International Journal of Science Engineering and Advance Technology

Shared Data Integrity Using Public Auditing Mechanism

1 Supriya Menon, [2] Sameena Masrath, [3] I.Narsimaha Rao

[1]Associate Professor, [2]Student, [3]Associate Professor, HOD

[1,2,3]Dept of CSE., Medha Institute of Science & Technology for Women, Saiprabhatnagar, Pedathanda, Khammam Rural, Khammam Dist, Telangana, India

ABSTRACT:

Cloud providers assure a safer and dependable environment to the users, the honesty of data in the cloud may still be cooperation, due to the survival of hardware/software failures and human errors. To make certain shared data honesty can be established publicly, users in the group require calculating signatures on all the blocks in shared data. Dissimilar blocks in shared data are usually signed by different users due to data changes do by different users. For security reasons, once a user is cancelled from the group, the blocks which were beforehand signed by this revoked user must be re-signed by an existing user. The straightforward method which agrees to an existing user to download the parallel part of shared data and re-signs it during user revocation, is inept due to the large size of shared data in the cloud. In this paper, we recommend a new public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By employing the plan of proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users in user revocation, so that existing users do not need to download and re-sign blocks by themselves.

KEYWORDS: Public auditing, shared data, user revocation, cloud computing.

INTRODUCTION:

To defend the honesty of data in the cloud, a number of mechanisms have been proposed. In these mechanisms, a signature is fond of to each block in data, and the honesty of data relies on the rightness of all the signatures. One of the most important and common features of these mechanisms is to consent to a public verifier to powerfully check data honesty in the cloud without downloading the entire data, referred to as public auditing or denoted as Provable Data Possession. This public verifier could be a customer who would like to make use of cloud data for particular purposes e.g., search computation, data mining, etc. or a third party auditor (TPA) who is proficient to supply verification services on data integrity to users. In addition, a public verifier is for all time able to inspection the integrity of shared data without retrieving the entire data from the cloud even if some part of shared data has been re-signed by the cloud. Besides, our method is proficient to prop up batch auditing by authenticating several auditing tasks concurrently.

I. RELATED WORK:

Wang et al. leveraged homomorphic tokens to make sure the accuracy of removal code-based data dispersed on multiple servers. To diminish the communication transparency in the phase of data repair, Chen et al. initiated a apparatus for auditing the exactness of data with the multi-server scenario, where these data are programmed with network coding. More recently, Cao et al. put up an LT code-based secure cloud storage mechanism. Compared to previous mechanisms this mechanism can shun high decoding computation costs for data users and put away computation possessions for online data owners through data repair. Recently, Wang et al. planned a record less public auditing mechanism to diminish refuge risks in certificate executive contrast to previous certificate based solutions.

II. PROBLEM DEFINITION:

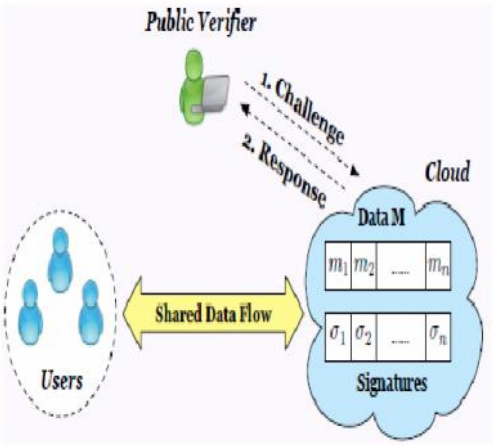
In existing mechanisms, a signature is connecting to each block in data, and the veracity of data relies on the precision of all the signatures. One of the most momentous and ordinary features of these mechanisms is to tolerate a public verifier to capably check data honour in the cloud without downloading the entire data, referred to as public auditing. This public verifier could be a client who would like to use cloud data for particular purposes or a third-party auditor (TPA) who is clever to give confirmation services on data integrity to users. Though the contented of shared data is not distorted throughout user revocation, the blocks, which were before signed by the revoked user, still need to be re-signed by an existing user in the group. As a result, the honesty of the entire data can still be established with the public keys of existing users

only. Straightforward method may price the existing user an enormous amount of communication and computation resources. The number of re-signed blocks is fairly great or the partisanship of the group is often altering.

PROPOSED APPROACH:

We suggest Panda, a narrative public auditing mechanism for the truthfulness of shared data with competent user revocation in the cloud. In our system, by using the thought of proxy re-signatures, once a user in the group is revoked, the cloud is talented to leave the blocks, which were symbol by the revoked user, with a re-signing key. As a result, the competence of user revocation can be drastically improved and totalling and communication resources of existing users can be simply saved. The proposed mechanism is scalable, which points to it is not only capable to resourcefully prop up a large number of users to divide data and but also able to touch multiple auditing tasks at once with batch auditing. We can also lengthen our mechanism into the multi-proxy model to decrease the ability of the misuse on re-signing keys in the cloud and improve the reliability of the entire mechanism. It goes after protocols and does not pollute data integrity dynamically as a malicious adversary. Cloud data can be powerfully shared among a large number of users, and the public verifier is intelligent to handle a large number of auditing tasks simultaneously and efficiently.

