International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-3, June 2015
ISSN: 2395-3470
www.ijseas.com

A mechanism of user revocation based public auditing for shared data in the cloud

A Pichai Mari[1], M John Basha M.E (Ph.D)[2]
[1] PG Student, [2] Head of the Department, Department of Computer Science and Engineering,
PTR College of Engineering and Technology, Tamilnadu, (India)

ABSTRACT:

Cloud mechanism is the most popular emerging technology which satisfies various technical adequacies. The main usage of the cloud environment is sharing resource and now – a –day's security threats and data confidentiality are most disused issues in the cloud environment. In the cloud environment certain members can able to form a group and access the information by sharing. To make the process efficient and secured the data integrity is verified publicly, for this every user needs to compute their signature on each block. For security reason if a user revoked from the group and the remaining user in the group has to resign the signature on all blocks. But this mechanism is inefficient and more complex in dealing with the large amount data stored in the cloud. In order to over these drawbacks we proposed a novel architecture of public auditing mechanism for maintaining the integrity of shared data by means of efficient user revocation in mind. By means of keeping a public auditing, a proxy re-signature handles resigning instead of doing by every existing user in the group. So the public verifier examines the data integrity without retrieving the entire data from the cloud. Our proposed mechanism has the ability of supporting batch auditing by means of verifying multiple auditing tasks concurrently. The overall result justifies the proposed work improves the user revocation mechanism effectively.

Index Term: Cloud computing, public auditing, shared data and user revocation

INTRODUCTION:

Now –a –day's technology growth is very enormous due to the technical requirement in order to improve the overall performance. In this aspect cloud computing plays a vital role which provides a solution for technical imbalance. It provides cloud services as Paas, Naas, Saas, DBaas which enables resources sharing and data sharing in a prominent manner. The major discussion in cloud computing is data transaction done in a secured manner or whether those data are outsourced. The thing is the originality of data is maintained as well as user privacy is also to be maintained. The cloud services can be achieved over internet in which the user can register their details. Based on that identity the server can provided to the user at any time. The improved technology provides virtualization and distributed services by computing resources as well as IT services. The cloud provide data storage and services by means of google drive and drop box, so that multiple user can combine a group and access their data in a secured manner. In this an owner user can manage the original data and every user can view the data, edit and modify with the rest of the group. In order to maintain the data confidentiality the cloud provided process some policy based on that

the group has be to be performed . However it has various advantages but still it suffers from certain issues like reliable performance and maintaining the data integrating. To maintain the data integrity the cloud environment has evolved the mechanism of public auditing. It is nothing but a third part authority for thrusting the user in the group and providing the service in order to maintain the flexibility and scalability.

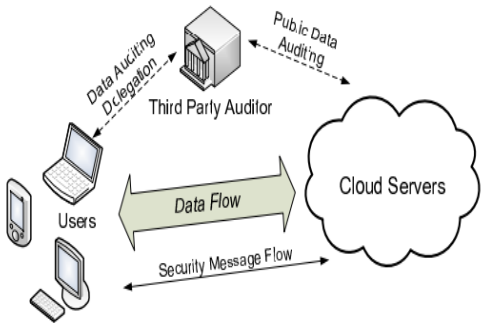

Fig 1: Architecture of cloud data storage service

From the figure 1 it is clear how the processing from the cloud server by means of TPA as public auditing. But in case of group the size stored data in the cloud data is huge and additional mechanism is added for effective data integrity maintenance. So the concept of user revocation is evolved to provide verification services on maintaining the data integrity among the users. In which user revocation is nothing but allowing the every users in the group to access the data by providing signature with the tpa. In case the user leaves the group the remaining members have to revoke the signature in order to maintain the privacy of the data stored in the storage environment. But it increases the computation of cost and complexity in dealing with large amount of data. Then the public key is verified by the tpa to ensure the process working in a secure manner. Then those data can be shared between the group in a trusted manner between the group and the cloud server without any leakage.

