International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 7 4542 - 4546

Improved Third Party Auditing Approach For Shared Data In The Cloud With Efficient Revocation Of User

Miss Madhuri Kulkarni
PG Student, Dept. Of Computer Engineering,
Alard Collage of Engineering and Management,
Savitribai Phule Pune University,
Pune, India
madhuri.kulkarni85@gmail.com

Prof.Sonali Patil
Professor, Dept. Of Computer Engineering,
Alard Collage of Engineering and Management,
Savitribai Phule Pune University,
Pune, India
Sonalin69@gmail.com

Abstract:- verify the integrity of the shared information publically, users within the cluster to ensure that shared information all got to figure out the signatures on blocks. Sharing information by different users in different blocks of information typically changes entirely by individual users are signed. Once a user has canceled the cluster, for security reasons, blocks that antecedently the revoked by signed by associate an existing user must sign in nursing again. The Direct transfer of information sharing that same methodology, half and this user to sign in again over the cancellation of existing user in nursing associate permits, mostly due to the size of share data within is disabled. Over the course of this paper, we share information with the user in mind affordable revocation is a completely unique integrity of public auditing mechanisms to propose is a trend. Proxy re-signature thought of using signatures we didn't order that transfer existing user and blocks by themselves again to sign on behalf of the current cloud blocks users. User to sign in again over are knowledge with the rest of the latest version of the cluster is the cancellation, to allow for a trend. In addition, a public vouchers are often part of the shared although some information has been signed by the cloud while cannot share to retrieve information from the cloud, complete information to audit the integrity of is ready. In addition, our systems at the same time by multiple auditing functions to support verification, auditing is in batch. Experimental results show that our system fairly can improve the efficiency of user cancellation.

Keywords:- *Cloud Computing, Public Auditing, User Revocation, Third Party Auditing (TPA), Shared Data, Security.*

*****

I. INTRODUCTION

The integrity of the knowledge defined in, there are a number of mechanisms are employed. These mechanisms to block the signature information are attached to each, and also the integrity of the knowledge depends on the accuracy of all signatures. One of the most important of these mechanisms and common between options and efficiently check data integrity within the cloud all knowledge, while not a public download Verifier allow as public comment audit. This public Verifier a client who for special purposes cloud data or a third-party auditor (TPA) which user's data integrity is able to provide verification services may want to. Most of the previous work focused on auditing the integrity of personal data. These works, Shared data from audit integrity of the verifiers during the public how to recognize privacy protected on many recent works from consideration. Unfortunately, none of the above performance, efficiency considers user revocation accuracy of shared data in the cloud over the course of the audit.

Knowledge storage and cloud services provided by (such as Drop box and Google drive), with people sharing just as a bunch with each other will work by sharing knowledge with. Once a user makes, especially a lot of shared knowledge within the cloud, each user within the group to gain access to and share knowledge to not completely modified, But conjointly share knowledge with the rest of the latest version of the cluster is ready to share. Although cloud suppliers to a safe and reliable environment promise, the integrity of knowledge within the cloud, hardware/software failures and human errors due to the existence of the agreement has to be evaluated.

In addition, our planned system indicates that it's not climbable, efficiency to share knowledge with users to support an out-sized range perfectly and although the batch audit at the same time with multiple is ready to handle the auditing functions. In addition, the Shamir secret sharing by taking advantage, we additionally within our system in Re: signature key to reduce the chances of abuse on and mechanisms to improve the responsibility of multi-proxy model will expand.

Once a user modifies the shared a block with the revised section to calculate a new need for signature. Modifications from individual users, due to the various blocks are signed by individual users. When a user leaves the group or misbehaves, for security reasons will be canceled for this user from the group. As a result, the revoked users now use shared data should be able to modify the generated signatures revoked user group are no longer valid.

A. Public Data Auditing in Cloud[1]-[15]

On cloud we can able to store data as a group and share it or modify it within a group. In cloud data storage two entities can play important role cloud user (group members) and cloud service provider cloud server. Cloud user is a person who stores large amount of data on cloud server which is managed By the cloud service provider. Users are able to upload their Data on cloud which can be shared within a group. A cloud service provider will provide services to cloud user. The major Issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done by unauthenticated member. To achieve security data auditing concept is come into picture. This can be achieved in 2 ways as:

- without trusted third party
- With trusted third party which is also known as Third Party Auditor who performs verification.

