM MODEL

Fig.1. Proprietor, third party auditor and cloud server in System model

This paper involves three parties, the cloud server, the outside verifier (TPA) and proprietors. There are two types of proprietors in a group the original user and a various other proprietors. We consider how to review the uprightness of imparted information in the cloud with dynamic groups. It implies the group is not predefined before shared information is made in the cloud and the enrolment of another proprietor can be included into the group and a current group and an existing group member can be revoked during data sharing while still preserving identity privacy. The original proprietor is responsible for deciding who is able to share her data before outsourcing data to the cloud.

At the point when a proprietor (either the original proprietor or a group proprietor) wishes to check the respectability of shared information, she first sends an examining request to the TPA. In the wake of accepting the inspecting demand, the TPA produces an evaluating message to the cloud server, and recovers a reviewing evidence of shared information from the cloud server. At that point the TPA confirms the accuracy of the evaluating confirmation. At long last, the TPA sends an auditing report to the proprietor.

3. DESIGN OBJECTIVES

This mechanism is designed to achieve following properties

a. Public Auditing

The outsider verifier has the capacity freely verify the respectability of shared information for a group of proprietor without recovering the whole information.

b. Correctness

The outsider verifier has the capacity effectively identify whether there is any erroneous block in shared information.

c. Unforgeability

Just a proprietor in the gathering can create substantial confirmation data on shared information.

d. Identity Privacy

During auditing, the TPA cannot distinguish the identity of the designer on each block in shared data.

e. Auditing on dynamic groups

Auditing process takes place with the help of outsider verifier, where he/she has no prior idea of group before auditing. Insertion, deletion and modification operation are done on the blocks.

4. METHODOLOGY

4.1 Ring signature scheme

4.1.1 Overview

The configuration of new homomorphic authenticable signature (HARS) scheme, which is extended from a classic ring signature scheme. The ring signatures generated by HARS are not only able to preserve identity privacy but also able to support block less verifiability. We will demonstrate to fabricate the protection safeguarding open evaluating component for shared information in the cloud in light of this new ring signature scheme.

4.1.2 Construction of HARS

HARS consists of three algorithms

i. KeyGen

Every proprietor in the group creates his/her open key and private key.

ii. RingSign

A proprietor in the group has the capacity create a signature on identifier is a string that can recognize the relating block from others.

iii. RingVerify.

A verifier has the capacity check whether a given piece is signed by a group member.

4.2 Auditing Mechanism

4.2.1 Overview

Utilizing HARS and its properties, we now develop component, a privacy preserving public auditing mechanism for shared data in the cloud. The verifier can confirm the honesty of shared information without recovering the whole information. Then, the identity of the endorser on every piece in shared information is kept private from people in general verifier during auditing.

4.2.2 Construction of auditing mechanism

Construction of auditing mechanism consists of five algorithms

i. KeyGen

Proprietor create their own open/private key to register ring signature on each block.

ii. SigGen

A proprietor (either the original proprietor or a group proprietor) is able to compute ring signatures on blocks in shared data.

iii. Modify

Each proprietor in the group is able to perform an insert, delete or update operation on a block, and compute the new ring signature on this new block.

iv. ProofGen

It is worked by the outside verifier (TPA) and the cloud server together to produce a proof of ownership of shared information.

v. ProofVerify

The outside verifier (TPA) checks the confirmation and sends an examining report to the proprietor.

4.3 Security analysis of auditing mechanism

We discuss security properties of auditing mechanism, which includes its correctness, unforgeability, identity privacy and data privacy.

Theorem: A public verifier is able to correctly audit the integrity of shared data under public auditing mechanism.

Proof: According to the description of **ProofVerify, a** public verifier believes the integrity of shared data is correct if Equation holds. So, the correctness of our scheme can be proved by verifying the correctness of Equation. Based on properties of bilinear maps, the right-hand side (RHS) of Equation can be expanded as follows

