ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 08, pp.35929-35933, August, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

PUBLIC AUDITING WITH CLOUD BASED GROUP USER REVOCATION WITH DATA INTEGRITY

***Swati J Avhad and Prof. Ashok V. Markad**

Department of Information Technology, Amrutvahini College of Engg, Sangamner, Ahmednagar Dist., India

ARTICLE INFO

Article History:
Received 29th May, 2016
Received in revised form
21st June, 2016
Accepted 19th July, 2016
Published online 20th August, 2016

Key words:

Public Auditing, Cloud Computing,
User revocation, data Recovery.

ABSTRACT

In the current information technology scenario cloud storage is one of the best database platforms which provide the high security to stored data, and also decrease the burden of local data storage and maintenance. Main problem in cloud computing was the problem of data security and data access by unauthorized users. Storage and sharing of data in cloud can be changed simply by user. To overcome this data modification idea by cloud signature is provided to each individual who access data in cloud once the data modified by the user on block the user must ensure that the signature is provided on specific block when user get revoked from accessing cloud the existing user of that cloud must resign data signed by the revoked user to resigned data user must download the entire data and signed it. This difficulty is rectified with novel public auditing mechanism.

Citation: Swati J Avhad and Prof. Ashok V. Markad, 2016. "Public auditing with cloud based group user revocation with data integrity", *International Journal of Current Research*, 8, (08), 35929-35933.

INTRODUCTION

Cloud storage services, is common place for cloud shared across multiple users and cloud data to be stored. Public auditing for shared data, while preserving identity privacy remains to be an open ultimate test. When we share data among various users, it encourages cloud storage (Boyang Wang *et al*., 2015). The way to preserve identity privacy from the TPA, because the identities of signers on shared data may point out that a desired user in the group is a higher valuable target than others, which is one of the significant problem introduced during public auditing for shared data in the cloud. We apply our project so as to accentuate the efficiency of user revocation in the cloud and provides highly developed scheme for cloud data signatures and thus avoiding unnecessary loss of time of the user to sign these data blocks again and again. Digital signature is a scheme use for demonstrating the authenticity of a digital message or documents which are uploaded by the valid or authorized user. To protect the integrity of knowledge within the cloud and it's best to introduce a 3rd party auditor (TPA) to perform auditing tasks on behalf of users. Such as third party auditor enjoys computation/communication resources that users might not possess. Previous information possession (PDP), 1st planned by, permits a booster to perform public auditing on the integrity (of information of knowledge of information) keeps in Associate in the untrusted server while not retrieving the complete data (Wang, 2013). Resultant work centered on however dynamic information and information privacy may be supported throughout the general public auditing method. However, most of the previous works solely specialize in auditing the integrity of non-public information. A privacy-preserving public auditing mechanism for shared information in Associate in the untrusted cloud, so the identity of the signer on every block in shared information isn't disclosed to the third party auditor (TPA) throughout Associate in auditing task (Wang *et al*., 2013). By protective identity privacy, the TPA cannot comprehend that user within the cluster or that block in shared information may be a higher valuable target than others. info used for verification are computed with ring signatures; as a result, the dimensions of verification info, further because the time it takes to audit with it, are linearly increasing the number of users in a very cluster. to create matters worse, once adding new users to a bunch, all the prevailing verification info can be re-computed if ring signatures are used, introducing a big computation burden to any or all users. To propose a replacement privacy-preserving mechanism to audit information keeps in a very untrusted cloud and shared among an oversized variety of users in a cluster. We tend to make the most of the cluster signatures to construct homomorphic authenticators, so the third party auditor is ready to verify the integrity of shared information while not retrieving the complete information, however cannot reveal the identities of signers on all blocks in shared

****Corresponding author: Swati J Avhad***
Department of Information Technology, Amrutvahini College of Engg, Sangamner, Ahmednagar Dist., India.

information (Zhu *et al*., 2011). Meanwhile, the dimensions of verification info, further because the time it takes to audit with it, aren't affected once the quantity of users sharing the info will increase.

