 ISSN: 2321-8169
4085 - 4089

A Novel Approach for Efficient User Revocation with Maintaining Shared Data Integrity on Cloud

Ms. Gauri R. Thorat
PG Student ME (Computer)
JSPM'S Imperial College of Engineering
and Research Wagholi, Pune - 412207
gauri.thorat@yahoo.co.in

Prof. S. R. Todmal
Assistant Professor
JSPM'S Imperial College of Engineering
and Research Wagholi, Pune - 412207
srtodmal@gmail.com

Abstract—Cloud computing is the biggest innovation in computing world. It provides great facilities of data sharing and data storing to its users. Here a main risk occurs as data security in aspects of data integrity, data privacy and data access by unauthorized users. TTA (Trusted Third Party) is used by cloud service providers to ensure data security and privacy. In cloud, data modification and data sharing among the group of users is very simple task .To maintain integrity of the shared data,group members needs to compute signatures on all shared data which are available in blocks. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. User revocation is one of the biggest security issue during data sharing. After user revocation, shared data signed by revoked user, needs to re-sign by existing user.This task is very inefficacious due to the large size of shared data needs to download before re-signing it.
This paper is a detail description of cloud public auditor which is used for the maintaining integrity of shared data with efficient user revocation in the cloud. This mechanism uses concept of proxy re-signatures which allows the cloud to re-sign blocks on behalf of existing users during user revocation, so there is no need of data downloading. It also performs batch monitoring to verify multiple tasks simultaneously.
Keywords —Cloud computing; Data integrity; Public auditing;User revocation component;

*****

I. INTRODUCTION

Cloud computing is nothing but internet based computing which can be simply stated as a computing paradigm that provides dynamic computing environment for end users that is reliable and customized and which provides guarantee of quality of service (QoS),which is cost saving and improves data sharing and data storing capabilities. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider [1].It lacks behind due to some security issues like data integrity, data privacy and unauthorized data access.
Maintaining data integrity is one of the difficult tasks. Integrity is nothing but consistency. It ensures completeness of data.

A. Public Data Auditing in Cloud

On cloud we can able to store data in 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 used cloud server for storing large amount of data which is managed by the cloud service provider. Users are able to upload their data on cloud which can be shared it in the group. A cloud service provider will provide services to cloud user. The main 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.

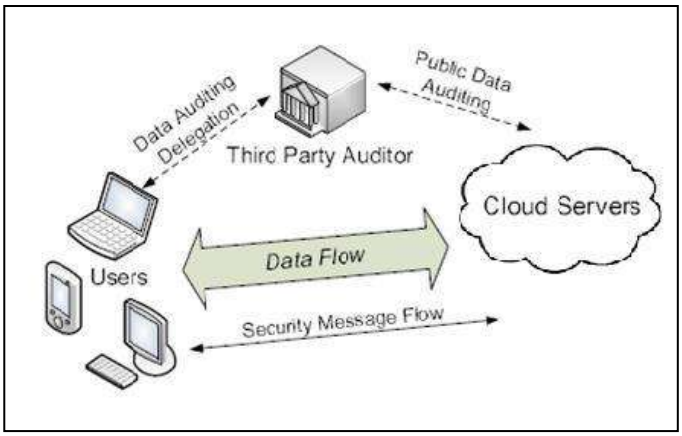


Fig. 1. Architecture of Cloud Data Storage Service

Fig 1. represents the role of Third Party Auditor in cloud computing architecture. It helps cloud to manage data and provide security centrally. The reliability is increased as data is handled by TPA but data integrity is not achieved. TPA uses encryption to encrypt the contents of the file. It checks data integrity but there is threat of TPA itself leaks user's data. Researchers of [2] specify way to achieve storage correctness without Trusted Third Party (TTP). They achieve this by using secure key management, flexible access right managements and light weight integrity verification process for checking the unauthorized change in the original data without requesting a local copy of the data.