$$
\begin{aligned}
RHS &= \left(\prod_{i=1}^{d} e\Big(\prod_{j\in\mathcal{J}} \sigma_{j,i}^{y_j}, w_i\Big)\right) \cdot e\Big(\prod_{l=1}^{k} \lambda_l^{h(\lambda_l)}, g_2\Big) \\
&= \left(\prod_{j\in\mathcal{J}} \Big(\prod_{i=1}^{d} e(\sigma_{j,i}, w_i)^{y_j}\Big)\right) \cdot e\Big(\prod_{l=1}^{k} \eta_l^{\gamma_l h(\lambda_l)}, g_2\Big) \\
&= \left(\prod_{j\in\mathcal{J}} e(\beta_j, g_2)^{y_j}\right) \cdot e\Big(\prod_{l=1}^{k} \eta_l^{\gamma_l h(\lambda_l)}, g_2\Big) \\
&= e\Big(\prod_{j\in\mathcal{J}} \big(H_1(id_j)\prod_{l=1}^{k} \eta_l^{m_{j,l}}\big)^{y_j}, g_2\Big) \cdot e\Big(\prod_{l=1}^{k} \eta_l^{\gamma_l h(\lambda_l)}, g_2\Big) \\
&= e\Big(\prod_{j\in\mathcal{J}} H_1(id_j)^{y_j} \cdot \prod_{l=1}^{k} \eta_l^{\sum_{j\in\mathcal{J}} m_{j,l} y_j} \cdot \prod_{l=1}^{k} \eta_l^{\gamma_l h(\lambda_l)}, g_2\Big) \\
&= e\Big(\prod_{j\in\mathcal{J}} H_1(id_j)^{y_j} \cdot \prod_{l=1}^{k} \eta_l^{\mu_l}, g_2\Big).
\end{aligned}
$$

4.4 Construction of dynamic groups

We now examine the situation of dynamic groups under our proposed system. In this process a new proprietor can be included in the group or existing proprietor can be revoked from the group, then this group is considered as dynamic group. To support dynamic groups while yet permitting the outside verifier to perform open evaluating, all the ring signatures on shared information should be re-registered with the signers private key and other proprietors public key when the enrolment of the group is changed.

4.4.1 System Architecture for Dynamic group

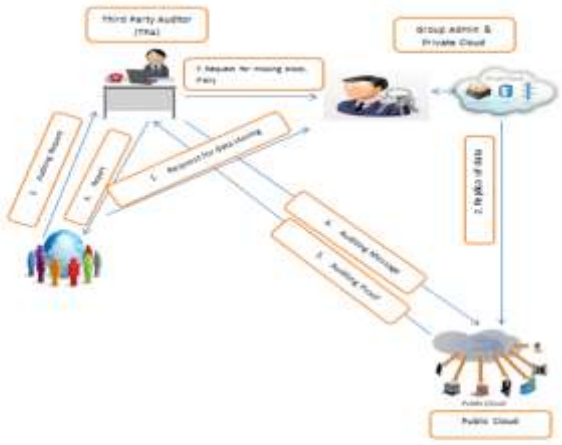

Fig.2. Proprietor, third party auditor and cloud server, group admin in System architecture for dynamic groups.

The proposed system consists of four modules, where the proprietor request owner of cloud for data to store the information and use the resource of respective cloud. Proprietor can then request the outside verifier to audit the particular information. The outside verifier sends auditing message to public cloud server and in return server sends back the auditing proof. After examining the information, the examined result is sent back to proprietor.

During the auditing process if there is any error in the information, then the outside verifier requests the owner of the private cloud for ssing or erroneous block of data.

4.4.2 Operations on dynamic groups

There are three operations can be performed during verification of blocks of information, they are as follows

i. Insert
ii. Delete
iii. Modify

Fig.3a shows insertion operation, a block can be added to existing block of information. The information will not be affected except the index value of the block.

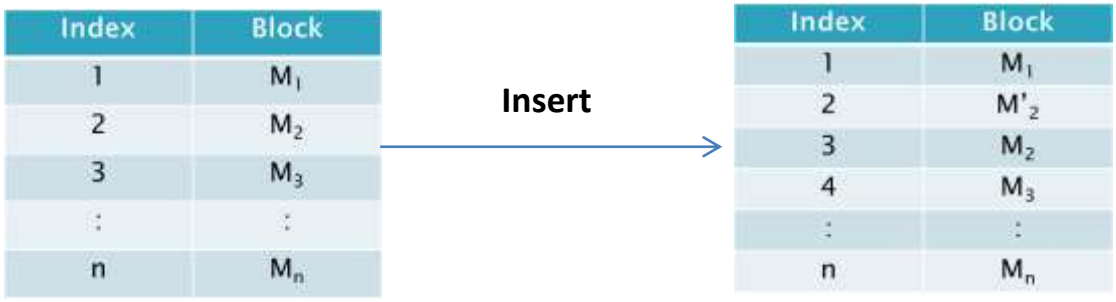

Fig.3a. Change of index after inserting block

Fig.3b shows deletion operation, it is similar to insert operation. A block can be deleted from existing block of information. The information will not be affected except the index value of the block.