RELATED WORKS:

As the technical enhancement increased in the same manner security threats also raised which makes to turn the attention of the researchers in improving the secured group sharing in the cloud environment. This section deals with various methodologies evolved by researchers and processing capabilities in detail. Most of the cloud providers providing a secured services but still there is a possibility of compromising due to its existence of hardware/software failures and human errors [1] [2]. To maintain the data integrity in cloud various approach were evolved [3] – [15]. On those mechanisms the process is separate into several blocks and a signature is attached to every block. Based on the correctness of the signature in each block the user can access the data and shared with their group. The next level of this process is it allows a public verifier to verify the data integrity which is known as public auditing denoted as provable data possession. In which several works [14], [15] were focused on preserving the identity privacy from the public verifiers. But all of these mechanisms were failed to maintain the efficiency of user revocation during auditing the trustiness of shared data in the cloud environment. According to paper [16] once the user modifies the block he has to compute a new signature for that modified block but in case of different user modifies then all the different user has to provide a new signature which makes the process complex. Then the users leave a group for security reason he can’t able to access and modify shared data since he was no longer valid to the group. According to the idea of idea of proxy re-

signatures [17], the user revoked on the group he can be res-sign the block with a re-signing key. As per Shamir Secret Sharing [18] he introduced multi proxy model in order to tough the possibility of misuse on re-signing keys. By means of [19] [20] the integrity of shared data is protected by common group private key if a user revoked then a new private group key is required thus maximize the complexity of key management and decreases the efficiency of user revocation. Some of the traditional proxy re-signature schemes [17], [21], [22] are not block less verifiable it can be directly applied but the user has to download the entire data to check the integrity it results in poor auditing performance. According to the resent work in [23] it is must for a cloud service provider to keep different keys on different user in cloud. An additional mechanism, such as [24], preserves the privacy which can be utilized but that was out of scope. The analysis of batch verification in [25] most of the cases by batch auditing the public verifier accepts an invalid auditing proof which leads to serious problem at the same time it increases time consumption.

EXISTING SYSTEM:

The existing system uses the mechanism of provable data possession (PDP) a public auditing is evolved to check the data correction. It enables erasure codes-based data distributed on multiple servers that not only supports dynamic data but also indentifying the misbehaving server. It maintain a semi trusted protocol so that it does not cause any fault in malicious advisory such as incorrectness on shared data as well as reputation of its data services which leads to losing money on its data services. But by means of the mechanism the user cant able to trust the cloud with shared data integrity because there is a possibility of incorrectness due to the hardware/software failures or human errors happened in the cloud. In order to guarantee the TPA it utilize the homomorphic authenticator and random masking. It supports in elimanating the burden of cloud user but too expensive regarding the auditing task. It uses single key for computation based on that it cant able to affirm the identity of the signer on all block.

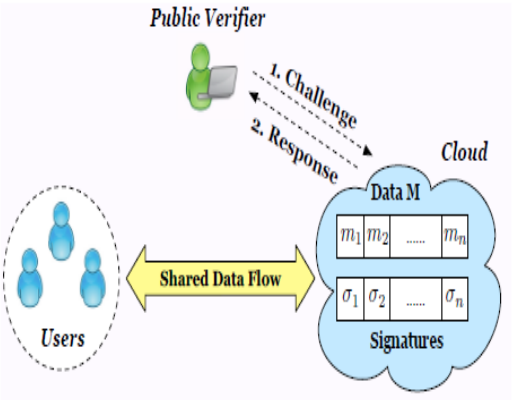

Fig 2: A design view of existing model

PROPOSED SYSTEM:

Our proposed system is based on public auditing system with user revocation which work based on these essential properties such as correctness, efficient – secure revocation, public auditing and scalability.

Correctness: While sharing the data, the public verifier should maintain the data integrity checking correctly.

Efficient – Secure Revocation: If the user is revoked from the group the signed block can be resigned effectively. Only the existing user must valid the signature during shared data.

Public Auditing: Without retrieving the entire data the public verifier can do

auditing even some of the blocks have been resigned by the cloud.

Scalability: The cloud environment is a vast environment and the number cloud users are in huge number as well as the data volume is also high. The public verifier must have the capacity in handling the large number of auditing tasks concurrently and proficiently.

