ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Efficient Group user Revocation Mechanism with a Public Integrity Auditing System for Sharing Data in Cloud

Shruti Suresh Adhav, Prof. Swati Jaiswal

M. E Student, Department of Computer Engineering Smt. Kashibai Navale Sinhgad Institute of Technology and Science Kusgaon (Budruk), Lonavala, Pune, Maharashtra, India

Assistant Professor, Department of Computer Engineering, Smt. Kashibai Navale Sinhgad Institute of Technology and Science Kusgaon (Budruk), Lonavala, Pune, Maharashtra, India

ABSTRACT: The improvement in the field of the cloud computing provides storage outsourcing becomes a new approach, which provide the secure remote data auditing a new subject that exist in the research literature. Previous research considers the difficulties occur in secure and effective public data integrity auditing for dynamic data which is shared within group. However, proposed methods are still unsecured against the collusion of storage over cloud server and users were revoked from group during user revocation in cloud storage system. In proposed system, we provide an efficient public integrity auditing method with secure user revocation from group which based on vector commitment and verifier local revocation group signature. Proposed system supports avoiding duplication of file shared by user when they are stored and also for efficient access of file keyword based search can be done.

KEYWORDS: Public integrity auditing, victor commitment, group signature, cloud computing.

I. INTRODUCTION

The improvements in cloud computing as well as third party cloud service providers (CSP's) provides efficient way to organization, enterprises to outsource their important data to which overcomes the data storage restrictions of resource constrain local devices. There are already many cloud storage services are available in market like Amazon's simple storage service (S3) [1] andcloud‘s software as a service like Google Drive, Dropbox, Mozy, Bitcasa and Memopal [2][3][4][5][6]. Sometimes invalid results are provided by cloud server due to human maintenance,failure of hardware or software and malicious attack. There should be need to protect privacy and security of cloud user's data by means of accessibility and data integrity.

To overcome today's cloud storage service's security issues, Rabin's data dispersion scheme for simple replication and protocols are not sufficient for practical application .Various methods and their different variants for achieving the integrity and availability of remote cloud storage have been proposed. In these proposed methods, when a scheme supports modification of data, it is known as dynamic scheme, otherwise it is known as static scheme. When the data owners and the third party auditor (TPA) both can performs the data integrity check then the scheme is *publicly verifiable.*However, the focus of the dynamic scheme is on the cases where only and only data owner could modify the data of cloud. But due to more and more use of information it should be shared by any user in the group.Also the integrity checking should be done by any user and also by data owner. Revocation of user should be efficient so that revoked user should be unable to access the data.

In previous methods used the data owner does not take part in the user revocation phase,where the cloud itself could conduct the user revocation phase. In this case, the collusionof revoked user and the cloud server will give chance to malicious cloud server wherethe cloud server could update the data and when user tries to access data false datais retrieved.The deficiency of above schemes motivates us to explore how to design anefficient and reliable scheme, while achieving secure group user revocation.In previousscheme all the files shared by users are stored irrespective of their

DOI: 10.15680/IJIRCCE.2017. 0504301

names which causesduplication of files which motivates us to develop the system which can avoid thisduplication and give efficient storage and access of file.Also need for easy and fast access to files motivates us to design scheme by generating keywords of file and access fileswith that keywords.

II. RELATED WORK

Recently, Yuan and Yu [9] designed a dynamic public integrity auditing scheme with securegroup user revocation. The scheme is based on polynomial authentication tags andadopts proxy tag update techniques, which makes their scheme support public checkingand efficient user revocation. However, the authors do not consider the ciphertextstore. Also, to make the scheme efficient, the data owner (the data owner as privatekey is not necessary) does not take part in the user revocation phase, where the cloudcould conduct some malicious operation of userˆas data when it colludes with the revokedusers. Wang et al. [10] designed another scheme based on the assumption that no collusion
occurs between cloud servers and revoked user. As a matter of fact, they assumedthat the private and authenticated channels exit between each pair of entities and collusionbetween invalid users and cloud servers will lead to the disclosure of secrets of allother valid users. Group signature is introduced by Chaum and Heyst [14]. It providesanonymity for signers, where each group member has a private key that enables the userto sign messages. However, the resulting signature keeps the identity of the signer secret.Usually, there is a third party that can conduct the signature anonymity using aspecial trapdoor. Some systems support revocation [12], where group membership can be disabled without affecting the signing ability of unrevoked users.