 ISSN: 2321-8169
4085 - 4089

II. LITERATURE REVIEW

In cloud public auditing different techniques like MAC,HLA, Virtual Machine etc. are used in different auditing mechanism for different purposes like data integration, data authentication etc. Balkrishna proposed efficient Automatic Protocol Blocker technique for error correction which checks data storage correctness [3].Kiran Kumar proposed automatic protocol blocker to avoid unauthorized access [4]. Jachak K. B. proposed privacy preserving Third party auditing without data encryption. It uses a linear combination of sampled block in the servers response is masked with randomly generated by a pseudo random function (PRF) [5]. Hovav Shacham and Brent Watersy [6] proposed proof-of-retrievability system.In this system, data storage centre must prove to a verier that he is actually storing all of a client's data. Two homomorphic authenticators are proposed by them the first, based on PRFs, gives a proof-of-retrievability scheme secure in the standard model. The second, based on BLS signatures [7], gives a proof-of-retrievability scheme with public variability secure in the random oracle model. Giuseppe Ateniese et all introduce a model which based on provable data possession (PDP)[8]. This is used for verifying that server is processing the original data without retrieving it.Cong Wang Proposed Privacy Preserving Public Auditing technique [9].In this technique public auditing allows TPA and user to check the integrity of the outsourced data stored on a cloud and Privacy Preserving allows TPA to do auditing without requesting data.Here TPA can audit the data by maintaining cloud data privacy. Ning Cao et all explore the problem of secure and reliable cloud storage with the efficiency consideration of both data repair and data retrieval, and design a LT codes-based cloud storage service (LTCS)[10]. Boyang Wang et all proposed Oruta, the first mechanism for privacy preserving and public auditing of shared data in the cloud in [11].They have used ring signatures to construct homomorphic authenticators, so the TPA is able to maintain integrity of shared data, without retrieving the entire data. They have used HARS and its properties for constructing Oruta.

III. SYSTEM MODEL AND ITS DESIGN GOALS

A. System Model

As shown in Fig. 2 system model consists of 3 entities: the cloud, the public verifier and users who share data in a group. By using data storage and sharing services of cloud user can share data in group, they not only access and modify data but also share the latest version with group. Second entity public verifier is nothing but the group admin or a thirdparty auditor (TPA) who can provide verification services to maintain integrity of data on cloud. During data is uploading one user act as a original user who is original owner of the data and others are group members. Owner of data initially upload data with his signature. Shared data is always divided into small data blocks. When group user perform modification operation on any data block he needs to compute a new signature for the modified block. As data is shared in a group, different blocks may be signed by different users because of modifications by different users. Due to the some reason when any user from group leaves the group or or misbehaves, the group needs to revoke this user. The original user acts as the group manager

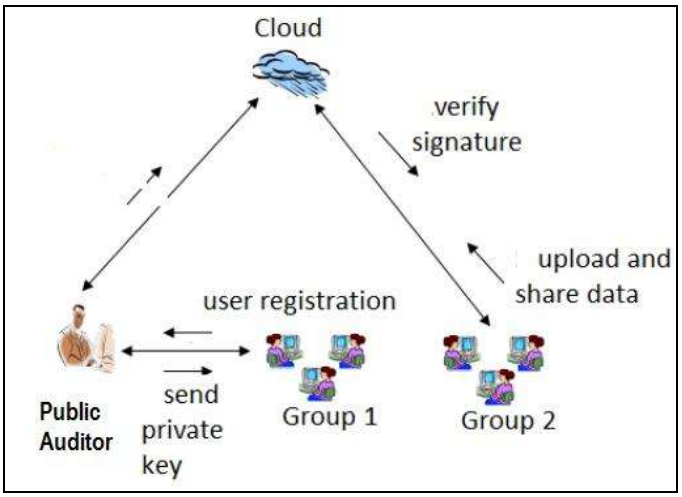


Fig. 2. System Model

and is able to revoke users on behalf of the group. Once a user is revoked, the signatures attached by this revoked user become invalid and the blocks that were previously signed by this user needs to be re-sign with existing users private key, so that the correctness of the entire data can still be verified with the public keys of existing users only.

