Light Weight Secure Auditing Scheme for Shared Data in Cloud Storage

Naveena P[1] , Soundarya R S[2], Asst. Prof. Mohanapriya K A[3]
1,2 Student Department of Computer Science and Engineering
3 Assistant Professor in Computer Science and Engineering
Velalar College of Engineering and Technology, Thindal, Erode-12.

Abstract **A cloud platform providers users with shared data storage services, Users can remotely store the data to the cloud and realize the data sharing with others. An audit scheme that enables group members to modify data conducts the integrity and verification of the shared data. This results in the complex calculations for the group members who shared the data in the cloud .It ignores the security risks between the group members and the agents. A lightweight secure auditing scheme can be used to protect the shared data. To introduce an effective Third Party Auditor, the auditing process of the shared data is easy towards user privacy and introduce no additional burden to users in the cloud storage. The third party auditor can be used to secure the data on behalf of the users.It supports the privacy preserving public auditing.The security analysis and the performance evaluation proves that the proposed system is highly secured and efficient to trust in the cloud service platform.**

Keywords – Shared data, Auditing scheme, Security, Cloud service Providers.

1.INTRODUCTION

Cloud computing is a new computing method that was introduced after peer-to-peer computing, grid computing, utility computing and distributed computing. It is the delivery of on-demand computing services from applications to storage and processing power. The main concept of cloud computing is to rent resources, application hosting and service outsourcing[1].With the enormous growth of data, it is too difficult to store and maintain the sheer amount of data locally. It is becoming the default options for many applications. Many organizations and individuals users are willing to store the data in the cloud. Cloud storage systems give users mass storage capacity at the relatively low costs and provide a platform for sharing data between users. But the data in the cloud may be corrupted or lost due to the inevitable software bugs, hardware failures and human errors in the cloud. Highly centralized computing resources means cloud storage faces severe security challenges.

According to the survey done by Gartner in 2009,70% of CEOs refused to use the cloud computing on a large scale due to the problem in privacy in the cloud data.In March 2011, Google Gmail failed, which caused data loss to approximately 150,000 users. Amazon's enormous EC2 cloud service crashed, permanently destroying some users' data[2].Thus the secure data storage in the cloud has blocked the large-scale use of cloud computing in the IT field.

2.BACKGROUND

In 2007,Ateniese et.al proposed a Provable Data Possession model which can verify the integrity of cloud data without retrieving all the data[3].Juels et.al. proposed the Proofs of Retrievabiity scheme which enables backup or archive services to produce proof that data can be retrieved by the verifier.Ateniese et.al implemented a PDP scheme that supports dynamic operations which means that the data uploader has full control over any operation performed on the cloud data,including block deletion,modification and insertion[4].

In 2016,Yang et.al. proposed a BLS based signature scheme supporting management in the group[5]. Jiang et.al. proposed data integrity based on vector commitment technique which is resistant to collusion attacks of a cloud service provider and a group member[6].By combining proxy cryptography with the encryption technique, in 2017 Luo et.al. proposed a scheme with secure user revocation[7].

Huang et.al. realized efficient key distribution within groups based on the logical hierarachy tree to protect the identity privacy of the group members[8].He proposed a certificateless audit scheme by eliminating key escrow,which further improved the user's privacy security[9].

In order to verify the integrity of the shared data stored in the cloud, the group members need to block the data and then calculate data authentication labels for each blocks.Then the group members upload the shared data along with the corresponding authentication labels to the cloud. The integrity verification of the shared data relies on the correctness of these data authentication labels. The cost of calculating the authentication label is generally great because the formula requires a large number of exponentiations. For example, Consider the block size is 2 KB,the authentication label generation overhead for a 10 GB is nearly 18 hours to upload the data in the cloud.