III. PROPOSED SYSTEM

In proposed system proposes a construction which not only supports group data encryption and decryption during the data modification processing, but also realizes efficient and secure user revocation. The proposed system involves four parties:

1. Group Users
2. Cloud Storage Server(CSS)
3. Third Party Auditor(TPA):
4. De-duplication

1. Group Users: Group users consist of a data owner and a number of users who are authorized to access and modify the data by the data owner. In our system, the data owner could encrypt and upload its data to the remote cloud storage server. Also, he/she shares the privilege such as access and modify (compile and execute if necessary) to a number of group users. The data owner is different from the other group users, he/she could securely revoke a group user when a group user is found malicious or the contract of the user is expired. data owner is able to trace the last user who update the data (data item), when the data is generated by the generation algorithm and every signature generated by the user is valid. Data owner (the data owner’s private key is not necessary) does not take part in the user revocation phase, where the cloud could conduct some malicious operation of user’s data when it colludes with the revoked users. In their scheme, if the data owner trivially shares a group key among the group users, the defection or revocation any group user will force the group users to update their shared key. The group user use the AGKA protocol to encrypt/decrypt the share database, which will guarantee that a user in the group will be able to encrypt/decrypt a message from any other group users. The group signature will prevent the collusion of cloud and revoked group users, where the data owner will take part in the user revocation phase and the cloud could not revoke the data that last modified by the revoked user.

2. Cloud Storage Server(CSS): The cloud storage server is semi-trusted, who provides data storage services for the group users. The cloud storage server colludes with the revoked group users, and they want to provide a illegal data without being detected. Actually, in cloud environment, we assume that the cloud storage server is semi-trusted. Thus, it is reasonable that a revoked user will collude with the cloud server and share its secret group key to the cloud storage server. In this case, although the server proxy group user revocation way brings much communication and computation cost saving, it will make the scheme insecure against a malicious cloud storage server who can get the secret key of

revoked users during the user revocation phase. the position binding property of vector commitment of the scheme allows the cloud storage server to prove the data item correctness of certain position. Our scheme is secure against the collusion attack of the cloud storage server and the revoked users in the efficient scheme, and it is also efficient, since the computational resources invested by the client is independent on the size of the database. The reason is that, most of the expensive computation overhead is outsourced to the cloud storage server. Finally, the cloud storage server store all the database and its relevant materials. Thus, except some private key materials, the group users do not require to store any data locally.