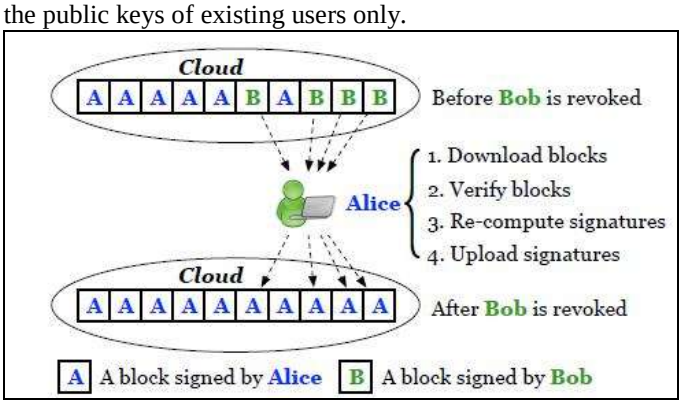


Fig. 3. Traditional Process of User Revocation

Fig. 3 illustrated the most remarkable and common features of previously proposed mechanism which allows public verifier to efficiently check data integrity in the cloud without downloading the entire data. As shown in Fig. 3 cloud data blocks are signed by 2 users Alice and Bob. When Bob revoked from the group Alice needs to first download the blocks previously signed from the group Alice needs to first download the blocks previously signed. by Bob then its verification for correctness of data, then need to re-sign these blocks and finally uploading of data blocks with new signature. This approach of public verifier is time consuming and its not able to handle large data, scalability can not be achieved. Also this not suitable for resource limited devices like mobile phones. Other approach is if cloud stores each user's private key then it can easily perform re-signing task without downloading the data blocks but cloud is not in the trusted domain and outsourcing the users private details to cloud will introduce a security threats. While considering all this factors its important that the re-computation of signature

 ISSN: 2321-8169
4085 - 4089

during revocation should not trouble the basic duty of public auditor of maintaining data integrity. The main challenge is to allow public verifier to check the integrity of shared data without downloading the entire data and efficiently reduce the burden which occurs during user revocation task. In our auditing system, we are introducing the cloud public auditing mechanism which utilizes proxy re-signatures [12] concept for efficient user revocation with maintaining integrity of shared data in the cloud. Fig 4. Illustrated the easy and small process of proxy re-signature during user revocation. By designing a new proxy re-signature scheme which can improve the efficiency of user revocation and computation and communication resources of existing users can be easily saved. Cloud can only able to convert a signature of the revoked user into a signature of an existing user on the same block, but it cannot sign random blocks on behalf of revoked user or an existing user.

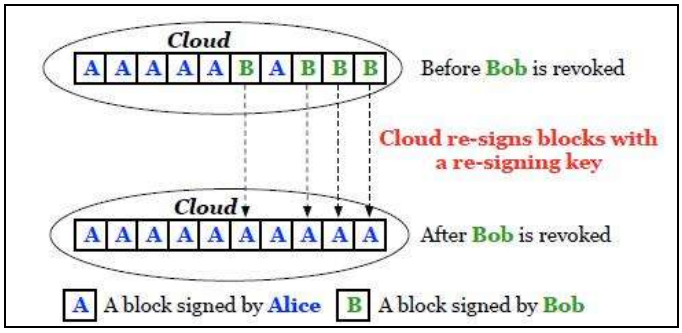


Fig. 4 User Revocation by re-signing data with the help of Public auditor

B. Design Goals

This proposed Cloud public auditor should achieved below mentioned design objectives:

- Correctness – Public verifier is able to maintain data integrity.
- Efficient User Revocation – Public verifier should able to provide user revocation process securely and re-signature of data efficiently.
- Public Auditing – It should be able to perform batch monitoring without retrieving data.
- Scalability – Public verifier should easily handle a large number of auditing tasks simultaneously.

IV. PROPOSED SYSTEM

Proposed system is based on proxy re-signature concepts. Blaze et al first proposed the concept of proxy re-signature in[12].Proxy signature is a digital signature scheme where original user delegates his signing capability to a proxy signer, and then the proxy signer performs message signing on behalf of the original signer. In simple word it allows semi-trusted proxy to work as a converter of signatures between two users belonging to same group.
This concept is the heart of our system which includes below mentioned algorithms -

1. KeyGen - It is a key generation algorithm, it is the one of the important step where public key and private key for each and every group user is created.
2. ReKey - In this step cloud computes a re-signing key for all group users.
3. Sign - When original user upload his data on cloud and shared it within group, he attach his signature on each data block as Sign. Also when other member from a group modified data shared by original user he computes his signature on modified data block.
4. ReSign - In this step, when user revoked from the system, cloud re-signs the data blocks which were signed by revoked user by using his resigning key.
5. ProofGen - Data integrity is verified by using challenge-and-response protocol between the cloud and a public verifier. In ProofGen step cloud can generate a proof of possession for shared data.
6. ProofVerify - In this step a public verifier can check the correctness of a proof responded by the cloud. It verifies data without retrieving it. Here it uses HAPS (a homomorphic authenticable proxy re-signature scheme) with Blockless Verifiability.

