International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 04
February 2016

Dynamic group data share in cloud computing by user revocation using TPA

P Sushma[1]& Ch.Ravindra Reddy[2]

[1]M-Tech Dept. of CSE Sree Vahini Institute of Science and Technology Tiruvuru Andhra Pradesh

[2]Asst.Professor Dept. of CSE Sree Vahini Institute of Science and Technology Tiruvuru Andhra Pradesh

ravindrareddy.ch94@gmail.com

ABSTRACT

The Cloud Utilizes gets scalable, secure and reliable environment from the Cloud Service Providers. Many Cloud Utilizes are and their data storage is subject to mistrust and scrutiny because data in an un-trusted cloud can be easily misplaced, corrupted or vanished due to integrity threats. Hence, in order to maintain the truthfulness of cloud, we need one Third person who will audit all the data which are stored in cloud. Such a person is called as Third Party Auditor (TPA). TPA provides auditing services to the users who give request to do so. PDP (Provable Data Possession) and WWRL (Wang et al.) are two mechanism which supports public auditing and data privacy but do not support identity privacy and block less verification. Hence

The identity privacy in dynamic group is achieved through the mechanism One Ring to Rule Them All. In this proposed mechanism Third Party Auditor is able to verify the truthfulness of shared data for a dynamic group of users without retrieving the whole data and also the user's identity is also kept private from the TPA. Also supports batch auditing and dynamic operations during public auditing.

Keywords: public auditing; user revocation; dynamic group; share data; cloud computing.

1. INTRODUCTION

The Cloud Storage services, which is common place where not only data stored over it but also shared among users who are using simultaneously. Enterprise-class infrastructure is provided by the Cloud service provider to cloud utilizes. Some of the cloud offerings are Drop box and Google Docs. The integrity of cloud services are subject to mistrust and scrutiny, because of the threats. Threats reveal the important information about the shared data or the user who is working on it. PDP and WWRL mechanisms are used for data privacy and security of data over cloud. But the problem occurred that how to preserve the identity from the TPA, who is auditing the system on request of the user. The identity may reveal sensitive information like which part of data is a higher valuable or which is user in group or block is special. Existing mechanisms do not perform public auditing over shared data on dynamic group while preserving identity. The previously used mechanism provides only public auditing services and data privacy only. The mechanism Provable Data Possession (PDP) [1] provides public auditing service only. PDP mechanism allows a verifier to check the fineness of a client's data stored at an un-trusted server. RSA-

based encryption method and sampling strategies are utilized by this PDP. The verifier needs not to retrieve whole data and he can easily audit the truthfulness of shared data, which is referred to as public auditing. PDP[4] does not support identity privacy. The mechanism Wang et al. (WWRL) [2] proposed public auditing mechanism which is able to protect the secret data from Third Party Auditor by utilizing random[5] masking technique. In this mechanism the private content which belongs to a personal user is not published to the third party auditor. It supports only public auditing and data privacy. Identity[6] privacy is not achieved in WWRL.

2. RELATED WORK

Existing System:

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[7] 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[8] 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. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud.

Proposed System:

In this paper, we propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures[8], we allow the cloud to re-sign blocks on behalf of existing users during user revocation[9], so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit[10] 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. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental[11] results show that our mechanism can significantly improve the efficiency of user revocation.

3. IMPLEMENTATION

Ring Signature:

The concept of ring signature is first proposed by Rivest et al. Using these ring signatures a verifier is convinced that a signature is computed using one of group members' private keys, but the verifier is not able to determine which member private key[3]. Hence this property can be used to preserve the identity of the signer from a verifier. Author Boneh introduced ring Signature Scheme which referred as BGLS. It is constructed from bilinear maps. These Ring signatures are extended in construct public auditing mechanism. It supports batch auditing where multiple auditing tasks from different users efficiently made by leveraging aggregate signature [4].

Hars:

HARS is one of the most suitable mechanisms used for public auditing. However, traditional ring signatures [6,7] cannot be directly used into public auditing mechanisms, because these ring signature schemes do not support block less verification. Without block less verification, the TPA has to download the whole data file to verify the correctness of shared data. Hence it

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 04
February 2016

consumes excessive bandwidth and takes long verification times. In Classic Ring signature scheme data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking. Homomorphism Authenticable Ring Signature allows block less verification. It contains mainly three algorithms Key Gen, Ring Sign and Ring Verify. First each user in the group generates their own public key and private key in Key Gen Process. In Ring Sign, a user in the group is able to sign a block with her private key and all the group members' public keys. A verifier is allowed to check whether a given block is signed by a group member in Ring Verify.

4. EXPERIMENTAL RESULTS

Fig 1: Uploading page.

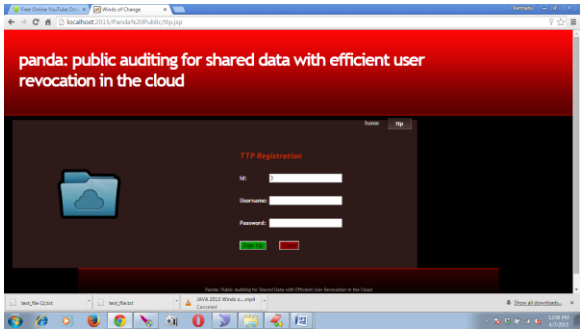


Fig 2: Download File.