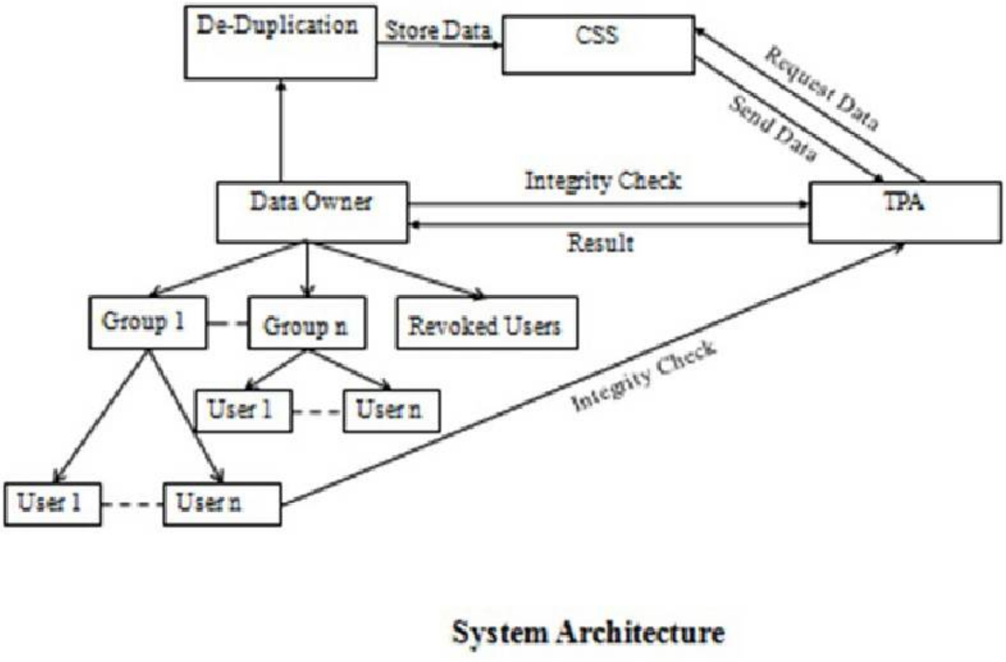


Fig : System architecture of proposed system

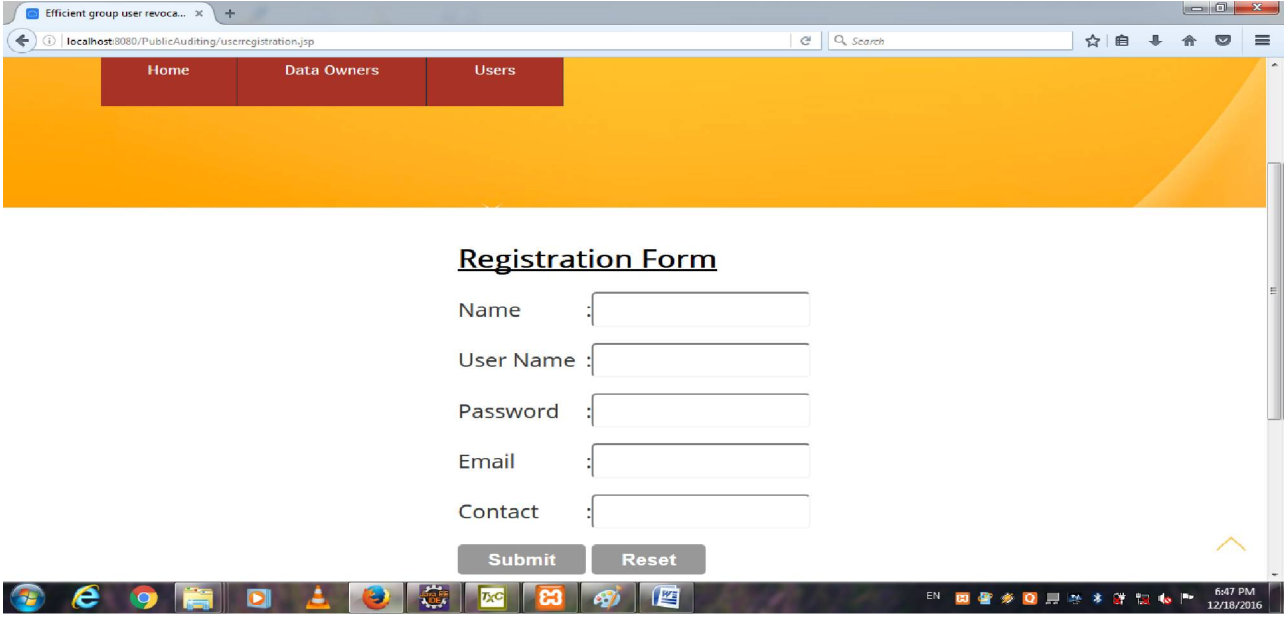
3. Third Party Auditor(TPA): TPA could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server. The TPA could efficiently verify the integrity of the data stored in the cloud storage server, even the data is frequently updated by the group users. if for any data the TPA can provide a proof for this misbehavior, when the dishonest cloud storage server has tampered with the database.

4. De-duplication: When user shares the file in the group the file get stored at CSS and also one copy at TPA. At this point the duplication of files is avoided by using de-duplication means when user tries to store file with same name which already exist system gives message file already present.

IV. RESULTS

After implementation above process flow we get the desire result which was the aim behind this study.

1. User registeration:


Efficient group user revoca...
localhost:8080/PublicAuditing/userregistration.jsp
Search
Home
Data Owners
Users

Registration Form

Name :

User Name :