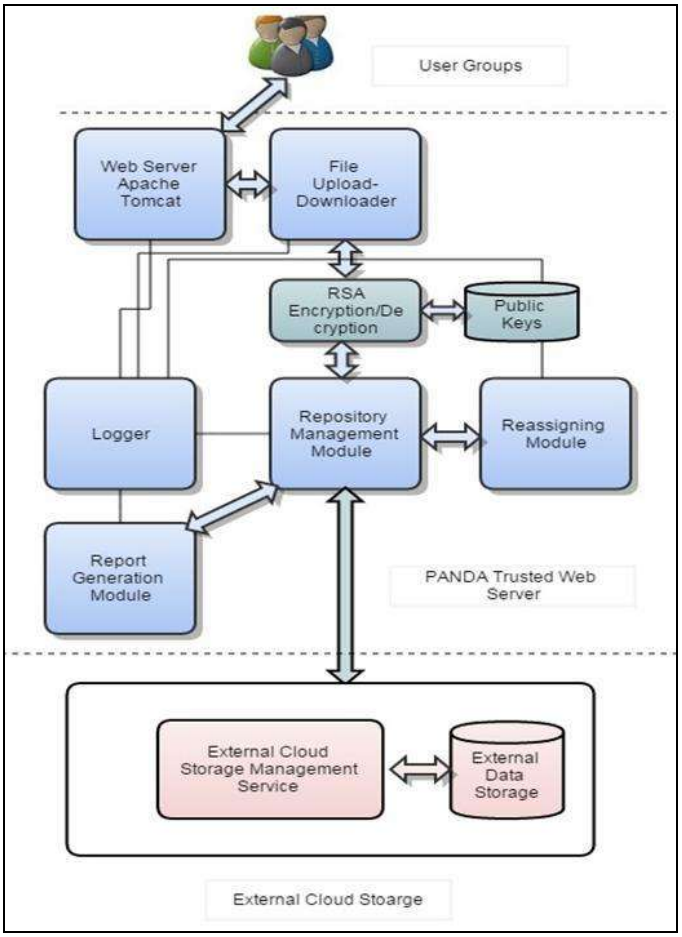


Fig. 5 Architecture of Cloud Public Auditor

A. System Architecture

Architecture of proposed cloud public auditor is shown in Fig.5. It consists of different modules which are responsible for different process which are required for efficient user revocation and to check correctness of data.

1) User Module:

User module is consisting of small sub-modules like Registration, File Upload, Download, Re-upload and

 ISSN: 2321-8169
4085 - 4089

Unblock. When user join group he can register by using web server. After successful registration user can able to upload his data on cloud. He can select data file and upload it on cloud. RSA algorithm converts plain text into cipher text and stored it into cloud database .After successful data uploading generated private key is provided to the user. If user or group member want to access that data they need to download it using their public key.

2) Repository Management Module:

Repository management module is responsible for storing user information and their public key. During verification whatever information required related to data blocks is stored in the repository module.

3) Reassigning Module:

This module is work on concept of proxy resignature. New signature is attaché to data blocks which were previously signed by revoked user.

4) Report Generation Module:

Report generation is attached to logger which maintaining logs of daily activities. These logs are used by report generation module for generation of scheduled reports. Generated reports contain information about users (revoked users and active users).They also produced graphical reports representing performance of system against time used and scalability.

5) External Cloud Storage Management:

For security reasons, it is required to store data and keys separately on different servers by cloud service providers. Therefore, in our mechanism, we assume that the cloud has a server to store shared data, and has another server to manage resigning keys.

V. RESULTS

This section demonstrate the implementation results and experimental performance analysis is carried out on the basis of revocation time and overall auditing time by implementing our proposed mechanism. Graphically presented analysis is most feasible analysis of our mechanism with the existing public auditor.

Fig. 6 Registration Module

Fig.7 Login Module

Fig. 8 Admin Module (Reassignment Module)

Fig.9 User Revokation Report

A. *Impact on revocation time:*

Performance comparison between Cloud Public Auditor and normal method used by TPA during user revocation is presented in Fig.10.When 500 data blocks need to resign traditional mechanism needs 22 seconds while our system performs same operations in 15 seconds.