SYSTEM ARCHITECTURE:



The scheme contains three entities: the cloud, the public verifier, and users who share data as a group. The cloud offers data storage and sharing services to the group. The public verifier, such as a consumer who would like to make the most of cloud data for particular purposes e.g., search, computation, data mining, etc. or a third-party auditor (TPA) who can make available substantiation services on data integrity, means to confirm the veracity of shared data via a challenge-and reply protocol with the cloud. In the group, there is one original user and a number of group users. The original user is the original owner of data. This original user produces and shares data with other users in the group from side to side the cloud. Both the original user and group users are competent to access, download and modify shared data. Shared data is divided into a number of blocks. A user in the group can modify a block in shared data by performing an insert, delete or update operation on the block.

PROPOSED METHODOLOGY:

USER:

REGISTRATION:

Every user registers his user particulars for using files. Only registered user can capable to login in cloud server.

FILE UPLOAD:

User uploads a block of files in the cloud with encryption by means of his secret key. This makes certain the files to be confined from unauthorized user.

DOWNLOAD:

This allows the user to download the file by means of his secret key to decrypt the downloaded data of blocked user and authenticate the data and reupload the block of file into cloud server with encryption. This makes certain the files to be sheltered from unofficial user.

REUPLOAD:

This will consent to the user to reupload the downloaded files of blocked user into cloud server with resign the files. The files are uploaded with new autograph like new secret with encryption to protect the data from not permitted user.

UNBLOCK:

This permits the user to clear his user account by responding his safety query concerning to answer that offered by his at the time of registration. Once the answer is coordinated to the answer of registration time answer then only account will be unlocked.

AUDITOR MO:

FILE VERIFICATION MODULE:

The public verifier is clever to accurately make sure the honesty of shared data. The public verifier can review the truthfulness of shared data without get back the entire data from the cloud, even if some blocks in joint data have been re-signed by the cloud.

FILES VIEW:

Public auditor observation the all information of upload, download, blocked user, reupload.

ADMIN:

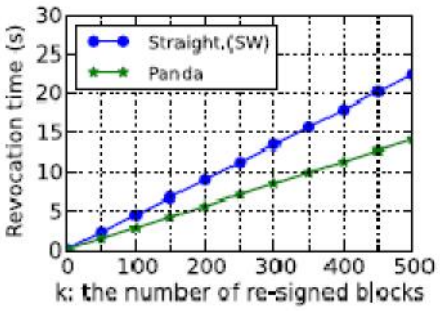
VIEW FILES:

Public auditor outlook the all particulars of upload, download, blocked user, re upload.

BLOCK USER:

Admin wedge the misbehave user account to defend the honesty of shared data.

RESULTS:



The presentation assessment between Panda and the straightforward method in user revocation is presented. With our method, the cloud is intelligent to not only resourcefully re-sign blocks but also save existing users' computation and communication resources. When the number of re-signed blocks is 500, which is only 0.05% of the total number of blocks, the cloud in Panda can re-sign these blocks within 15 seconds. In disparity, without our system, an existing user needs about 22 seconds to re-sign the same number of blocks. Both of the two revocation time are linearly greater than ever with an increase of k—the number of re-signed blocks. As we take for granted the cloud and an existing user have the similar level of computation aptitude in this experiment, it is simple to see that the gap in terms of revocation time between the two lines is mostly bring in by downloading the re-signed blocks.

CONCLUSION:

We anticipated a new public auditing mechanism for shared data with well-organized user revocation in the cloud. When a user in the group is annulling, we agree to the semi-trusted cloud to re-sign blocks that were marked by the revoked user with proxy re-signatures. Tentative results explain that the cloud can pick up the competence of user revocation, and existing users in the group can keep a momentous quantity of calculation and communication resources for the duration of user revocation.

III. FUTURE WORK:

Because collusion-resistant proxy re-signature methods normally have two levels of signatures i.e., the first level is signed by a user and the second level is re-signed by the proxy where the two levels of signatures are in dissimilar forms and need to be established in a different way, attaining block less verifiability on both of the two levels of signatures and validate them collectively in a public auditing mechanism is challenging.

IV. REFERENCES:

[1] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revoation in the Cloud," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, 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] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90–107.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.

[8] 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 the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557.
[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.
[10] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing, accepted.
[11] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.
[12] J. Yuan and S. Yu, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," in Proceedings of ACM ASIACCS-SCC'13, 2013.
[13] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, accepted.
[14] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in the Proceedings of IEEE Cloud 2012, 2012, pp. 295–302.
[15] S. R. Tate, R. Vishwanathan, and L. Everhart, "Multi-user Dynamic Proofs of Data Possession Using Trusted Hardware," in Proceedings of ACM CODASPY'13, 2013, pp. 353–364.