Improved Secure File Sharing In Cloud By Enabling File Key Revocation

Ravi Kumar P[1], Rakshanaa R[2], Reshma M[3], Yamini R[4]

[1, 2, 3] Dept of Computer Science and Engineering

[4]Assistant Professor, Dept of Computer Science and Engineering

[1, 2, 3, 4] Adhiyamaan College of Engineering, Hosur, India.

Abstract- *Cloud storage auditing schemes for shared data refer to checking the integrity of cloud data shared by a group of users. User revocation is commonly supported in such schemes, as users may be subject to group membership changes for various reasons. Previously, the computational overhead for user revocation in such schemes is linear with the total number of file blocks possessed by a revoked user. The overhead, however, may become a heavy burden because of the sheer amount of the shared cloud data. We propose a novel storage auditing scheme that achieves highly-efficient user revocation independent of the total number of file blocks possessed by the revoked user in the cloud. This is achieved by exploring a novel strategy for key generation and a new private key update technique. Using this strategy and the technique, we realize user revocation by just updating the non revoked group users' private keys rather than authenticators of the revoked user. Meanwhile, the proposed scheme is based on identity-based cryptography, which eliminates the complicated certificate management in traditional Public Key Infrastructure (PKI) systems. Instead of changing non revoked user key we can implement Random key generator for file accessing in a group. Hence unauthorized user as well authorized user could not access the file with the key generated again and again. Hence our system provide high security and increases performance compared to other available methods.*

Keywords- Cloud computing, User revocation,Cloud storage auditing,Identity based cryptography.

I. INTRODUCTION

The data sharing is one of the most widely used services that the cloud storage provides. With data sharing service, users can share their data in the cloud with a group of users, and reduce the burden of local data storage. Users, however, will lose the physical control over their data when they share them in the cloud. In order to check the data integrity, some cloud storage auditing schemes for shared data are proposed. When a group user misbehaves or leaves the group, the user should be revoked from the group. Therefore, user revocation is a common realistic necessity in cloud storage auditing for shared data. In cloud storage auditing schemes, the data owner needs to use his/her private key to generate authenticators(signatures) for file blocks. These authenticators are used to prove that the cloud truly possesses these file blocks. When a user is revoked, the user's private key should also be revoked. For traditional cloud storage auditing schemes for share data, all of authenticators generated by the revoked user should be transformed into the authenticators of one designated nonrevoked group user. In this case, this non-revoked group user needs to download all of revoked user's blocks, re-sign these blocks, and upload new authenticators to the cloud. Obviously, it costs huge amount of computation resource and communication resource due to the large size of shared data in the cloud. In order to solve this problem, recently, some auditing schemes for shared data with user revocation have been proposed. When a user is revoked, the cloud will transform the authenticators of the revoked user's blocks into the authenticators of one non-revoked group user corresponding to these blocks, with a re-signing key. The computation overhead of user revocation is still linear with the total number of file blocks stored by the revoked user in the cloud. Although this method relieves the burden on the non-revoked group user, it transfers the burden to the cloud.

We construct a novel cloud storage auditing scheme for shared data supporting real efficient user revocation in this paper. In this design, the group's public key is replaced by the group's identity information, which remains unchanged in the whole lifetime. The group's private key derives from two components. One component remains fixed since being issued, and the other component alters with user revocation. We also propose a novel private key update technique to support user revocation. When users are revoked from the group, all of the non-revoked users can update their private keys by this technique to make the cloud storage auditing still work, while the identity information of the group does not need to change. In addition, the revoked users are not able to upload data and authenticators to the cloud any more. In this way, all of the authenticators generated before user revocation do not need to be recomputed. Therefore, the overhead of user revocation is fully independent of the total number of the revoked user's blocks. Even when the amount of data is immense, the group can still complete user revocation very efficiently. Besides, our scheme is based on identity-based cryptography, which eliminates the complicated certificate management in traditional PKI systems, including certificate generation, certificate revocation, certificate renewal, etc.

II. LITERATURE REVIEW

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service.With cloud computing and storage services, data is not only stored in the cloud, but routinely shared among a large number of users in a group. It remains elusive, however, to design an efficient mechanism to audit the integrity of such shared data, while still preserving identity privacy. In this paper, we propose Knox, a privacy-preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group. Enabling file key revocation, we improve the secure file sharing in cloud storage.

