International Journal of Research

Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation

[1]Mrs. K.PRASANTHI, [2] Mr. P.GIRIDHAR

[1] M.Tech(CSE) from Jagruti Institute of Engineering and Technology
[2] Assistant Professor, Department of Computer Science and Engineering,
Jagruti Institute of Engineering and Technology , Telangana State, India.

Abstract: Cloud computing is the protracted revelation of computing as effectiveness, where data owners can remotely store their data. The essential service presents by the Cloud is Data Storage. On the other hand, it is a tricky task for sharing data in multi-owner manner anywhere group admin and all group members can store and alter data while protecting data and identity privacy from an untrusted cloud server, due to the frequent change of the membership. So secure multi-owner data sharing scheme for dynamic groups in the cloud computing have been projected which absorb addition of group signature and broadcast encryption techniques. However this system also recognized some boundaries in terms of competence and security. since multi-owner data storing and sharing in a dynamic surroundings dumps enormous amount of data files in the cloud, which leftovers in cloud for imprecise period of time. The confidential information stored may changed by service providers. To maintain cloud file's security and privacy regular elimination of unwanted files is needed. To determine this drawback we propose new framework which is Reliable and Scalable Secure Method to Store and Share Secrete Data for groups in Cloud i.e MONA that remove unnecessary files automatically when the predefined time period for sharing specified by data owner has been run out which improve performance of the system in terms of security and efficiency. Also this method decreases the overhead at the time of upload and download file in the cloud. At last proposed method by name Multi Owner Data Sharing Over Cloud (MODOC) declares required efficiency and most importantly security. We apply a working prototype of the MODOC method and assess its performance based on the time addicted during various operations The results give you an idea about that MODOC has the prospective to be effectively used for secure data sharing in the cloud.

Keywords – Dynamic group, group signature, dynamic broadcast encryption, data sharing, privacy-preserving.

1. INTRODUCTION

Cloud computing based solutions are becoming well-liked and adopted extensively because of its low-maintenance and commercial uniqueness. With the help of authoritative data centers it is possible for cloud service providers (CSP) to express various services to cloud users on demand. The Cloud server usually store data in very lower cost and makes it available for 24 hours over the internet Cloud [5]. For e.g. Company allows its staffs in the same group or department to store and share records in the cloud. Company saves significant investment on their local infrastructure by utilizing the cloud. But these data application in the cloud storage is inattentive by some security issue such as data leakage because cloud service providers are not completely trusted especially, when highly sensitive and confidential data stored in the cloud such as medical records, business plans etc. As a result security and privacy have always been very important aspects in cloud Computing. A basic clarification provided by existing system to keep responsive user data confidential against untrusted server is encrypting the data files, before uploading into the cloud server. However unfortunately scheming a secure and efficient cloud data sharing scheme for active groups in the cloud is not simple task because of the some difficult issues.

1.1. Identity Privacy

The major issue for the wide selection of computing is Identity Privacy. Cloud clients may unsure to join cloud based figuring frameworks without the evidence of character security in illumination of the fact that if client protection is not kept up legally then the real personalities

of the client can be reveal effortlessly to the different sorts and cloud administration suppliers (CSP).

1.2 No Multiple-Owner Manner

Multiple-owner manner is more flexible than single owner manner as multiple owner manners permit every member in the group should be capable to alter their own data i.e. Each part will be ready to examine the information as well as adjust the piece of information in the whole information document, though single owner way permit just Group Admin to store and alter information in the cloud and individuals can just read the information.

1.3 Effect of Dynamic Groups

The combination of new staff and revocation of current member of staff makes the group active in nature. The common variations of membership make capable and secure data sharing in Cloud very complex and hard due to the next two primary reasons: First, new decide users not approve to learn the content of data files stored before their contribution by the unspecified system, since it impossible for new approved users to openly contact with data owners and get the matching decryption keys. Second, to decrease the difficulty of key management, it is necessary to get an efficient membership revocation mechanism without updating the private keys of the remaining users.

There are more than a few security methods that have been planned up-to-date for capable and secure data sharing on untrusted servers. In all of these the encrypted data files are stored in untrusted storage and allocate the matching decryption keys only to approved users by the data owners. But, the issues of user revocation and multiple-owner manner have not been addressed very efficiently.

2. OBJECTIVE OF THE PROPOSED WORK

To solve these problems we propose MODOC, a secure multi-owner data sharing over cloud. The main objective of this paper includes:

i)To implement secure multi-owner data triming scheme which is capable to maintain dynamic group efficiently. It implies that any group member able to store and share data file by untrusted cloud as well as new user joining and user revocation are easily attained without relating remaining users.

ii)To supply secure and privacy-preserving access control to users, this assures any member in a group to secretly make use of the cloud resource. It means that group members can right to use the cloud without enlightening the real identity.

iii) To progress search effectiveness and decrease storage overhead.

iv) To give a protected way for key distribution.

