

Secured Shared Dynamic Cloud Data with Group User Revocation

Yedulla Surender Reddy

M.Tech, Computer Science & Engineering

Sri Indu Institute of Engg. & Tech, Sheriguda (Vi), IBP (M), RR Dist.

M. Ajay Kumar

Assistant professor, Department of CSE

Sri Indu Institute of Engg. & Tech, Sheriguda (Vi), IBP (M), RR Dist.

Dr. I. Satyanarayana

PRINCIPAL

Sri Indu Institute of Engg. & Tech, Sheriguda (Vi), IBP (M), RR Dist.

Abstract: With the immoderate use of web cloud has got much of the awareness. With the aid of cloud data will also be conveniently stored on cloud and can also be accessed on demand. There are issues related to the integrity of the data which is saved on the cloud. There are various factors for the dearth of integrity like error may arise due to human errors, hardware disasters, malicious clients and many extra. Not too long ago some research considers the predicament of comfortable and effective public data integrity auditing for shared dynamic data. As lot of data is shared on the cloud it's tricky to manipulate this data as good as hold its privacy. Now days we face lot of protection quandary in sharing dynamic data among the group users. As a consequence to make the sharing more comfortable we incorporate the vector dedication, team signature, and asymmetric staff key agreement scheme. In this we certainly present the sharing of data between the multiple team users. We additionally include some homes like secure team user revocation, efficiency, and depend potential.

Key Words: Dynamic data, cloud computing, Public integrity auditing, Group Key Agreement scheme (ASGKA).

I. INTRODUCTION

The improvements and enhancements in cloud computing motivates institution as well as agencies to outsource their data to third party authority cloud service providers (CSP's) a good way to outcomes in upgrades the data storage obstacle of useful resource constrain neighborhood instruments. In market, already some cloud storage offerings are to be had like simple storage service (S3) [1] online data backup services of Amazon and software like Google drive, [2] Dropbox, [3] Mozy, [4] Bitcasa and [5] Memopal built for cloud application. In some cases cloud server someday

returns invalid outcome corresponding to hardware/program failure, malicious attack and human maintenance. Security and privateness of cloud person's data will have to be covered by way of data integrity and accessibility. To overcome the security problems of at present's cloud storage services, easy replication and protocols like Rabin's data dispersion scheme usually are not adequate for useful software.

For achieving the integrity and availability of remote cloud storage, some various options and their extraordinary variations were proposed. In these options, when a scheme supports amendment of data, it is referred to as dynamic scheme, in any other case static one. A scheme is publicly verifiable that suggests the integrity examine of data may also be performed not most effective by means of data owners, but in addition by using the third party auditor (TPA). However, the focal point of the dynamic scheme is on the cases the place only and only data proprietor might alter the data of cloud. Lately, the development of cloud computing emerged some purposes the place the services of cloud can be used as a collaboration platform. In these application progress environments, one or a couple of (a couple of) clients in a bunch must share supply code as well as they wishes to access, assemble, regulate and run the source code share with the aid of user at any time. The new model of cooperation community in cloud presents the infeasibility of data for auditing the remote data, the place handiest the data owner can replace its data. It'll effect in exquisite communication and computation to the data proprietor which causes the one factor of data owner. To gain multiple data

operation, Wang et al. Put forth data integrity situated on ring signature. Within the scheme, it does not forget the user revocation problem and the rate of auditing is linear to the data dimension and staff measurement.

To additionally raise up the prior scheme and aid staff person revocation, Wang et al. Proposed a scheme based on proxy re-signatures. However, this scheme assumes that authenticated and private channels exist between the pair of entities and there's no collusion among them. Also, cost of auditing the scheme is linear to the scale of the staff.