III. EXISTING SYSTEM

The data sharing is one of the most widely used services that the cloud storage provides. When a group user misbehaves or leaves the group, the user should be revoked from the group. Therefore, user revocation is a common realistic necessity in cloud storage auditing for shared data. In cloud storage auditing schemes, the data owner needs to use his/her private key to generate authenticators (signatures) for file blocks. These authenticators are used to prove that the cloud truly possesses these file blocks. When a user is revoked, the user's private key should also be revoked. For traditional cloud storage auditing schemes for share data, all of authenticators generated by the revoked user should be transformed into the authenticators of one designated non-revoked group user.

DISADVANTAGES:

- Costs huge amount of computation resource and communication resource due to the large size of shared data in the cloud.
- Reconstruction key for the entire group or shared data is a huge process.
- The matter will be even worse when the membership of the group frequently alters.

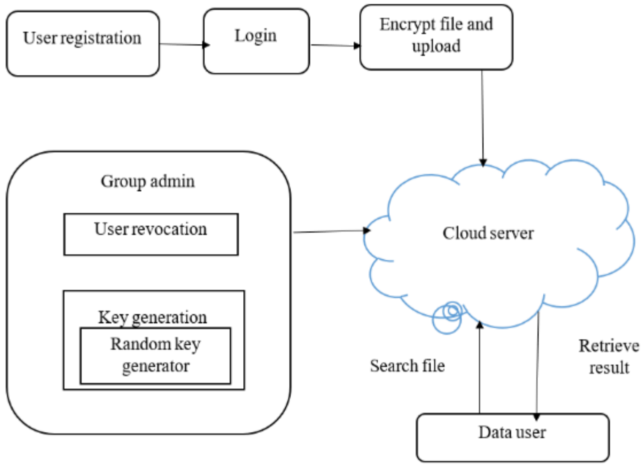
IV. PROPOSED SYSTEM

In cloud when a user register their detail to utilize the facility of cloud he/she will be allotted with a unique ID and password. When user wants to upload their data he/she can encrypt it for security and upload it in cloud. Cloud will not provide complete security therefore we trust third party for key generation and maintenance. If a new user needs particular file that particular user need file accessing key first. Once the file accessing key received he/she can download that specific file from cloud in encrypted format. To decrypt the file that particular user need that specific file key. Instead of changing the key in the remaining members in a group we are going to change the file access key randomly each time. Therefore if a user revoked from a group instead of changing the key for remaining member in our proposed we are going to change file access key which enhances security level and avoid unauthorized user access. Similarly computation process and cost consumption process are reduced in our work which increases performance of our system.

ADVANTAGES:

- Unauthorized user does not access the file without user knowledge.
- Key revocation process was completely reduced which reduces overhead of our system.

V. SYSTEM DESIGN



VI. MODULE DESCRIPTION

A. CLOUD SERVER:

Cloud is the huge storage of resources. Cloud is responsible for storing all members of data and access to the file within a group to other group members based on publically offered revocation list which is maintained by Group Admin. We imagine that the cloud server is honest but curious. That is, the cloud server will not unkindly delete or alter user data, due to the security of data auditing schemes.

B. USER REGISTRATION:

After successful creation of cloud setup, members want to get registered with the system through user registration process. While registering, members have to submit their personal details for completion of registration process. User registered with their information such as identity (user name, mobile no and email-id). During registration process, user got unique identity and access structure. This generates secret key for the members. For registered users they will obtain private key, that secret key is used for file encryption and decryption.

File upload is the method of storing specified data files into the cloud. Uploaded files remains in the cloud up to the time specified while uploading the file. Before uploading the file, file has to be encrypted and compacted to ensure security and privacy of the files.

To access the data that are store in the cloud, group member will give request as group id, data id. Cloud server will verify their signature, if the group member in the same group then allow to access file. Group member have rights to access data, but not having rights to delete or alter the data that are store in the cloud.

C. GROUP MEMBERS:

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. Both Group Admin and group member can login using their login details. After successful login, Group Admin activates newly added users of the cloud by generating keys for each member using bilinear mapping and send it to the corresponding group members. He can also check the group details, and assign group signature. After successful login, Group Members signature is verified. After successful verification, the member can upload, download and can modify the files. Group member must be encrypting data file before uploading to the cloud. Here encryption will be done through Random key generator for ensuring high level security.

D. GROUP ADMIN:

The Group Admin is acted by the administrator of the company. Therefore we imagine that the Group Admin is fully trusted by the other parties. Group Admin perform various operations such as system parameters generation, user registration, group creation, assign ring signature, generation of private key using bilinear mapping and assign to the requested user, maintain revocation list and migrate this list into cloud for public use, and traceability.

Key Distribution: Means of distribute secret keys through the Group Admin that is valid only if the group members are not revoked from the group. Key can be updated by generating new key from an old key.