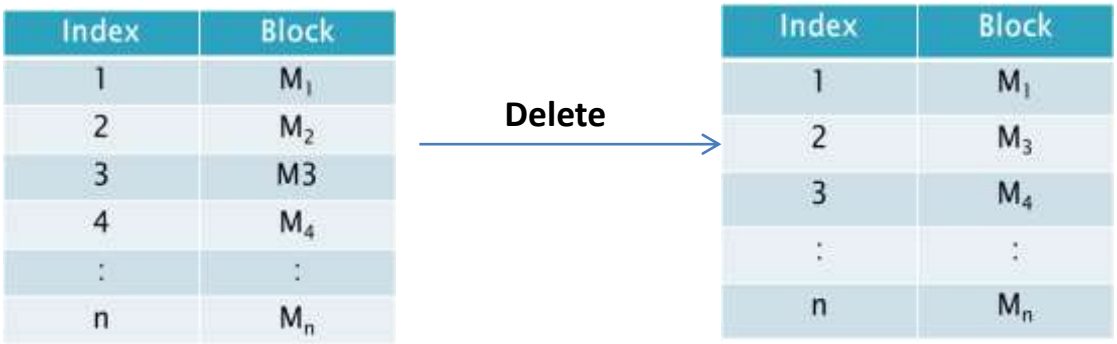

Fig.3b. Change of index after deleting block

Modify operation includes both insert and delete operations which is performed on the block of data, during the process of auditing by the outside verifier.

5. CONCLUSION AND FUTURE WORK

In this paper, we purpose privacy preserving – public auditing mechanism of shared information with dynamic groups in cloud. The outside verifier is able to verify the blocks of information by utilizing the homomorphic ring structure. The signature of proprietor is kept private, yet the outside verifier can examine the blocks for checking the uprightness of the information.

The interesting issues we will keep on considering for our future work. One of them is traceability, which implies the capacity for the group supervisor (i.e., the original proprietor) to uncover the identity of the signer in light of confirmation metadata in some extraordinary circumstances.

6. REFERENCES

[1] 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, "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in *Proc. ACM Conference on Computer and Communications Security(CCS)*, 2007, pp. 598–610.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, 2010, pp. 525–533.

[4] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer- Verlag, 2001, pp. 552 565.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in *Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Springer-Verlag, 2003, pp. 416–432.

[6] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer-Verlag, 2008, pp. 90–107.

[7] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in *Proc. ACM Symposium on Applied Computing (SAC)*, 2011, pp. 1550–1557.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, 2010, pp. 534–542.

[9] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer-Verlag, 2001, pp. 514–532.

[10] D. Boneh and D. M. Freeman, "Homomorphic Signatures for Polynomial Functions," in *Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Springer-Verlag, 2011, pp. 149–168.

[11] L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen,"Practical Short Signature Batch Verification," in *Proc. RSA Conference, the Cryptographers' Track (CT-RSA)*. Springer-Verlag, 2009,pp. 309–324.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine Grained Access Control of Encrypted Data," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2006, pp. 89–98.

[13] A. Juels and B. S. Kaliski, "PORs: Proofs pf Retrievability for Large Files," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2007, pp. 584–597.

[14] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in *Proc. International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2008.

[15] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2009, pp. 213–222.

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in *Proc. IEEE/ACM International Workshop on Quality of Service (IWQoS)*, 2009, pp. 1–9.

[17] B. Chen, R. Curtmola, G. Ateniese, and RBurns, "Remote Data Checking for Network Coding-based Distributed Stroage Systems,"in *Proc. ACM Cloud Computing Security Workshop (CCSW)*,2010, pp. 31–42.

[18] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes based Secure and Reliable Cloud Storage Service," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*,2012.

[19] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of Ownership in Remote Storage Systems," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2011, pp. 491–500.

[20] Q. Zheng and S. Xu, "Secure and Efficient Proof of Storage with Deduplication," in *Proc. ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2012.