The initial user, United Nations agency creates and shares the info within the cloud, is ready to feature new users into a bunch while not re-computing any verification info (Armbrust *et al*., 2010). Additionally, the initial user (acts because the cluster manager) will trace cluster signatures on shared information, and reveal the identities of signers once it's necessary. We tend to additionally utilize homomorphic MACs to effectively cut back the quantity of space for storing required to store verification info. As a necessary trade-off, we tend to enable the third party auditor to share a secret key try with users that we tend to sit down with as approved auditing. Though we tend to enable a certified TPA to possess the key try, the TPA cannot cypher valid cluster signatures as cluster users as a result of this secret key try is just an area of a bunch user's personal key. To our greatest data, we tend to gift the primary mechanism designed with quantifiability in mind once it involves support auditing information shared among an oversized variety of users in a very privacy-preserving fashion. 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 Cloud 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 over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning 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 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT. (Wang *et al*., 2014)

G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. 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 metadata 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. H. Shacham and B. Waters, In a proof-of-retrievability system, a data storage center convinces a verifier that he is actually storing all of a client's data. Both schemes rely on homomorphic properties to aggregate a proof into one small authenticator value (Wang *et al*., 2013) C. Wang, Q. Wang, K. Ren, and W. Lou, Cloud Computing has been envisioned as the next generation architecture of IT Enterprise.

Literature survey

Boyang Wang, Baochun Li, and Hui 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. 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. 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, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, 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 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 results show that our mechanism can significantly improve the efficiency of user revocation. (Boyang Wang *et al*., 2015)

Problem definition

Problem of efficient and secure public data authorization inspection for shared data this schema still not secure against the data leakage of cloud storage server from unauthorized attacker and revoked group user revocation in cloud storage system.

Proposed system

The deficiency of these schemes motivates us to explore how to design an efficient and reliable scheme, when achieving secure user revocation. we propose a construction which not only supports group data encryption during the data processing, but also realizes efficient and secure user revocation. Idea is to apply vector commitment technique over the database. Then we used the Asymmetric Group Key Agreement (AGKA) and group signatures to support decrypted data base modified among group users and effective group user revocation respectively. The group user uses the AGKA protocol used for encrypt/decrypt the share database.

The group signature will prevent the problem of cloud and revoked group users, in the user revocation phase where the data owner will take part and the cloud could not revoke the data that last modified by the revoked user.

Contribution

We will explore on the secure and efficient shared data public auditing with some new featured with data backup and storage as there ever increasing data storage on cloud there is a need to the duplicated files is removed and available more storage spacehence we will be using deduplication algorithm for eliminating this problem.

Implementation detail

A. System Overview

The proposed system shows the following architectural view

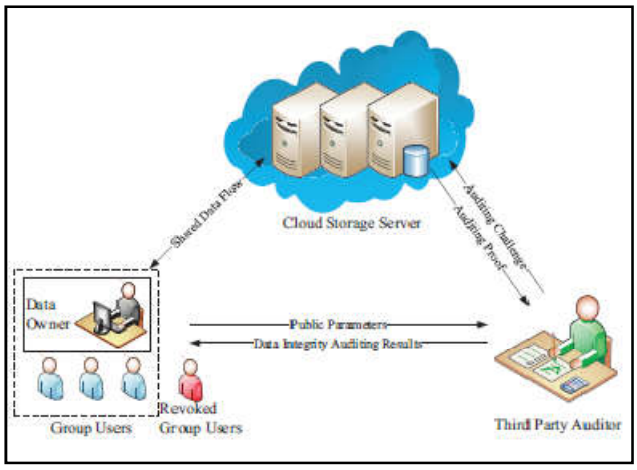


Fig. System architecture

User module can perform following operation.

Registration

In this each user register his user details for using files. Only registered user can able to login and proceed in cloud server

2) File Upload
In this user upload a block of encryption files in the cloud by using his secret key this ensure the files to be protected from unauthorized user.

3) Download
In that module download the file using his secret key to decrypt the downloaded data of blocked user and verify the data with encryption. This ensure the files to be protected from unauthorized user.

4) Reupload
This allow the user to need to reupload the downloaded files of blocked user into cloud server with resign the files(i.e) the files is uploaded with new signature protected the data from unauthorized user.

5) Update/delete file

6) Key generation: generate key by applying key generation algorithm.