User Revocation: User revocation is the method of removal of user from system user list which is performed by group admin. Group admin can directly revoke multiple users through public revocation list at every time without affecting any non revoked user. If the login credentials of the specified user matches with the details of revocation list then access denied.

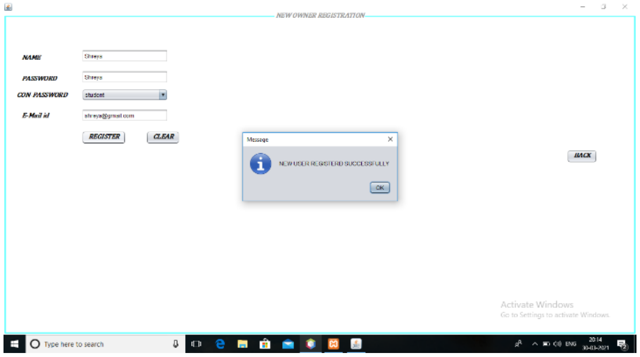
E. RANDOM KEY GENERATOR:

To create Random key Matrix of size (16x16) we have to take any key. The size of key must be less than or equal to 16 characters long. These 16 characters can be any of the 256 characters (ASCII code 0 to 255). The relative position and the character itself is very important in our method to calculate the randomization number, the encryption number and the relative shift of characters in the starting key matrix. We take an example how to calculate randomization number, the encryption number and relative shift from a given key.

VII. CONCLUSION

In this paper, we propose an identity-based cloud storage auditing scheme for shared data, which supports real efficient user revocation. In our scheme, the cloud or the non-revoked user does not need to change the key of exist user in cloud. The overhead of user revocation in our scheme is fully independent of the number of the revoked user’s blocks. Security proof and experimental results show that our proposed scheme is secure and efficient.

VIII. RESULTS



NEW OWNER REGISTRATION

NAME Shreya

PASSWORD Shreya

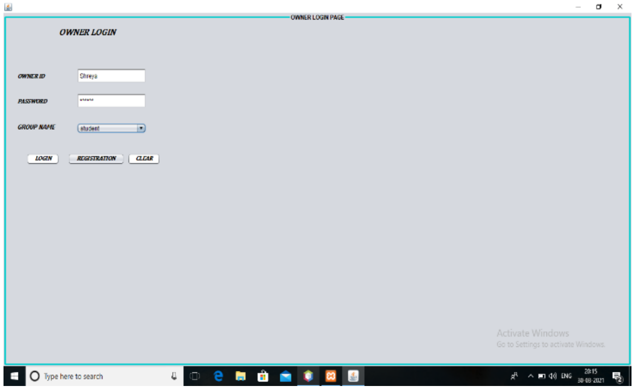
CON PASSWORD student

E-Mail id shreya@gmail.com

Message

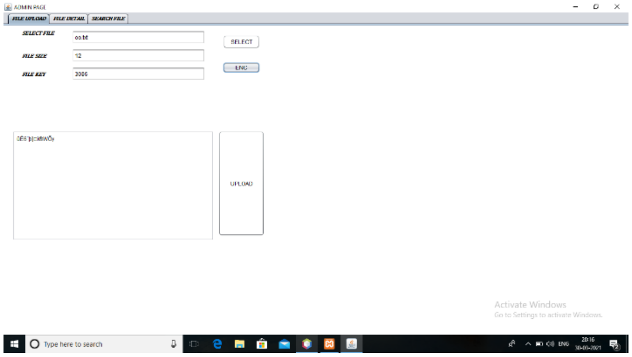
NEW USER REGISTERD SUCCESSFULLY

Fig. 1.User registration page



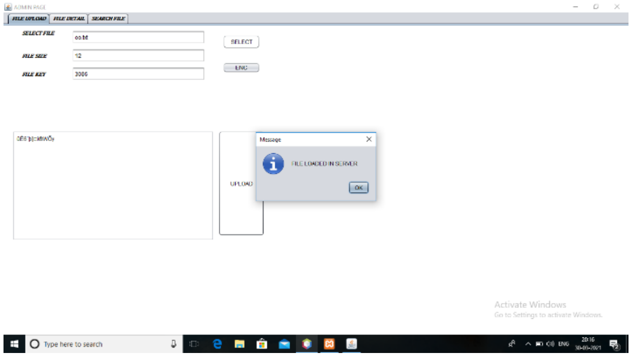
OWNER ID Shreya
PASSWORD ******
GROUP NAME student