ISSN: 2321-8169
4085 - 4089

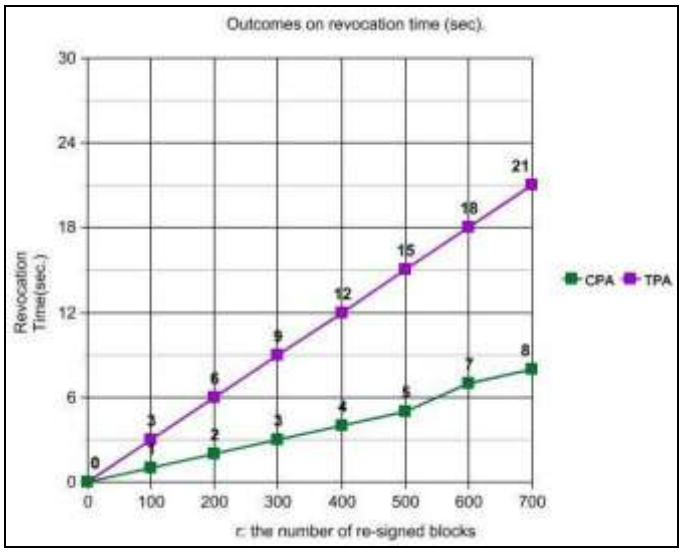
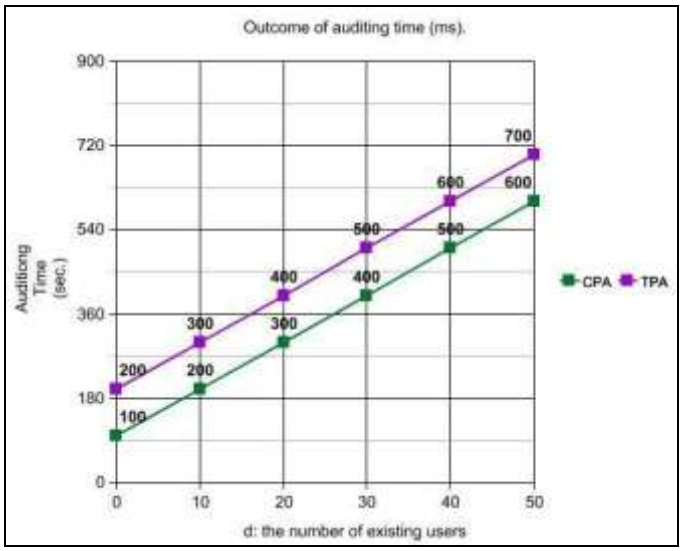


Fig. 10 Comparison of revocation time

B. *Impact on overall auditing:*

Previous public auditor needs more time and extra communication burden to complete auditing task. Also this auditing process is time consuming and cost increasing. Experimental results represented in Fig. 8 can shows our system is quite efficient and handles easily large data and large groups.



VI. Conclusion And Future Scope

Cloud public verifier plays an important role when dealing with security aspects of cloud. In this paper, we have proposed a new public auditing mechanism for cloud for efficient user revocation while maintaining shared data integrity which allows cloud to re-sign blocks signed by revoked user with proxy re-signature. In this mechanism we can able to achieve properties like correctness and scalability while improving the user revocation task. Experimental results demonstrate that it can helps in saving significant amount of computation and communication resources during user revocation.

Future work includes improving performance of the overall system using distributed cloud. Proxy re-signature can be carried out on two or more cloud servers which reduces risk of increased in data or users. It also helps in improving security factors.

ACKNOWLEDGEMENT

This is a great pleasure & immense satisfaction to express my deepest sense of gratitude & thanks to everyone who has directly or indirectly helped me in completing my Dissertation work successfully. I express my gratitude towards project guide Prof.S.R.Todmal Head, Department of Computer Engineering, JSPMs Imperial College of engineering and research, Wagholi Pune. Who guided & encouraged me in completing the Dissertation work in scheduled time. I would like to thanks our Principal Dr.S.V.Admane, for allowing us to pursue my project in this institute. I also thank to Prof.R.N.Phursule, ME Coordinator and Prof. Vinod S. Wadne for his guidance and for being a constant source of support.

References

[1] P. Mell and T. Grance, “Draft NIST working definition of cloud computing”.

[2] 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.

[3] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, “Implementation of EAP with RSA for Enhancing The Security of Cloud Computig”, International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012

[4] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan.S, “Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud”, International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012

[5] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J.,“Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing”, Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012

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

[7] 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

[8] 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, pp. 598–610.

[9] 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.

[10] 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.

[11] H. Wang, “Proxy Provable Data Possession in Public Clouds,” IEEE Transactions on Services Computing, accepted.

[12] 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