2) Auditor module:
File Verification

The public verifier can audit the integrity of shared data without need to retrieving the entire data from the cloud, sometimes if some blocks in shared data have been re-signed by the cloud

3) Admin module:
View Files:
In this public auditor view the all details of upload, download, blocked user, reupload.
Block User:
In this admin block the unauthorized user account to protect the integrity of shared data

Algorithm

Construction of panda:

Panda include six algorithms: key_gen, re_key, sign, re_sign, proof_gen, proof_verify.
key_gen: it is used for key generation like private key and public key by each client in this process.
re_key:re-sign key of each pair of client is evaluated
re_sign – revoked user block resigning by this key.
proof_gen-- cloud produced proof data under the challenge of public verifier
proof_verify --conform the correctness of a proof by the cloud.

Mathematical module

S is represented system S={M,E, A,K,F,D}
1.INPUT DATA
2.M={m1 ,m2 ,m3 ,……..mn}
Where M is the data file and m1, m2, m3…..mnare the number of documents.
2. Encryption
E={e1, e2, e3,…….en}
E is represent as a set of Encrypted data and e1, e2, e3,…….en is number of encrypted file.
3. AES Algorithm
A={K,F} where A=AES encryption decryption algorithm
F= File to be encrypted K is AES key which is randomly selected number from S_Box tables.
4. Decryption
D={d1,d2 ,d3, ..dn} where D is the set of Decrypted data
d1, d2, represents number of decrypted data.
a) Uploading file:
U (Z) = {u1, u2,u3.....un}
F (Z) = {f1, f2,f3.....fn}
S (Z) = {s1, s2,s3.....sn}
MAC (Z) = {m1,m2,m3....mn}
D (Z) = {d1, d2,d3.....dn}
Where,
U (Z): Total number of users.
F (Z): Total number of files.
S (Z): Total number of secret key.
MAC (Z): Master key.
D (Z): Total data
U (Z) U F(Z): S(Z) U MAC (Z)

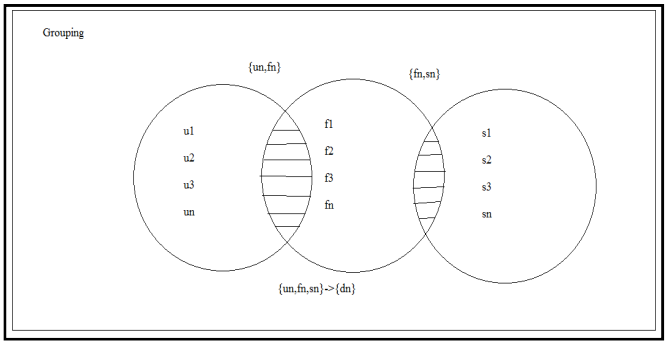


Fig. 2. Uploading files

Downloading Files:

U (Z) U S (Z) U MAC (Z):D (Z)

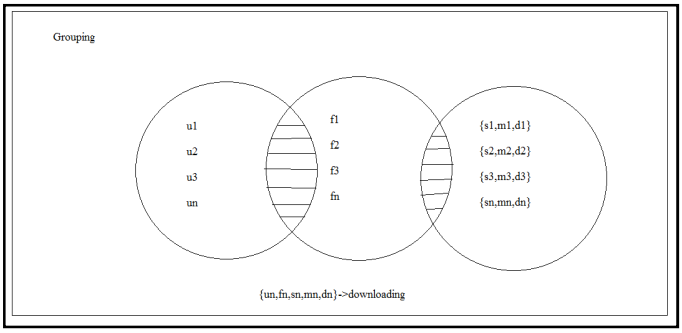
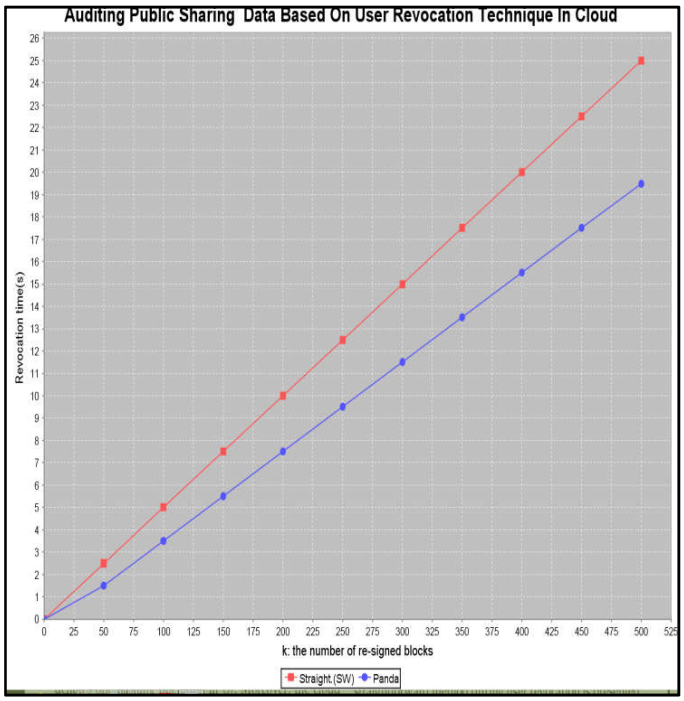