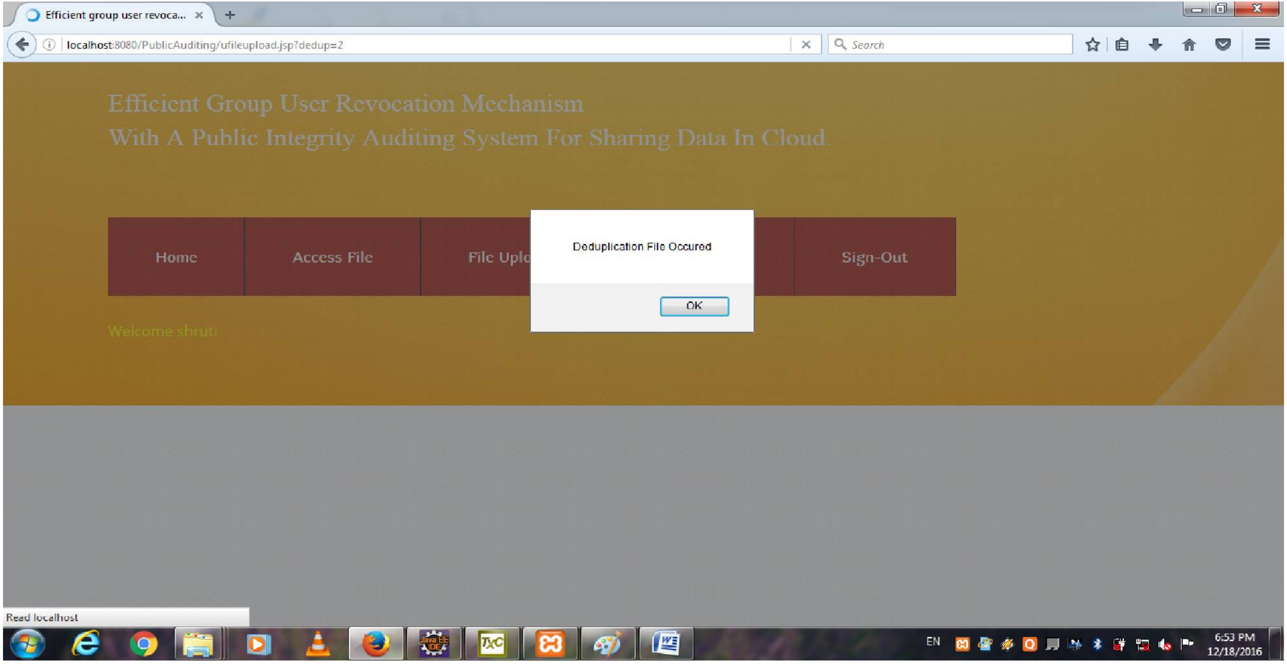
Password :

Email :

Contact :

Submit Reset

2. De-Duplication: This page shows that when user tries to store same file again duplication of file occur and system sends the same message to user for avoiding duplication of file.


Efficient group user revoca...
localhost:8080/PublicAuditing/ufileupload.jsp?dedup=2
Search
Home
Access File
File Uplo
Sign-Out
Read localhost

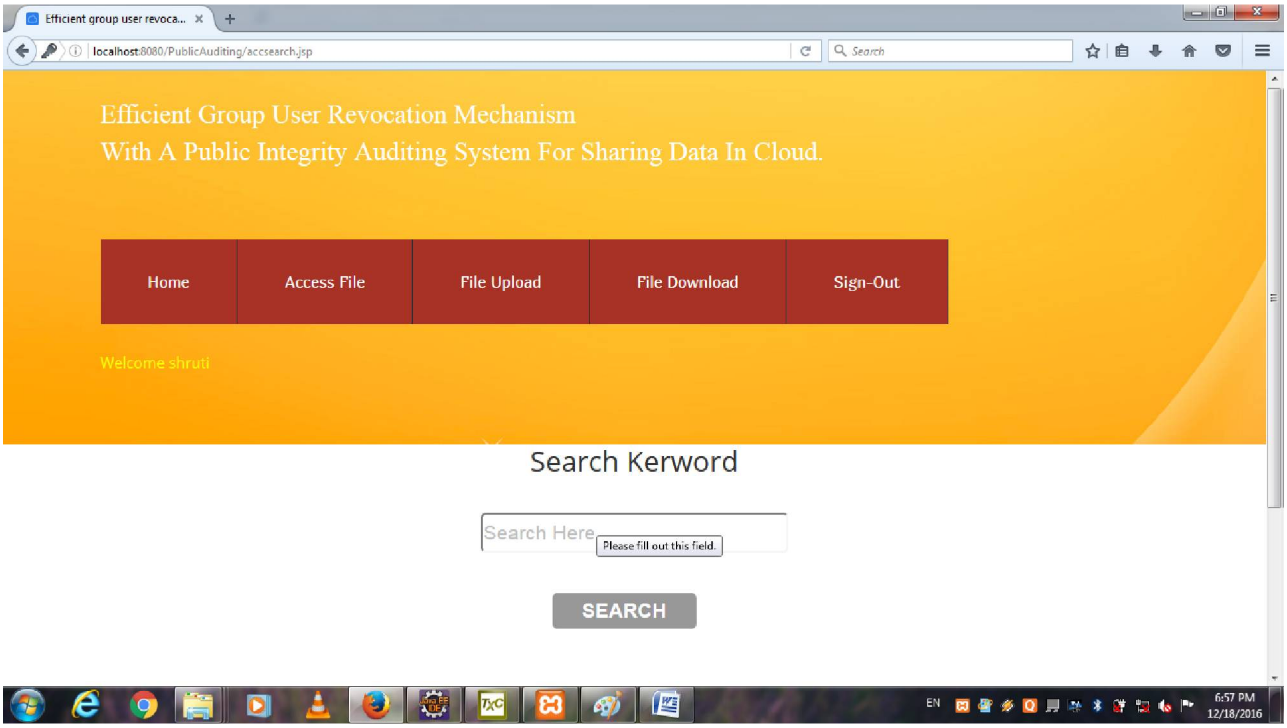
Efficient Group User Revocation Mechanism
With A Public Integrity Auditing System For Sharing Data In Cloud.

