ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Integrity Preservation and Identity Privacy of Shared Data in Untrusted Clouds

Lima L G[1], Swapna H[2]

M. Tech Student, Marian Engineering College, Trivandrum, Kerala, India[1]

Asst. Professor, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India[2]

ABSTRACT: With cloud storage services, it is a platform for data to be not only stored but also shared across multiple users. Public auditing is an important factor while considering shared data, but the identity privacy remains to be a challenge. In this work, the integrity preservation and identity privacy of shared data in the cloud is taken in to consideration. Here utilize a ring signature to verify the integrity of shared data. Concept of third party auditor (TPA) is introduced, who is able to verify the integrity of data without retrieving the entire file. Identity of each signer is kept private from TPA. Experimental analysis shows the effectiveness and efficiency of proposed mechanism.

KEYWORDS: Cloud computing, public auditing, Identity privacy, Shared data, Integrity.

I. INTRODUCTION

Cloud computing is a recent advancement technology where in IT infrastructure and its applications are provided many services. Cloud service providers manage the infrastructure of cloud and offer a secure, scalable and reliable platform for users at a lower cost. Data sharing is one of the standard features of most cloud storage offerings such as Google Docs and Drop box[1].

All the data processing task of cloud services is handled by a large number of distributed computers, end users get access to the computer and storage system through network. So there are so many security issues associated with the cloud storage since network is subject to problems [2], [5]. Main challenges are how cloud provider will provides authentication and integrity over user's data? How cloud providers protect data from attackers? The data stored in an untrusted cloud can sometimes easily be lost or corrupted due to manual errors, and hardware failures [7]. So it is necessary to protect the integrity of data. In this paper, concept of ring signature is used within a group of user's to achieve the integrity of shared data in clouds.

II. RELATED WORK

Earlier studies related to public auditing of shared data is based on PDP [provable data possession] mechanism [3],[8] perform public auditing by only checking the correctness of data stored in an untrusted server, but there were chances to lost or corrupt the data. Second public auditing mechanisms introduced by C.Wang [6] perform auditing but the entire content of data disclosed to the third party auditor. This was a challenge that disclosure of data to third party affects confidentiality of data.

III. SYSTEM MODEL

Sharing data among multiple users is one of the most engaging features recently motivates cloud services. Main contribution is to preserve identity privacy from third party auditor and to achieve integrity, because identities of particular signer reveal the higher valuable target than other signers. Whenever the users want to perform dynamic operation such as insert, delete, update each user in the group should provide their private key in a ring signature pattern only after providing key by each user the data successively. Similarly, the retrieval of data from the cloud storage system also needs each member's private key. Ring signature manner is used here in order to save time taken for accessing file by each member. There are three parties mainly including in this work .Cloud server, Users and Third

DOI: 10.15680/IJIRCCE.2016. 0405233

party auditor. Here cloud server provides a platform for storing the user's data. Third party auditor able to check the integrity of shared data in the cloud server. Two types of users, the original user and a group of users both are members of the group. Group members have only the permission to access the data created by original user. Each members of the group are assigned in a ring like manner and the priority of providing key is assigned earlier. This arrangement can be performed in any way like members age, qualification etc.

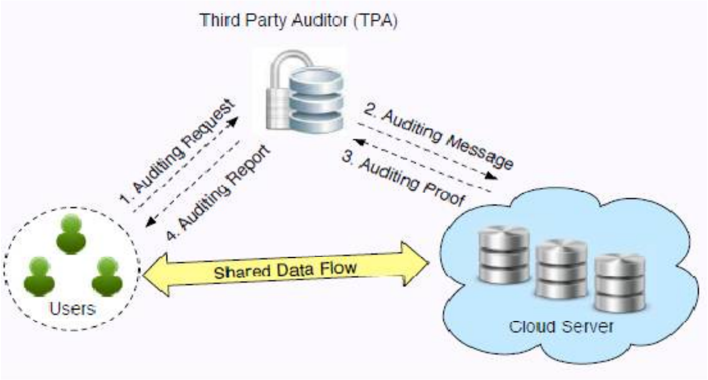

Fig.1. System architecture

IV. PROPOSED SYSTEM

Earlier works only perform public auditing of shared data in the cloud using static group only. That means the members of the group are predefined .In this work the ring signature perform public auditing for both static and dynamic group .Whenever a group member is deleted from the group the corresponding person will be eliminated from the ring and the person below the deleted member assigned to that position. If a new member is introduced in the group, the ring is again rearranged based on their priority. All these tasks are performed by the original group member like admin.

V. PERFORMANCE ANALYSIS

Performance analysis has done through measuring the performance of signature generation. The generation time of a ring signature on a file is determined by the number of group members. The generation time of a ring is linearly increases with the size of the group. Efficiency has measured through calculating the auditing time taken by TPA and cloud server.

VI. CONCLUSION AND FUTURE WORK

In this paper, a new mechanism for public auditing for shared data is introduced which preserve the identity privacy and integrity of shared data. Here used a ring signature to verify the integrity of shared data. The TPA is able to audit the integrity of data without retrieving entire file. Identity privacy achieved by keeping the signers identity. Future work will base on how to efficiently support batch auditing.

REFERENCES

1. Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE," Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE 5th International Conference on Cloud Computing Year 2014.
2. 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.
3. 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.

4. 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.
5. 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.
6. 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.
7. 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.
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.

BIOGRAPHY

Lima L G is a M.Tech student in Computer science Department, Marian Engineering college, Kerala university.

Swapna H is an Asst.Professor, in Computer science Department, Marian Engineering College, Trivandrum, Kerala, India.

DOI: 10.15680/IJIRCCE.2016. 0405233