Fig. 3. Downloading files

Success Condition: Properly generated Secrete key As well as MAC key.

Failure Condition: Handle unauthorized user

RESULT ANALYSIS



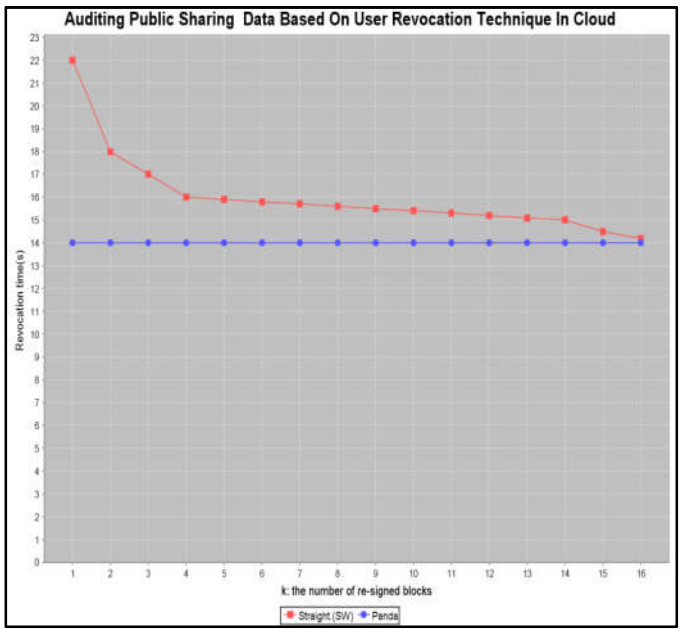


Fig.4. Analysis

Let two groups of order p, g be a generator of G1, e: G1 X G1-> G2 be a bilinear map w be another generator of G1 .The parameters are (e, p, G1, g2, g, w, H), Where H is a function with H:{ 0,1}*-> G1.

- Keygen
- Rekey
- Sign
- Re-sign
- Verify

Time Complexity: O (5n)

Experimental setup

In this the System consists of technology like Advance JAVA, HTML, CSS and JavaScript. For back end SQL Server is used. Also, Hence before experimental set up Software like Eclipse, Tomcat is projected to be installed on server. User should have basic windows family, good browser to view the results.

Conclusion & Future scope

Solve the security and efficiency problem of public data integrity auditing with multiuser modification. Also introduced ages algorithm for security of data in cloud. Data recovery server is used for data backup on the cloud.

REFERENCES

Armbrust, M., 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,” Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

Boyang Wang, Baochun Li and Hui Li, “Public Auditing for Shared Data with Efficient User Revocation in the Cloud”, *IEEE Transactions on services computing*, vol. 8, no. 1, January/February 2015.

Shacham H. and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'08), pp. 90-107, and 2008.

Wang B., B. Li, and H. Li, "Oruta: Privacy Preserving Public Auditing for Shared Data in the Cloud", Proc IEEE CLOUD, pp. 295,302, 2014.

Wang, C., Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th ACM/IEEE Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

Wang, C., Q. Wang, K. Ren, and W. Lou, "Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing", Proc. IEEE INFOCOM, pp. 525-533, 2010

Wang, C., Q. Wang, K. Ren, "Privacy-Preserving Public Auditing for Secure Cloud Storage Auditing", IEEE transaction on computer, 2013

Wang, H. "Proxy Provable Data Possession in Public Clouds", IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, Oct.-Dec. 2013.

Wang, Q., C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing", Proc. 14th European Conf. Research in Computer Security (ESORICS09), pp. 355-370, 2009.

Zhu, Y., H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, and 2011.

****