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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Survey on Efficient Group User Revocation Mechanism with a Public Integrity Auditing System for Sharing Data in Cloud

Shruti S. Adhav[1], Prof Swati Jaiswal[2]

M. E Student, Dept. of Computer Engineering, SKN College, Lonavala, India[1]

Professor, Dept. of Computer Engineering, SKN College, Lonavala, India[2]

ABSTRACT: The advancement of the cloud computing provides storage outsourcing becomes a new approch, 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 unsecure 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 the public auditing and effective user revocation with properties like traceability, efficiency and confidently of secure group user revocation.

KEYWORDS*:* Public integrity auditing, victor commitment, dynamic data ,group signature.

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] and cloud'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.

II. RELATED WORK

The Boyang Wang, Baochun Li and Hui Li[11] proposed a system which shows that services of cloud provide not only data storage in single share place, but also effective as well as secure sharing of data across multiple users. However, it remains create challenge to audit the shared data by preserving identity privacy. This system proposed public auditing of shared data stored in cloud by using privacy preserving scheme. The concept of group signature was

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

proposed in this paper which computes the verification information that is required for integrity auditing of shared data. With this mechanism, third party auditor (TPA) which can publicly verify shared data integrity without accessing entire data remains unaware about the signer identity of each block in shared data and data remains private. In extend this mechanism support batch auditing. This mechanism is responsible for auditing multiple shared data in just single auditing task[8]. The high level comparison between Oruta and its relevant existing systems are shown in following *Table 1*. This paper represent first attempt towards designing effective public auditing of shared data in the cloud storage by preserving privacy.

TABLE I. Comparison of Existing Schemes

	PDP	WWRL	Oruta
Public Auditing	Yes	Yes	Yes
Data Privacy	No	Yes	Yes
Integrity Privacy	No	No	Yes

Yuan and Yu[24] proposed a dynamic public integrity auditing scheme with group user revocation but secrecy of data among the group users is not considered. That means, their scheme could not support cipher text data update and integrity auditing. In their proposed system, if group key is shared by the data owner among the group users, group users need to update their key shared by data owner during revocation of any user from the group. Also, the owner of the data does not have any role in the user revocation phase, where cloud is responsible for the user revocation phase. In this case, the malicious cloud server will result in collusion of the cloud server and revoked user where the cloud server could update data number of times as designed and provide a true copy of data finally.

Due to above mentioned limitation; we propose a system which includes data encryption and decryption during the data modification processing with secure and efficient user revocation. Here, vector commitment method is proposed which will be applied over the database. Also the group signatures and Asymmetric Group Key Agreement (AGKA) that support efficient group user revocation and cipher text database update among group users respectively. The user in the group will be having rights to encrypt or decrypt a message from any other group users when the group users use the AGKA protocol to encrypt or decrypt data on the share database. The collusion of the cloud and revoked group users will be prevented by the group signature.

III. SYSTEM ARCHITECTURE

As illustrated in Fig.1, the proposed system involves three parties: the cloud storage server, the third party auditor (TPA) and users. In this system, there are two types of users in a group: the Data owner and a number of users in the group. The data owner and group users are both members of the group. Group members are allowed to access and modify shared data created by the data owner based on access control privileges.

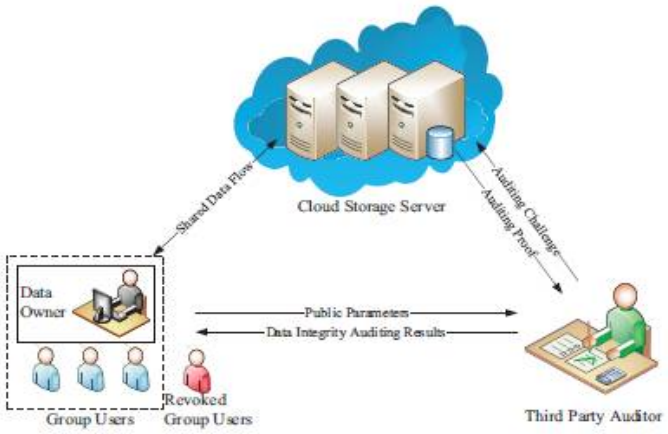

Fig.1. System Architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Data owner upload data on cloud storage server. Other users within same group can access files shared by data owner. Data owner also send request for auditing result from the Third party auditor (TPA). TPA generates auditing result for the data store on the cloud storage server and sends result to the data owner.

IV. IMPLEMENTATION DETAILS

Vector Commitment

The Vector Commitment provides a way that an adversary will be unable to explore a commitment at the same position of two different values. Vector Commitment's vector length is independent from the size of the commitment string and its openings. A vector commitment is a collection of six different algorithms.

i. **VC.KeyGen(1^k , q):** On the security parameter and the size k and q respectively it generates the outputs with some public parameters called pp.

ii. **VC.Compp(m1, ...,mq):** On input a sequence of q messages m1 to mq and by using the public parameters pp, the this algorithm outputs a an auxiliary and commitment string C.

iii. **VC.Openpp(m, i, aux):** This algorithm is used to produce a proof i that m is the ith committed message.

iv. **VC.Verpp(C,m, i,∧i). :** This algorithm is used to produce result if ∧i is the valid proof that C was created to a sequence that m = mi.