An extra try and toughen the prior scheme and make the scheme scalable, efficient and collusion resistant, Yuan and Yu designed a dynamic public integrity auditing scheme with workforce user revocation. However, of their scheme, the authors don't take into account the secrecy of data among the group users. That implies, their scheme could efficiently help undeniable textual content of data update and integrity auditing, whereas now not ciphertext data. Of their scheme, if data proprietor shares group key among the clients of group, revocation of any team user enable the workforce users to update their shared key. Also, the owner of the data does no longer take part in the user revocation segment, the place the user revocation section is itself performed by way of the cloud. In this case, the malicious cloud server will effect in collusion of revoked user and the cloud server where the cloud server might update data number of instances as designed and furnish a authorized data subsequently. Due to above acknowledged deficiency; we propose a building which entails data encryption and decryption for the duration of the data change processing, secure and effective user revocation and in addition removal of redundant data. Here, vector commitment scheme can be utilized over the database. Then we practice the asymmetric group Key agreement (AGKA) and group signatures to support ciphertext database replace amongst team users and effective team person revocation respectively.

The user within the staff will be ready to encrypt or decrypt a message from another workforce clients when the workforce users use the AGKA protocol

to encrypt or decrypt the share database. The collusion of the cloud and revoked team clients will likely be avoided by the staff signature. user's data.

II. RELATED WORKS

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 pair 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 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.

III. PROPOSED METHOD

In this paper, we gain data of the predicament of public authentication inspection for shared dynamic data with staff user revocation. Our contributions are:

1. In cipher textual content database, we discover on comfortable and shared data for multi-user operation.
2. An effective data auditing scheme with new futures reminiscent of traceability and count ability by using vector commitment primitives and group signature.
3. In the end the outcome shows that our scheme is comfortable. We provide the safety and efficiency of our scheme which the outcomes in back-up and the data storage on cloud.
4. Reproduction investigate the licensed in the hybrid cloud architecture supported via de-duplication and licensed replica verify scheme with ordinary operations.
5. We will make use of barcode scheme for enhancing the protection of the system, as barcode involves a certain identification element which is encrypted and might best read by means of barcode readers.
6. In our approach the person may download as well as add the data which is not supported in the [1]current procedure. This upload needs to be validated via the cloud admin and TPA, then data can be to be had to be used for other group participants.

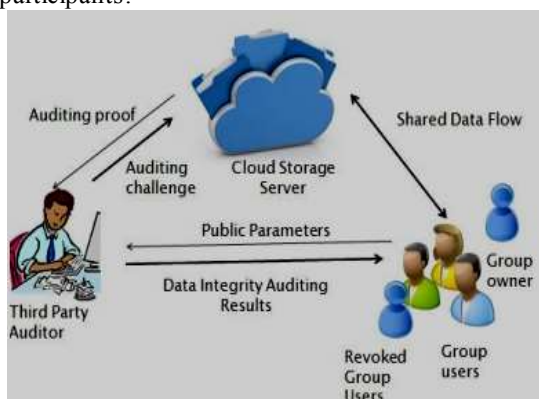


Fig 1. System Architecture

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 SaaS and it won't allow unauthorized group member to store their data in the cloud.

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.

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, VLRSig 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 $gsk=(gsk(1),gsk(2),\dots,gsk(n))$, the vector of user revocation tokens $grt=(grt(1),grt(2),\dots,grt(n))$.

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.

IV. CONCLUSION:

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

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: <http://www.dropbox.com/>
- [5] Mozy. (2007) An online, data, and computer backup software. EMC. [Online]. Available: <http://www.dropbox.com/>
- [6] Bitcasa. (2011) Infinite 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. 295–302.123.
- [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.

Author's Profile



Yedulla Surender Reddy pursuing M.Tech in Computer Science Engineering from **Sri Indu Institute of Engg. & Tech, Sheriguda(Vi), IBP(M),RR Dist.**



M. Ajay Kumar working as Assistant professor, Department of CSE in **Sri Indu Institute of Engg. & Tech, Sheriguda(Vi),IBP(M),RR Dist.**



Dr. I. Satyanarayana Completed B.E-Mechanical Engg. from Andhra University, M.Tech Cryogenic Engg. Specilization-IIT Kharagpur, Ph.D-Mechanical Engg.-JNTUH, Currently working as an Principal at **Sri Indu Institute of Engg. & Tech, Sheriguda(Vi), IBP(M),RR Dist.**