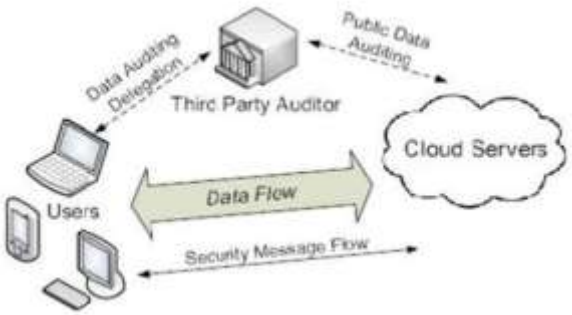

Figure 1: Architecture Of Cloud Data Strage service

Figure 1. Represents the role of Third Party Auditor in cloud Computing architecture.

II Literature survey

In this section we discussed about literature survey on cloud data

In [1]. B. Wang, B. Li, and H. Li, with data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user.

In [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 loud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about overprovisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or underprovisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1,000 servers for one hour costs no more than using one server for 1,000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT.

In [3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of meta data to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems. They present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation.

In [4] H. Shacham and B. Waters, The central challenge is to build systems that are both efficient and provably secure — that is, it should be possible to extract the client's data from any prover that passes a verification check. In this paper, They give the first proof-of-retrievability schemes with full proofs of security against arbitrary adversaries in the strongest model, that of Juels and Kaliski. their first scheme, built from BLS signatures and secure in the random oracle model, features a proof-of-retrievability protocol in which the client's query and server's response are both extremely short. This scheme allows public verifiability: anyone can act as a verifier, not just the file owner. Their second scheme, which builds on pseudorandom functions (PRFs) and is secure in the standard model, allows only private verification. It features a proof-of-retrievability protocol with an even shorter server's response than our first scheme, but the client's query is long. Both schemes rely on homomorphic properties to aggregate a proof into one small authenticator value.

In [5] C. Wang, Q. Wang, K. Ren, and W. Lou In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s).

In [6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of

 ISSN: 2321-8169
4542 - 4546

client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public verifiability or dynamic data operations, this paper achieves both.

II. PROPOSED WORK

A. *System Architecture*

Figure.2: System Architecture

Above diagram shows the proposed architecture which Avoid money loss on data sharing services because it may lie to the public verifier about the incorrectness of data to save the reputation. To avoid this problem we design new system which is shown in the above figure.2
This system consist of three modules,
1) User Module.
2) Auditor Module.
3) Admin Module.

Above mentioned fig.2 consist of the following entities:

- **Public Verifier:** It correctly checks the integrity And correctness of the shared data.
- **User:** Here user can able to share data as Individual or as group.
- **Cloud:** Cloud provides storage service for Shared data.
- **Public Auditing:** It is able to audit the integrity

Without gaining the complete data from the cloud.

In proposed work we are going to implement Multiple Third Party Auditing (MTPA) to share load of TPA, as our system has multi auditing system. So multiple users can access cloud using TPA, so to avoid the failure or to distribute traffic equally. we use multiple TPA concepts here. Besides this we can also implement back-up TPA for the backup purpose because of some reason if our TPA is crashes then we have a backup TPA. In cloud we do load balancing. As load balancing balance the load on the cloud. How this proposed system will be look like is shown in fig.2

As illustrated in fig.2 the system model during this paper includes three entities: the cloud, the public supporter, and users (who share knowledge as a group). The cloud offers knowledge storage and sharing services to the cluster. The public verifier, like a consumer UN agency would love to utilize cloud data for specific functions or a third-party auditor (TPA) UN agency will provide verification services on knowledge integrity, aims to check the integrity of shared knowledge via a challenge-and response protocol with the cloud. within the cluster, there is one original user and a variety of cluster users. The original user is that the original owner of information. This original user creates and shares knowledge with alternative users in the group through the cloud. Each the first user and group users square measure ready to access, transfer and modify shared knowledge. Shared knowledge is split into variety of blocks. A user within the cluster will modify a block in shared data by activity associate degree insert, delete or update operation on the block. Each blocks in the diagram having its own work or the advantages.