VC.Updatepp(C,m,m′,i).: This algorithm is used to produce C and wants to update it by changing the i-th message to m′. The old message m, the new message m′ and the position i is taken as input to the algorithm.

v. **VC.ProofUpdatepp(C, ∧j ,m′, i,U).:** Any user who holds a proof $\wedge_j$ for some message at position j with repect to C can run this algorithm, and then user can derive an updated proof $\wedge_j$ (and the updated commitment C′) such that $\wedge_j$ will be valid with regard to C′ which contains m′ as the new message at position i.

Group Signature with User Revocation

Some formal definitions for Group Signature presented as follow :

vi. **VLR.KeyGen(n):-**This algorithm takes n as a parameter where n is a number of group user. Its output gives group public key(gpk), n number of users keys gsk = (gsk(1),gsk(2),..,gsk(n)), n-element vector of group user revocation tokens grt=(grt(1),grt(2),…,grt(n)).

vii. **VLR.Sign(gpk, gsk[i], M):-** This algorithm takes group public key(gpk), a private key(gsk[i]) and a message M ϵ {0,1}* , and return user signature σ.

viii. **VLR.Verify(gpk, RL, σ ,M):-** This verification algorithm takes group public key gpk, a set of revocation tokens RL, and a purported signature σ on a message M input as a parameter. It returns valid or invalid result. It represent that σ is not a valid signature, or the user has been revoked who has generated it.

Asymmetric Group Key Agreement

To achieve the high degree of the data confidentiality, the user can use secret key to encrypt each data using an encryption process. The data user needs to select a random secret key and then encrypt the shared data using a symmetric encryption methods when there is only data user present in the group. However, shared secret key among group users will create a single point failure when the technique needs to handle multi-user data modification and simultaneously keeping the shared data encrypted and a. It means that any revoked group user may reveal the shared secret key that harms the confidentiality of the shared data. To overcome the mention problem, we proposed a new scheme called as an Asymmetric Group Key Agreement scheme (ASGKA). This technique proposed that, only a shared encryption key is used instead of using a common secret key in an ASGKA. Also, in the ASGKA, the public key can be used to verify signatures and at the same time encrypt messages while to decrypt cipher text under this public key any signature can be used.

V. RESULTS

The proposed system is useful to solve the security and efficiency issues of public shared data integrity auditing with multi-user modification environment, where the data has to be encrypted among a group and any user within the group can update data in secure and verifiable way. The proposed scheme provides a security against the collusion attack of the revoked users from the group and cloud storage server and in the efficient scheme.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

VI. CONCLUSION

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. Also, the proposed system is also efficient in different phases.

REFERENCES

1. Amazon. [Online]. Available: http://aws.amazon.com/s3/ Amazon. (2007) Amazon simple storage service (amazon s3)
2. Google. (2005) Google drive. Google. [Online]. Available:http://drive.google.com/
3. Dropbox. (2007) A file-storage and sharing service. Dropbox.[Online]. Available: http://www.dropbox.com/
4. Mozy. (2007) An online, data, and computer backup software.EMC. [Online]. Available: http://www.dropbox.com/
5. Bitcasa. (2011) Inifinite storage. Bitcasa. [Online]. Available:http://www.bitcasa.com/
6. Memopal. (2007) Online backup. Memopal. [Online].Available: http://www.memopal.com/
7. M. A. et al., "Above the clouds: A berkeley view of cloud computing," *Tech. Rep. UCBEECS*, vol. 28, pp. 1–23, Feb. 2009.
8. Tao Jiang, Xiaofeng Chen, and Jianfeng Ma," Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", in IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015
9. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren and Wenjing Lou," Privacy-Preserving Public Auditing forSecure Cloud Storage".
10. J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in *Proc. of IEEEINFOCOM 2014*, Toronto, Canada, Apr. 2014, pp. 2121–2129.
11. B. Wang, L. Baochun, and L. Hui, "Public auditing for shared data with efficient user revocation in the cloud," in *Proc. Of IEEE INFOCOM 2013*, Turin, Italy, Apr. 2013, pp. 2904–2912.
12. D. Catalano and D. Fiore, "Vector commitments and their applications," in *Public-Key Cryptography - PKC 2013*, Nara, Japan, Mar. 2013, pp. 55–72.
13. G. Ateniese, D. Song, and G. Tsudik, "Quasi-efficient revocation in group signatures," in *Proc. of FC 2002, Soughamption*, Bermuda, Mar. 2002, pp. 183–197.
14. Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement," in *Proc. of EUROCRYPT 2009, Cologne, Germany, Apr. 2009, pp. 153–170.*
15. D. Chaum and E. van Heyst, "Group signatures," in *Proc. Of EUROCRYPT 1991, Brighton, UK, Apr. 1991, pp. 257–265.*