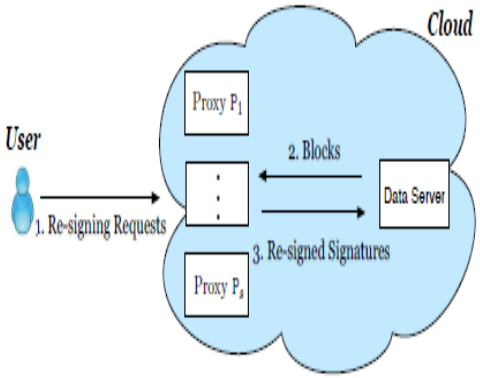

Fig 3: Proposed System

As shown in the figure the proposed system enables multiple resigning proxies in the cloud by storing the stored keys and data separately. Each proxy converts the signature and handles the revoked signature in the group by means of resigning keys. That enables the possibility of correcting the signatures when user revocation happens. That enables the data privacy and security which are compromised by an inside attacker. In addition to it our proposed system withheld a new proxy re-signature scheme which makes possibility on achieving block less verifiability and non-malleability thus enabling the proposed mechanism in well structured form. For this it requires five algorithms such as KeyGen, ReKey, Sign, ReSign and Verify. Let them discuss;

- **KeyGen:** An each individual user in the group has to create public key as well as private key
- **ReKey:** The cloud provider computes a resigning key for every pair of users in the group without any collision
- **Sign:** If the shared data created by the original user than that user has to sign on each block
- **Re Sign:** If the user revoked from the group the cloud resign the block which was created earlier with a resigning key by the revoked user.
- **Verify:** The public verifier verifying the correctness of proof which was responded by the cloud

IMPLEMENTATION MECHANISM:

The implementation section is done by creating a frame work by means of web application using c# with SQL- server. Before that a data base is created which was to be processed. On which block, signature, block identifier and signer identifier were segmented which enables the user to change the single block effectively without modifying the block identifiers of other blocks.

International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-3, June 2015
ISSN: 2395-3470
www.ijseas.com

Fig 4: Implementation architecture

Initially the user choose the prepared data to be processed and he creates a key generation for the group in which the data to be shared. Then the file is blocked and encrypted mean while the block segmentation is done as described above. The user in the data wants to shared by the user in the group then the cloud verifier check the validity and retrieval is done by decrypting the file the original data is viewed. If the user revokes from the group then those mechanism of public auditing using revocation mechanism is processed as discussed earlier.

RESULT AND DISCUSSION:

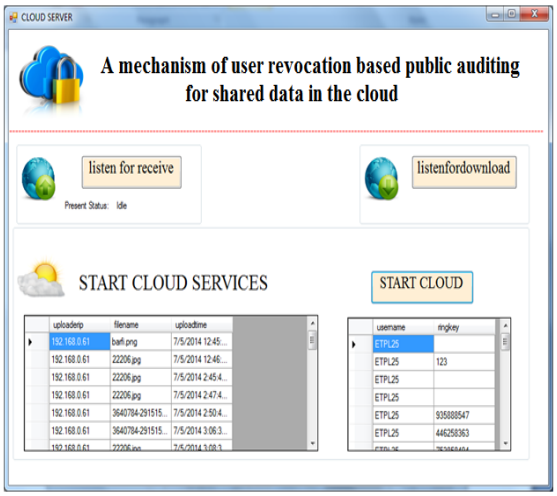

Fig 5: Enabling the cloud services

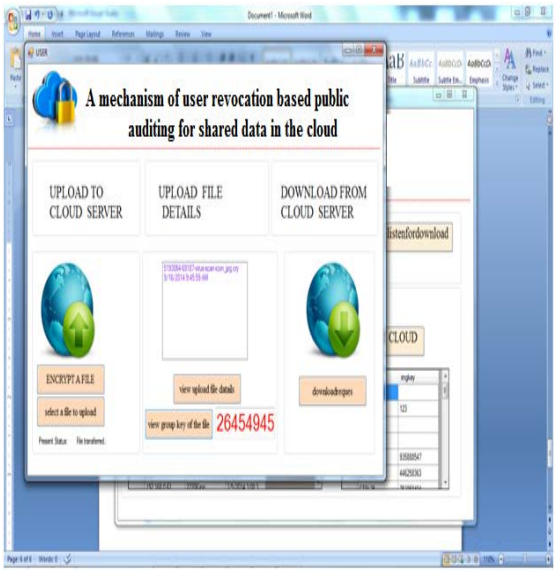

Fig 6: Sharing the data on the group

The fig 5 & 6 shows initially the cloud services were enabled which also provide the details of IP number , file location and which file is selected for process its user name as well as its ring key. According to fig 6 the selected file is selected and encrypted using the group key which was generated by the proxy signature scheme and shared among the group.

Fig 7: Security formats

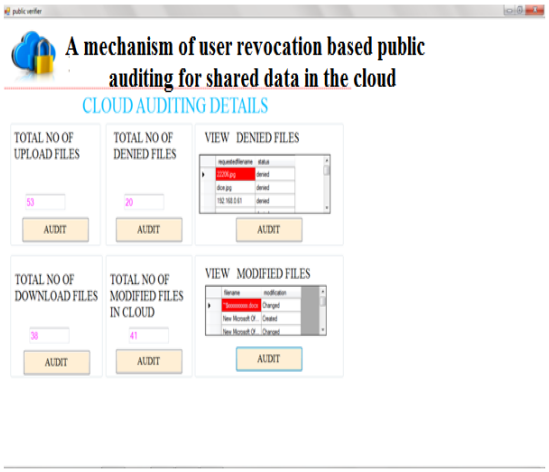

Fig 8: Public auditing on cloud

The fig 7 shows the how the formats of private key and public key are to be formatted. These keys are used and shared by the users which also verified by the cloud provider to ensure the data integrity. The fig 8 shows the result of cloud auditing which describes the details about the entire database used and how it's segmented into blocks. Especially how many files are uploaded and also denied then number of files downloaded as well as modified during of sharing in the cloud which all audited and verified by the public verifier.

CONCLUSION:

In this paper we have discussed the problem of sharing data among the group in a cloud environment. To overcome that, we proposes a new public auditing mechanism for shared data with efficient user revocation in the cloud by means of that a trusted resigned done by the revoked user. This minimizes the computation cost and increase the reliability by means of proxy re-signature scheme. The experimental result justifies our proposed scheme the overall performance of user revocation by allowing the existing users in the group by maintaining and minimizing the working out along with communication resources during user revocation.

REFERENCE:

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, 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) 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.
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. 507–525.
17) M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," in the Proceedings of EUROCRYPT 98. Springer-Verlag, 1998, pp. 127–144.
18) A. Shamir, "How to share a secret," in Communication of ACM, vol. 22, no. 11, 1979, pp. 612–613.
19) B. Wang, H. Li, and M. Li, "Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics," in the Proceedings of IEEE ICC 2013, 2013.
20) B. Wang, S. S. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in Proceedings of IEEE ICDCS 2013, 2013.
21) M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Private-Preserving Personal Profile Matching in Mobile Social Networks," in Proceedings of IEEE INFOCOM, 2011, pp. 2435 – 2443.
22) G. Ateniese and S. Hohenberger, "Proxy Re-signatures: New Definitions, Algorithms and Applications," in the Proceedings of ACM CCS 2005, 2005, pp. 310–319.
23) M. van Dijk, A. Juels, A. Oprea, R. L. Rivest, E. Stefanov, and N. Triandopoulos, "Hourglass schemes: how to prove that cloud files are encrypted," in the Proceedings of ACM CCS 2012, 2012, pp. 265–280.

24) X. Liu, Y. Zhang, B. Wang, and J. Yan, “Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud,” IEEE Transactions on Parallel and Distributed Systems (TPDS), vol. 24, no. 6, pp. 1182–1191, 2013.
25) A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, “Practical Short Signature Batch Verification,” in Proc. CT-RSA. Springer-Verlag, 2009, pp. 309–324.