Fig. 2.User login page



SELECT FILE oo.txt
FILE SIZE 12
FILE KEY 3086

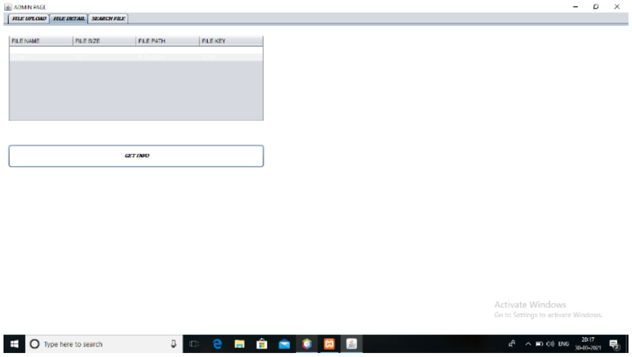
Fig. 3. File uploading page



SELECT FILE oo.txt
FILE SIZE 12
FILE KEY 3086

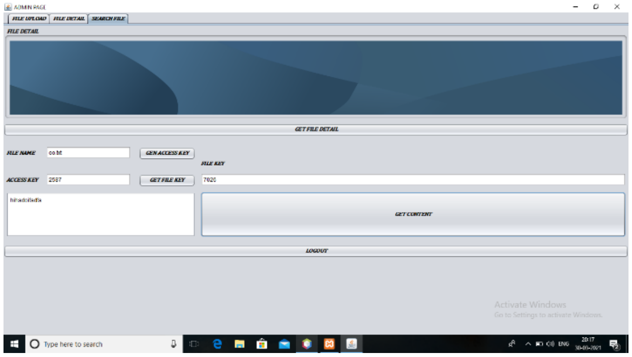
FILE LOADED IN SERVER

Fig. 4. File uploaded successfully



FILE NAME	FILE SIZE	FILE PATH	FILE KEY

Fig. 5. File details page



FILE NAME oo.txt
ACCESS KEY 2587
FILE KEY 7026
hihadsfadfa

Fig. 6. File search tab

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[2] B. Wang, B. Li, and H. Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,” In Proc. of IEEE Cloud 2012, pp. 295-302, 2012.

[3] B. Wang, B. Li, and H. Li, “Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud,” In Proc. of International Conference on Applied Cryptography and Network Security, pp. 507-525, 2012.

[4] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao. “Enabling Public Auditing for Shared Data in Cloud Storage Supporting Identity Privacy and Traceability,” Journal of Systems and Software, vol. 113, pp. 130-139, 2016.

[5] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu and R. Hao, “Light-weight and Privacy-preserving Secure Cloud Auditing Scheme for Group Users via the Third Party Medium,” Journal of Network and Computer Applications, vol. 82, pp.56-64, 2017.

[6] B. Wang, B. Li, and H. Li, “Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud,” IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92-106, 2015.

[7] J. Yuan and S. Yu, “Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1717-1726, Aug. 2015.

[8] Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, “Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation,” IEEE Trustcom/BigDataSE/ISPA, pp. 434-442, 2015.

[9] Goran Cˇ andrliC´ , “How Much Is Stored in the Cloud?”, online at http://www.globaldots.com/how-much-is-storedin- the-cloud/.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data

Possession at Untrusted Stores," In Proc. of ACM CCS 2007, pp. 598- 610, 2007.

[11] A. Juels and B. S. Kaliski Jr, "Pors: Proofs of Retrievability for Large Files," In Proc. of 14th ACM conference on Computer and communications security, pp. 584-597, 2007.

[12] H. Shacham and B. Waters, "Compact Proofs of Retrievability," In Proc. of ASIACRYPT 2008, pp. 90-107, 2008.

[13] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," In Proc. of 4th international conference on Security and privacy in communication netowrks, pp. 1-10, 2008.

[14] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol.22,no.5, pp. 847-859, 2011.

[15] Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 409-428, 2013.

[16] D. Cash, A. K¨upc¸ ¨u, and D. Wichs, "Dynamic Proofs of Retrievability via Oblivious Ram," In Proc. 32nd Intl Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT 13), pp. 279-295, 2013.

[17] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.

[18] M. Sookhak, A. Gania, M. K. Khanb, and R. Buyyac,"Dynamic Remote Data Auditing for Securing Big Data Storage in Cloud Computing," Information Science, vol. 380, pp. 101-116, 2017.

[19] L. Rao, H. Zhang, and T. Tu, "Dynamic Outsourced Auditing Services for Cloud Storage Based on Batch-Leaves- Authenticated Merkle Hash Tree," IEEE Transactions on Services Computing, Available online 26 May 2017 DOI: 10.1109/TSC.2017.2708116.

[20] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers, vol. 62, No. 2, pp. 362-375, 2013.