3. LITERATURE REVIEW

Literature review is the most vital step in software development process. Subsequent is the literature review of various existing methods for data sharing in the cloud.

In 2007 C. Delerablee [7] initiated new efficient creation for public-key transmit which propose stateless receivers, collusion-secure encryption, and high security. in the regular model; latest users can join anytime without involving any alteration of user decryption keys or eternally cancel any group of users. This system attain the finest clearity of O(1)-size either for cipher texts or decryption keys, also provides a dynamic transmit encryption system civilizing all earlier efficiency measures (for both execution time and sizes) in the private-key setting.

In 2010 Lu et al. [3] projected secure derivation scheme which records ownerships and process history of data object. This method is based on the bilinear pairing methods which rely upon group signatures and cipher text-policy attribute based encryption (CP-ABE) methods. The basic aspect of this scheme is to present the unknown authentication for user accessing the files, information privacy on sensitive documents stored in cloud and tracking the origin on unclear documents for revealing the identity. primarily, the system includes of a single attribute. After the registration, each user in this scheme gets two keys: a group signature key and an attribute key. Using attribute-base encryption (ABE) any user can encrypt a data file. For decryption of the encrypted data, an attribute keys is used by other in the group. To achieve privacy preserving and traceability features, the user signs encrypted data with group signature key. Regrettably, the drawback of this scheme is that user revocation is not supported.

In 2010 Lan Zhou et al. [2] projected a scalable and fine-grained data access control scheme by defining access polices based on data attributes and KP-ABE technique. The arrangement of attribute-based encryption (ABE), proxy re-encryption and lazy re encryption allows the data owner to allocate the calculation tasks to untrusted server without enlightening the necessary contents of data. Data files are encrypted using random key by data owner. Using key policy attribute-based encryption (KP-ABE), the random key is further encrypted with a set of attributes. Then the approved users are assigned an access formation and matching secret key by the Group Admin. Hence, only the user with data file attributes that gratify the access structure can decrypt a cipher text. This system has some drawback such as multiple-owner manner is not maintained by this system so that those single owner

manners make it less flexible as only Group Admin are answerable for altering the data file shared. And user secret key required to be simplified after each revocation.
In 2012 B. Wang et al. [6] payed attention on cloud computing and storage services, data is not only stored in the cloud, but regularly shared among a large number of users in a group. In this paper, they propose Knox, a privacy-preserving auditing method for data stored in the cloud and shared among a large number of users in a group. In exact, the utilize group signatures to construct homomorphic authenticators, so that a third party auditor (TPA) is capable to confirm the integrity of shared data. For the time being, the characteristic of the signer on each block in shared data is kept private from the TPA. The original user can capably add new users to the group and reveal the identities of signers on all blocks. With Knox, the amount of information used for confirmation, as well as the time it takes to audit with it, are not exaggerated by the number of users in the group.
In 2013 Xuefeng Liu et al [1] planned new technique "MONA". This method explains the design of secure data sharing scheme for dynamic groups in an untrusted cloud which occupy integration of group signature and transmit encryption techniques. This technique sustain dynamic group i.e. User can be withdraw easily through revocation list without updating left over users and as well as new user can decrypt data file without make contact with the data owner. consequently size and computation costs of encryption are autonomous with the number of revoked users. This system recognized some boundaries in terms of efficiency and security. In addition in revocation list the time given for each user is set after time expire user cannot access the data until Group Admin update the revocation list and give it to the cloud.
In 2013 Yong CHENG et al [4] planned a security for customers to store and share their responsive data in the cryptographic cloud storage. It offers a basic encryption and decryption for providing the security and data confidentiality. On the other hand, the cryptographic cloud storage still has some shortcomings in its presentation. Initially, it is incompetent for data owner to allocate the symmetric keys one by one, especially when there are a huge number of files shared online. Secondly, the access policy revocation is much in cost, for the reason that data owner has to recover the data, and re-encrypt and re-publish it. The first difficulty can be resolved by using cipher text-policy attribute-based encryption (CP-ABE) algorithm. To optimize the revocation process, they present a new efficient revocation system. In this system, the original data are first separated into a number of slices, and then published to the cloud storage. When a revocation takes place, the data owner requires only retrieving one slice, and re-encrypting and re-publishing it. Therefore, the revocation process is affected by only one slice as a replacement for of the whole data.

