Group User Revocation in Cloud for Shared Data

Mahesh Salunke, Harshal Meher, Ajay Tambe, Sudir Deshmukh,Prof.Sanjay Agarwal

Abstract— **With the excessive use of internet cloud has received much of the attention. With the help of cloud data can be easily stored on cloud and can be accessed on demand. There are issues concerning the integrity of the data which is stored on the cloud. There are many reasons for the lack of integrity like error may occur due to human errors, hardware failures , malicious users and many more. Recently some research considers the problem of secure and efficient public data integrity auditing for shared dynamic data. As lot of information is shared on the cloud it is difficult to manage this data as well as maintain its privacy. Now days we face lot of security problem in sharing dynamic data among the group users. Thus to make the sharing more secure we include the vector commitment, group signature, and asymmetric group key agreement scheme. In this we clearly present the sharing of data between the multiple group users. We also include some properties like secure group user revocation, efficiency, and count ability.**

Index Terms— **Dynamic data, cloud computing, Public integrity auditing, Group Key Agreement scheme (ASGKA), Vector commitment.**

I. INTRODUCTION

The improvement in cloud computing motivates the organization as well as outsource their data to third party cloud service providers (CSP, s) which will result in improvements the data storage limitation of local devices. In market, already some cloud storage services are available like simple storage service (S3) [2] on-line data backup services of Amazon and software like Google Drive, [3] Dropbox, [4] Mozy, [5] Bitcasa and [6] Memopal built for cloud application. But in some cases the cloud server returns invalid results such as hardware/software failure ,attack and maintenance.

Manuscript received Mar, 2016.
Mahesh Salunke *Information Technology, Marathwada Mitra Manadal's Institute of Technology, Pune ,India,7083569860.*
Harshal Meher*, Information Technology, Marathwada Mitra Manadal's Institute of Technology, Pune ,India,8793256097.*
Ajay Tambe*,Information Technology Marathwada Mitra Manadal's Institute of Technology, Pune, India, 9604777986.*
Sudir Deshmukh, *Information Technology, Marathwada Mitra Mandal's Institute of Technology,Pune,India,9011135481,*
Prof.Sanjay Agarwal,working as a professor at Marathwada Mitra Mandal's Institute of technology

User's data should be protected by data integrity because of security and privacy. To avoid the security issues the cloud storage service , simple replication and protocols sufficient for practical application.

The only and only one the data owner cloud modify the data of the cloud. The development of cloud computing some application where the services are used as a collaboration platform. In this software environments, the one or many user can share source code as well as they needs to access, compile, modify and run the code to share by any user at any time. The new model of cooperation in cloud can provides the data for the remote data, where the data owner can updates its data. The result will be in communication and computation to the data owner which contended the single point of data owner. The data integrity based on ring signature, it does not consider the user revocation problem and the cost of auditing to the data size and group size. The authenticated and private channel exist between the pair of entities and then there is no collusion. Also, the costing of audit is linear to the size of group. Also another attempt to improve the scheme and the scalable and collusion with dynamic public integrity auditing scheme with group user revocation. The schema can supports plain text of data update and integrity auditing, so it's not a cipher text data. So the data owner can share key among the user to update their shared key. Also the owner cannot take part in the user revocation, where the user revocation is work itself as a cloud.

II. RELATED WORK

To support multiple user data operation, Wang et al. [8] proposed a data integrity based on ring signature. In the scheme, the user revocation problem is not considered and the auditing cost is linear to the group size and data size. To further enhance the previous scheme and support group user revocation, Wang et al. [10] designed a scheme based on proxy re-signatures. However, the scheme assumed that the private and authenticated channels exist between each pare of entities and there is no collusion among them. Also, the auditing cost of the scheme is linear to the group size. Another attempt to improve the previous scheme and make the scheme efficient, scalable and collusion resistant is Yuan and Yu [12], who designed a dynamic public integrity auditing scheme with group user revocation. The authors designed polynomial authentication tags and adopt proxy tag update

ISSN: 2278 – 1323

techniques in their scheme, which make their scheme support public checking and efficient user revocation. However, in their scheme, the authors do not consider the data secrecy of group users. It means that, their scheme could efficiently support plaintext data update and integrity auditing, while not cipher text data. Our idea is to apply vector commitment scheme [9],[1] over the database. Then we leverage the Asymmetric Group Key Agreement (AGKA) [11],[1] and group signatures [13],[1] to support cipher text data base update among group users and efficient group user revocation respectively. With these features we will be using barcode scheme which will enhance the security of the system as the barcode can be used for login purpose and for key generation purpose as well. We will be recording the userid and its corresponding ip address for revocation or for auditing purpose.