Deduplication File Occured

OK

Welcome shruti

3.Keyword based search:This is the same page which shows when user want to access file to make the search efficient user has to enter the keyword related to file he want to search.



Efficient Group User Revocation Mechanism
With A Public Integrity Auditing System For Sharing Data In Cloud.

Welcome shruti

Search Kerword

Search Here

Please fill out this field.

V. Conclusion and Future Work

The propose system provides efficient and secure data integrity auditing for dynamic data that is share with multi-user modification. The proposed schemes likes vector commitment, user revocation with group signatures and Asymmetric Group Key Agreement(AGKA) are used to achieve the high data integrity auditing of data stored on remote side. In the public auditing for data, the combination of the three primitive provides our scheme that provide secure users revocation from the group to dynamic data shared within group. Also proposed system shows provide use data confidentiality in the group, and it also provide security against the collusion attack from the revoked users from group and cloud storage server. Future work includes improving performance of the overall system using distributed cloud. Proxy resignature 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 also efficient group user key management is carried out that focus on revoking users privatekey, without changing public key.

REFERENCES

[1] Tao Jiang, Xiaofeng Chen, and Jainfeng Ma.,ˆaPublic Integrity Auditing for sharedDynamic Cloud Data with Group User Revocationˆa,IEEE TRANSACTION ONCOMPUTERS VOL:pp NO:99 Year 2015.
[2] Amazon. [Online]. Available: http://aws.amazon.com/s3/ Amazon. (2007) Amazonsimple storage service (amazon s3)
[3] Google. (2005) Google drive. Google. [Online]. Available:http://drive.google.com/
[4] Dropbox. (2007) A file-storage and sharing service. Dropbox.[Online]. Available:http://www.dropbox.com/
[5] Mozy. (2007) An online, data, and computer backup software.EMC. [Online]. Available:http://www.dropbox.com/
[6] Bitcasa. (2011) Inifinite storage. Bitcasa. [Online]. Available:http://www.bitcasa.com/
[7] Memopal. (2007) Online backup. Memopal. [Online].Available:http://www.memopal.com/
[8] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren and Wenjing Lou,"Privacy-Preserving Public Auditing forSecure Cloud Storage".

[9] J. Yuan and S. Yu, ”Efficient public integrity checking for cloud data sharing withmultiuser modification, in Proc. of IEEEINFOCOM 2014”, Toronto, Canada, Apr.2014, pp. 21212129.
[10] B. Wang, L. Baochun, and L. Hui, ”Public auditing for shared data with efficientuser revocation in the cloud”, in Proc. Of IEEE INFOCOM 2013, Turin, Italy, Apr.2013, pp. 29042912.
[11] D. Catalano and D. Fiore, ”Vector commitments and their applications, in Public-Key Cryptography ”- PKC 2013, Nara, Japan, Mar. 2013, pp. 5572.
[12] G. Ateniese, D. Song, and G. Tsudik, ”Quasi-efficient revocation in group signatures,in Proc. of FC 2002, Soughamption, Bermuda, Mar. 2002, pp. 183197.
[13] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer,”Asymmetric group keyagreement”, in Proc. of EUROCRYPT 2009, Cologne, Germany, Apr. 2009, pp.153170.
[14] D. Chaum and E. van Heyst, ”Group signatures”, in Proc. Of EUROCRYPT 1991,Brighton, UK, Apr. 1991, pp. 257265.

BIOGRAPHY

Shruti Suresh Adhavis a last year student of ME in Computer Engineering Department, SKN Sinhgad Institute of Technology and Science, Kusgaon, Pune, Maharashtra. He isperusing Master of ComputerEngineering degree from Savitribai Phule Pune University.

Prof Swati Jaiswal is an Assistant Prof. in Department of Computer Engineering, Smt. Kashibai Navale Sinhgad Institute of Technology and Science Kusgaon (Budruk), Lonavala, Pune, Maharashtra, India.