Based on the multiple auditing technique mentioned in proposed system, it will make our system more secure, robust & time saving as we are using the concept of multiple TPA with back-up.

B. *Algorithm*

This system uses five algorithm which is explained are as Follows:

1. KeyGen:
Key Generation is the first or basic algorithm of this system. In this algorithm user creates his own key or this key may be public or private.

2. Rekey:
After key generation cloud itself creates the task of rekey, to avoid the collusion.

3. Resign:
When user left the group then on behalf of that left person cloud sign the block which were signed by the left user, which is known as resigning task.

4. ProofGen:
In this type of algorithm by using some protocol that is some set of rules and regulation cloud can generate the proof.

5. Proof Verify:
In this last algorithm is performed by the public verifier whether it is right or not which is done under the proof verify.

III. WORK DONE

In this section we are discussing the practical environment, scenarios, performance metrics used etc.

A. *Hardware and Software Configuration*

- Processor : Pentium iv 2.6 GHz
- Ram : 512 mb dd ram
- Monitor : 15 color
- Hard Disk : 20 gb
- Floppy Drive : 1.44 mb
- CD Drive : lg 52x
- Keyboard : standard 102 keys
- Mouse : 3 buttons

Software *Requirements*

 ISSN: 2321-8169
4542 - 4546

- Front End : Java
- Tools Used : Eclipse
- Operating System : Windows XP/7

B. Re*sult*

This is a TPA tool window where we start a service. After Clicking start service the connection between server & client will be start.

This is a client window from where we use uploading, Modifying and file deletion from cloud.

IV. CONCLUSION

Knowledge sharing with the user in mind cheap revocation of. Proxy re-thought of using signatures, we didn't order that send existing user and blocks by themselves again to sign on behalf of the current cloud blocks users user revocation, to sign in again to enable a trend. In addition, a public booster Knowledge sharing knowledge sharing often although some of the integrity part of the cloud has been signed again by Complete knowledge of cloud, Do not audit is able to recover. In addition, our systems at the same time by multiple auditing functions to support confirmation, auditing is in batch. We have cloudy with user revocation in shared data for a proposed new public auditing mechanism. When a user in the group is canceled, we canceled by semi trusted cloud blocks the user with proxy re-signed again allow to sign.

V. ACKNOWLEDGMENT

It is with the greatest pleasure and pride that I present this paper. At this moment, I cannot neglect all those who helped me in the successful completion of this paper. I am very Thankful to my respected project guide. Associate Professor, for his ideas and help proved to be valuable and Helpful during the creation of this paper and guide me in the right path. I would also like to thank all the faculties who have cleared all the major concepts that were involved in the Understanding of techniques behind this paper. Lastly, I am Thankful to my friends who shared their knowledge in this Field with me.

REFERENCES

[1] B. Wang, B. Li, and H. Li, Public Auditing for Shared Data with Efficient User Revocation in the Cloud, in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 29042912.

[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. 5058, 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 theProceedings of ACM CCS 2007, 2007, pp. 598610.

[4] H. Shacham and B. Waters, Compact Proofs of Retrievability, in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90107.

[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. 19

[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. 355370.

[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. 525533.

[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. 15501557.

[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. 220232, 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. 693701.

[12] J. Yuan and S. Yu, Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud, in Proceedings of ACM ASIACCS-SCC13, 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. 295302.
[15] S. R. Tate, R. Vishwanathan, and L. Everhart, Multi-user Dynamic Proofs of Data Possession Using Trusted Hardware, in Proceedings of ACM CODASPY13, 2013, pp. 353364.
[16] B. Wang, B. Li, and H. Li, Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud, in the Proceedings of ACNS 2012, June 2012, pp. 507525.
[17] M. Blaze, G. Bleumer, and M. Strauss, Divertible Protocols and Atomic Proxy Cryptography, in the Proceedings of EUROCRYPT 98. Springer-Verlag,1998,pp.127144.
[18] A. Shamir, How to share a secret, in Communication of ACM, vol. 22, no. 11, 1979, pp. 612613.