It is necessary to propose a lightweight auditing scheme to reduce the resource utilization of the users.Li et.al. proposed a new cloud storage auditing scheme with a cloud audit server and cloud storage server[10].The cloud server generates authentication labels for users before uploading them to the cloud server.This method can reduce the user's computation overhead.But it will fully reveal the user's

private key and the user's data to the cloud audit server.This may result in the malicious cloud service providers to the verification without storing the data of the users in the data. To build an audit scheme for cloud storage,thereby reducing the time that is required to generate authentication labels but increasing time to verify the integrity of the cloud data.

Shen et.al. proposed a lightweight audit scheme by introducing the Third Party Medium which is used to replace the group members with the generation of authentication labels[11].This scheme protects the data privacy and the identity privacy of group members but it doesnot consider the illegal access of the shared data in the cloud.So the illegal group member can modify the data in the cloud.

3.PROPOSED SYSTEM

To fully certify the information integrity and save the cloud users' computation resources additionally as on-line burden, it's of important importance to change public auditing service for cloud information storage, so as that users could resort to AN freelance third party auditor (TPA) to audit the outsourced information once required. The TPA, World Health Organization has experience and capabilities that users do not , will sporadically check the integrity of all the data keep at intervals the cloud on behalf of the users, that provides additional easier and reasonable way for the users to form positive their storage correctness at intervals the cloud.

Moreover, in addition to help users to guage the danger of their signed cloud information services, the audit result from TPA would even be helpful for the cloud service suppliers to boost their cloud based mostly service platform, and even serve for freelance arbitration functions. In a word, sanctioning public auditing services can play an important role for this aborning cloud economy to become absolutely established, wherever users can would like ways in which to assess risk and gain trust within the cloud.
It motivates the general public auditing system of information storage security in Cloud Computing and supply a privacy-preserving auditing protocol. Our theme allows an external auditor to audit user's cloud information while not learning the data content. To the only of our information, our theme is that the primary to support scalable and economical privacy conserving public storage auditing in Cloud. Specifically, our theme achieves batch auditing wherever multiple delegated auditing tasks from completely different users usually performed at the same time by the TPA throughout a privacy-preserving manner. this technique proves the securities and justifies the performance of our projected schemes through concrete experiments and comparisons with the progressive. Ensures the cluster members needn't to perform time overwhelming calculations.Group members will realize the criminal members and take away them to attain security management of teams.

3.1 SYSTEM ARCHITECTURE

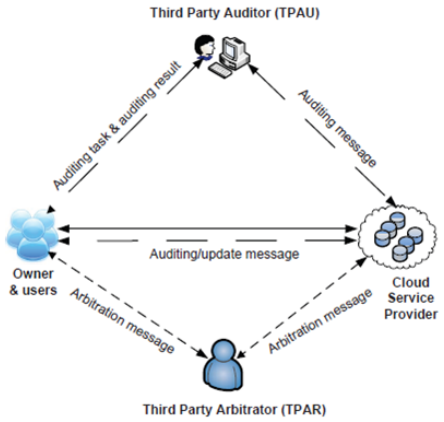

FIGURE 3.1A

4.MODULES DESCRIPTION

4.1 CLOUD STORAGE

Data outsourcing to cloud storage servers is raising trend among several companies and users as a result of its economic benefits. This primarily means the owner (client) of information| moves its data to a 3rd party cloud storage server that is meant to - presumptively for a fee - dependably store the info with it and supply it back to the owner whenever needed.

4.2 SIMPLY ARCHIVES

This downside tries to get and verify an indication that informationthat's hold on by a user at remote data storage within the cloud (called cloud storage archives or just archives) isn't changed by the archive and thereby the integrity of the info is assured. Cloud archive isn't cheating the owner, if cheating, during this context, means the storage archive may delete a number of the info or could modify a number of the info. whereas developing proofs for information possession at untrusted cloud storage servers we have a tendency to an usually restricted by the resources at the cloud server also as at the consumer.

4.3 SENTINELS

Only one key are often used no matter the dimensions of the file or the quantity of files whose retrievability it needs to verify. conjointly the archive must access solely atiny low portion of the file F not like within the key-has theme that needed the archive to method the whole file F for every protocol verification. If the prover has changed or deleted a considerable portion of F, then with high chance it'll even have suppressed variety of sentinels.