III. PROPOSED SYSTEM

In this paper, we study the problem of public authentication inspection for shared dynamic data with group user revocation. Our contributions are:

1. In cipher text database, we explore on secure and shared data for multi-user operation.
2. An efficient data auditing scheme with new futures such as traceability and count ability by vector commitment primitives and group signature.
3. Finally the result shows that our scheme is secure. We provide the security and efficiency of our scheme which the result in back-up and the data storage on cloud.
4. Duplicate check the authorized in the hybrid cloud architecture supported by de-duplication and authorized duplicate check scheme with normal operations.
5. We can make use of barcode scheme for enhancing the security of the system , as barcode contains a unique identification element which is encrypted and can only read by barcode readers.
6. In our system the user can also download as well as upload the data which is not supported in the [1]existing system. This upload needs to be validated by the cloud admin and TPA, then data will be available for use for other group members.

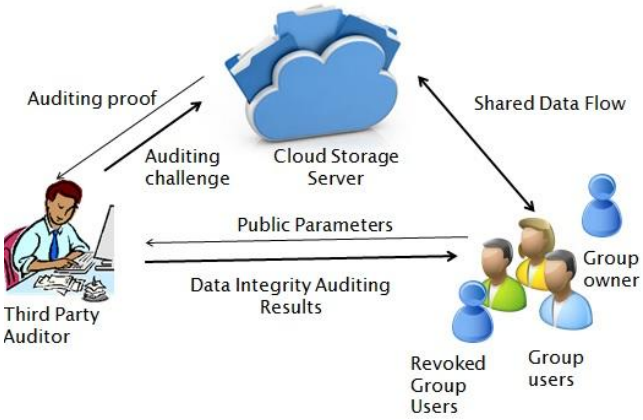

Fig 1.System Architecture

A] **File Upload**

File upload operation is performed by the data owner. The uploaded file can be accessed by the group members and then the file can be modified by the group user. But for sharing this file the group member needs to authenticate/validate the file for sharing it within the group. Once the modified file is uploaded on the cloud server by the group user, this file is then forwarded for auditing purpose. After successful auditing the file is then made accessible to the other group members.

B] **File Auditing**

File auditing the task of Third Party Auditor(TPA). According to some parameters the TPA will perform the auditing task. If TPA finds anything unusual then he has the right to revoke the particular user from that group.

C] **Re-assigning**

In this process of re-assigning the user assign the same group from which user was revoked. But for this task to be successfully completed the user should have the key which he/she used earlier.

D] **Group Sharing**

Data owner will store their data in the cloud and share the data among the group members. Who upload the data have rights to modify and download their data in the cloud. He can also set rights to other users in his group to edit or download data.

E] **Access control**

Cloud Server allows only the authorized group member to store their data in the cloud offered by cloud service providers as Sass and it won't allow unauthorized group member to store their data in the cloud.

ISSN: 2278 – 1323

F] **User Revocation**

Revocation can be done by user himself/herself or by the TPA. Once the user is being revoked from the group The group signature key in the database for the corresponding user is not removed, because if the user wishes to again join the same group then he/she has to enter the key which he/she used which enrolling in the group for the first time.

IV. SCHEMES APPLIED

1. Vector Commitment

In security protocols such as voting, identification for this the commitment fundamental primitive in cryptography it play an important role. The commitment requires the hiding property that it should not reveal information of the message and the binding property requires committing mechanism cannot allow a sender to change the mind about the message. Vector commitment can contain position binding should not be able to open a commitment to two different values at the same position that the size of the string and its openings have to be independent on vector length.

Definition 1: A vector commitment is a collection of six polynomial-time algorithms *(VC.KeyGen, VC.Com, VC.Open, VC.Ver, VC.Update, VC.ProofUpdate)* such that: *VC.KeyGen(*1*k , q)*. Given the security parameter k and the size q of the committed vector (with q =poly(k)), the key generation outputs some public parameters pp.

The problem of data outsourcing is solved by the primitive of variables database such a updates based on vector commitment.

2. Group Signature with User Revocation

We define the definition of group signatures with valid user revocation as bellow,

Definition 2. It can consist of authorized group user is a collection of three polynomial-time algorithms, which are VLRKeyGen, VLRSign and VLRVerify as follow:

VLRKeyGen(n). This algorithm takes n parameter as a input where n represent number of group user. The output of the result is in group public key(gpk),an n-element vector of user keys gsk=(gsk(1),gsk(2),....,gsk(n)),the vector of user revocation tokens grt=(grt(1),grt(2)....,grt(n)).

VLRSig(gpk,gsk[i],M). This algorithm takes group of public key(gpk),a private key(gsk[i]) and a message M.

VLRVerify(gpk,RL,M). This algorithm takes group public key gpk, set of revocation tokens RL,M as a input parameter.