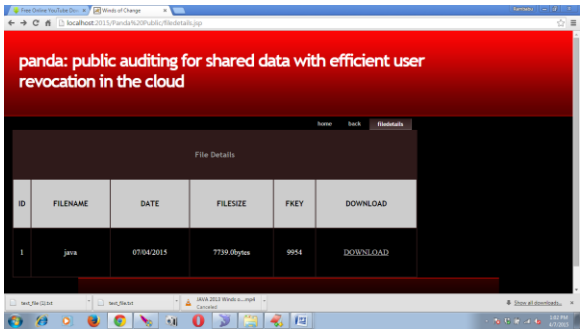


Fig 3: Verify Document Screen

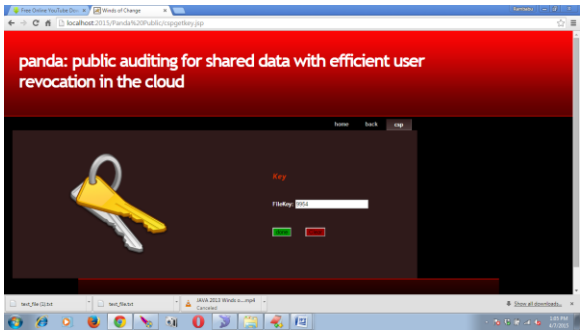


Fig 4: Block Insertion Screen:

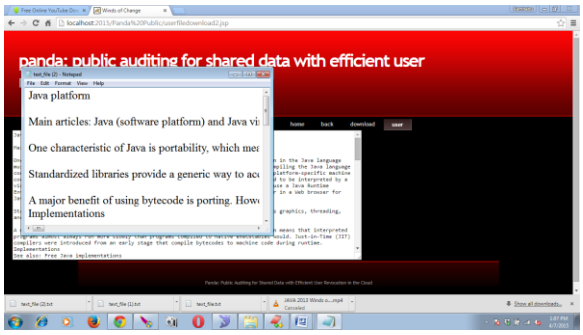
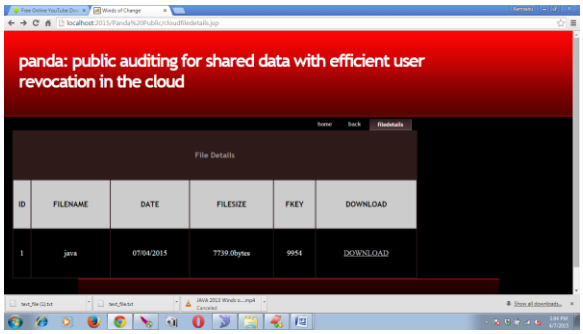


Fig 5: performance table



5. CONCLUSIONS

In order to check the integrity of shared data in dynamic group of users' new public auditing mechanism is defined. Users can revoke from the group due to any malicious behavior or want to exit from group. Hence each time, the auditing should be done with proper ring signature on the Shared block of data which are generated by the user. Efficiency is improved in terms of security and storage due to the user revocation, and communicational and computational resources are also improved. The

proposed method can also be extended with techniques such as Traceability and Data Freshness.

6. REFERENCES

[1] A. M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski,G.Lee, 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, Apil 2010.

[2] 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.

[3] A.Juels and B.S. Kaliski, "PORs: Proofs of Retrievability for Large Files," in Proc. ACM Conference on Computer and Communications Security (CSS), 2007, pp 584-597.

[4] H.Shacham and B.Waters, " Compact Proofs of Retrievability, "in Proc. International Conference on the Theory and Application of Cryptograpy and Information Security(ASIACYPT).SpringerVerlag,2008,pp 90-107.

[5] 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 525-565.

[6] D. Boneh, c. Gentry, B.Lynn, and H. Shacham," Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proc. International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT).Springer-Verlag,2003, pp 416-432. [7] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret ,"in Proc. International Conference on the Theory and Application of Cryptography and Information Security(ASIACRYPT).SpringerVerlag2001

[8] G.Athniese, R.D. Pietro, L.V.Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proc, International Conference on Security and Privacy in Communication Networks (SecureComm),2008, pp 552-565.

[9] G.Athniese, R.D. Pietro, L.V.Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proc, International Conference on Security and Privacy in Communication Networks (SecureComm),2008, pp 552-565.

[10] Y.Zhu, H.Wang, Z. Hu, G.-J.Ahn, H. Hu, and S.S.Yau, "Dynamic Audit Services for Inetgrity Verification of Outsourced Storage in Clouds," In Proc.ACM Symposium on Applied Computing(SAC), 2011, pp 1550-1557.

[11] C.Wang, Q.Wang, K.Ren, and W.Lou, "Ensuring Data Storage Security in Cloud Computing," In Proc. IEEE/ACM International Workshop on Quality of Service (IWQoS), 2009, pp1-9.

Authors Profiles

P SUSHMA
M-Tech Dept. of CSE
Sree Vahini Institute of Science and Technology
Tiruvuru Andhra Pradesh

CH.Ravindra Reddy
Asst.Prfessor Sree Vahini Institute of Science and Technology
M.TECH, MBA Email id: -
ravindrareddy.ch94@gmail.com