4.4 VERIFICATION PHASE

The protagonist before storing the file at the archive, preprocesses the file and appends some Meta information to the file and stores at the archive. At the time of verification the protagonist uses this Meta information to verify the integrity of the info. it's necessary to notice that our proof of knowledge integrity protocol simply checks the integrity of knowledge i.e. if the info has been illicitly changed or deleted. It doesn't stop the archive from

modifying the information of the shared data in the cloud storage.

5.CONCLUSION

We've worked to facilitate the shopper in obtaining a signal of integrity of the info that he desires to store within the cloud storage servers with clean minimum prices and efforts. Our theme was developed to scale back the machine and storage overhead of the shopper furthermore on minimize the machine overhead of the cloud storage server. we have a tendency to conjointly decreased the dimensions of the proof of knowledge integrity thus on cut back the network information measure consumption. several of the schemes projected earlier need the archive to perform tasks that require a great deal of machine power to come up with the proof of knowledge integrity. however in our theme the archive simply ought to fetch and send few bits of knowledge to the shopper.

5.1 FUTURE ENHANCEMENTS

- Apart from reduction in storage prices knowledge outsourcing to the cloud conjointly helps in reducing the upkeep.
- Avoiding native storage of knowledge.
- By reducing the prices of storage, maintenance and personnel.
- It reduces the possibility of losing knowledge by hardware failures.
- Not cheating the owner.

6.REFERENCES

[1]]M.Armbrustetal.,‘‘Abovetheclouds:ABerkeleyviewofcloudcomputing,’’Dept.Elect.Eng.Comput.Sci.,Univ.California,Berkeley,Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28,2009.

[2] K.Julisch and M. Hall, ‘‘Security and control in the cloud,’’ Inf. Secur. J. Global Perspective, vol. 19, no. 6, pp. 299–309, 2010.

[3] G.Atenieseetal.,‘‘Provabledatapossessionatuntrustedstores,’’inProc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007,pp.598–609.

[4] G.Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, ‘‘Scalable and efficient provable data possession,’’ in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw. (ICST), Istanbul, Turkey, 2008,pp.22–25.

[5] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ‘‘Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability,’’ J. Syst. Softw., vol. 113, pp. 130–139, Mar. 2016

[6] T.Jiang,X.Chen,andJ.Ma,‘‘Publicintegrityauditingforshareddynamic cloud data with group user revocation,’’ IEEE Trans. Comput., vol. 65, no. 8, pp. 2363–2373, Aug.2016.doi: 10.1109/TC.2015.2389955.

[7] Y. Luo, M. Xu, K. Huang, D. Wang, and S. Fu, ‘‘Efficient auditing for shared data in the cloud with secure user revocation and computations outsourcing,’’ Comput. Secur., vol. 73, pp. 492–506, Mar. 2018. doi: 10.1016/j.cose.2017.12.004.

[8] L. Huang, G. Zhang, and A. Fu, ‘‘Privacy-preserving public auditing for dynamic group based on hierarchical tree,’’ J. Comput. Res. Develop., vol. 53, no. 10, pp. 2334–2342, 2016. doi: 10.7544/issn10001239.2016.20160429.

[9] L. X. Huang,G. M. Zhang, andA. M. Fu, ‘‘Certificatelesspublic verification scheme with privacy-preserving and message recovery for dynamic group,’’ in Proc. Australas. Comput. Sci. Week Multiconf., Melbourne, VIC, Australia, 2017,p.76.

[10] J. Li, X. Tan, X. Chen, D. S. Wong, and F. Xhafa, ‘‘OPoR: Enabling proof of retrievability in cloud computing with resource-constrained devices,’’ IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 195–205, Apr. 2015. doi: 10.1109/TCC.2014.2366148.

[11] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, ‘‘Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,’’ J. Netw.mput. Appl., vol. 82, pp. 56–64, 2017. doi: 10.1016/j.jnca