3.Supporting Cipher text Database

The outsourced data is usually stored in encrypted database, in previous research. This schema is designed for auditing of both plaintext and cipher text database. This is support for encrypted database. The group consist of only one user that is data owner, then only need to choose random secrete key And encrypt the data using encryption. when it needs to support the multiuser data modification, then it is difficult to keep the shared data for encryption, so that the single point can share a secrete key among the number of user. But there is chance of leakage of shared secrete key which break the shared data. So to avoid this problem, we use scheme, which supports multi-user group modification.

4. Barcode Scheme

In java barcode scheme we use Java Barcode Decoder and Generator**.** A barcode works simply as generating a graphical design calling program specifications.

Barcode is scan using edge detection algorithm.

The barcode consists of a key value which is used as a login parameter for every user.

V. PROBLEM FORMULATION

In this section, first we describe cloud storage model of system and second we provide the threat model and also security goals:

A] **Cloud Storage Model**

Cloud storage model consist of three entities, such as cloud storage server, a Third Party Auditor (TPA) and group users. The group user can consist of data owner and user who authorised to access and the data can be

ISSN: 2278 – 1323

modified by the data owner. The group of user can provided the data storage services by the cloud storage server. The TPA can data integrity of the shared data store in the cloud server. In the remote storage cloud server the data owner could encrypt and upload its data. Also these data can access and modify and share to the number of group user.

B] **Threat Model And Security Goals**

This model consists of two types of attack:

1. The plain text of the data may be obtain by the attacker outside the group. This attacker can break the security of the group data encryption.
2. The cloud data storage server can revoked group users and then provide the data without being detected.

The cloud can make the data m' and in the user revocation it becomes valid to achieve the following security goals in this paper to overcome the problem as below:

a) Security: It should check the user authenticity by password to verify user identity. By using digital signature it should satisfy privacy certifications.

b) Efficiency: The efficiency for the any data computation as well as storage data issue can facilitated by any group user which is depend on the size of the shared data.

c) Countability: According to improper storage server of the cloud tampered with database.

d) Tracebility: In this the generation algorithm generates the data and the valid group signature, the data owner trace the last user who update the shared data.

e) Correctness: Data updated by valid group user which is supports to encrypted database by correct result.

CONCLUSION

In this the database with efficient and secure updates is way to solve the problem of verifiable data storage. We implement a scheme to realize secure and efficient auditing of data for share dynamic data with multiuser modification. In this paper, the Victor commitment algorithm helps for sharing data within the group on cloud in efficient way. Asymmetric key generation algorithm and barcode scheme adds on the security by storing the in encrypted form. The scheme vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures with user revocation are adopt to achieve the data integrity auditing of remote data.

ACKNOWLEDGMENT

We would like to express our gratitude to all those who helped us to publish this paper. We want to thank our guide Mr. Sanjay Agarwal for his continuous help and generous assistance. He helped in a broad range of issues from giving us direction, helping to find the solutions, outlining the requirements and always having the time to see us.

We have furthermore to thank Mr. S.S.Shinde, Head of the Department of Information Technology, to encourage us to go ahead and for continuous guidance. We also want to thank Mrs. Sneha Thakre for all her assistance and guidance for publishing the paper.

We would like to thank our colleagues who helped us time to time from preparing paper and giving good suggestions. We also extend sincere thanks to all the staff members of Department of Information Technology and Computer Engineering for helping us in various aspects. Last but not least we are grateful to our parents for all their support and encouragement.

REFERENCES

[1] T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," in Proc. Of IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015

[2] Amazon. (2007) Amazon simple storage service (amazon s3).Amazon. [Online]. Available: http://aws.amazon.com/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: ttp://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] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, " Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" in Proc. Of IEEE Cloud 2012, Hawaii, USA, Jun. 2012, pp. 295–302.

ISSN: 2278 – 1323

[9] D. Catalano and D. Fiore, "Vector commitments and their applications," in Public-Key Cryptography - PKC 2013, Nara, Japan, Mar. 2013, pp. 55–72.

[10] 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

[11] 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.

[12] J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in *Proc. of IEEE INFOCOM 2014*, Toronto, Canada, Apr. 2014, pp. 2121–2129.

[13] D. Boneh and H. Shacham, "Group signatures with verifier local revocation," in *Proc. of ACM CCS*, DC, USA, Oct. 2004, pp. 168–177.

Mahesh Salunke currently persuing BE in Information Technology,at Marathwada Mitra Manadal's Institute of Technology,

Harshal Meher, currently persuing BE in Information Technology,at Marathwada Mitra Manadal's Institute of Technology,

Ajay Tambe, currently persuing BE in Information Technology,at Marathwada Mitra Manadal's Institute of Technology,

Sudir Deshmukh, currently persuing BE in Information Technology,at Marathwada Mitra Manadal's Institute of Technology,

Prof.Sanjay Agarwal,working as a professor at Marathwada Mitra Mandal's Institute of technology

ISSN: 2278 – 1323