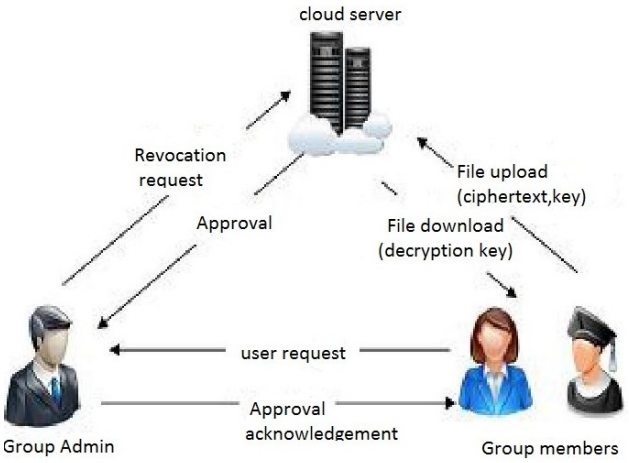
4. PROPOSED SYSTEM

The evaluation of literature has exposed that efficient and protective data sharing in cloud computing is still to be a demanding issue.
To resolve these issues, we recommend a new framework by name MODOC for secure data sharing in cloud computing by joining group signature and transmit encryption methods. In this method we are presenting how to direct risk in strongly sharing data among multiple group members. Evaluating to existing work our proposed system offers some exclusive characteristics such as
i) Provide tough security which is essential to store and preserve confidential data.
ii) Provide security against different attacks at the client side.
iii) This system offers exact security using encryption technique.
iv) This system maintains dynamic group professionally. It involves that new user joining and user revocation are easily attained without involving remaining users.

The system model includes three different entities:
i)A Group Admin (i.e., Admin)
ii)A large number of group members.
iii) The cloud server

Group Admin: The Group Admin will be notified by the administrator of the company. For that reason we take for granted that the Group Admin is completely trusted by the other parties. Group Admin carry out a variety of functions such as system parameters generation, user registration,

Figure 1:



group creation, assign group signature, generation of private key using bilinear mapping and assign to the requested user, sustain revocation list and transfer this list into cloud for public use, and traceability.

Group Members: Group members are collection of registered users who will store their confidential/personal data into the cloud server and distribute them with others in the group. Both Group Admin and group member can login using their login details. After successful login, Group Admin make active newly added members of the cloud by producing keys for each member using bilinear mapping and throw it to the corresponding group members. They can also check the group particulars, and assign group signature. After successful login, Group Members signature is verified. After successful confirmation, the member can upload, download and can alter the files. Group member must be encrypting data files before uploading to the cloud. The Group Members account can be revoked after he leaves the cloud by the Group Admin.

Cloud Server: Cloud is the bulky storage area of resources. Cloud is answerable for storing all users' data and surrendering access to the file within a group to other group members based on publically available revocation list which is preserving by Group Admin. We take for granted that the cloud server is truthful but curious. To be exact, the cloud server will not unkindly delete or modify user data, due to the protection of data auditing schemes

User Registration: After successful creation of cloud setup, users require to get registered with the system through user registration process. While registering, users need to present their personal details for achievement of registration process. User registered with their details such as identity (user name, mobile no and email-id). During registration process, user got single identity and access structure. This produces secret key for the members. For registered users they will get private key, that private key is used file encryption and decryption.

User Authentication: The user can login effectively only if user id and password are mention correctly. The login will fails if the incorrect user id or wrong password is entered by the user. This helps in stopping unauthorized access.

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

User Revocation: User revocation is the procedure of eliminating of user from system user list which is carry out by group admin. Group admin can openly revoke multiple users during public revocation list at any time without disturbing any non revoked user. If the login identification of the specified user equals with the particulars of revocation list then access denied.

File Upload: File upload is the procedure of storing particular data files into the cloud for sharing in the group. An uploaded file resides in the cloud up to the time specified while uploading the file. Before uploading the file, file has to be encrypted and compressed to ensure security and privacy of the files. Then it is summarize with equivalent decryption key and time to live (ttl) value for the file and send it to cloud.

File Download: To access the data that are stored in the cloud, group member will give request as group id, data id. Cloud server will confirm their signature, if the group member in the same group then agrees to the access file. Group member have rights to access data, but not have rights to erase or modify the data that are stored in the cloud.

File Deletion

In view of the fact that the system itself by design eliminate the shared files if time specified during upload process will expire. Therefore proposed system does not necessary open deletion mechanisms.

5. Mathematical Model

Let T is the main set described below.

MODOC = {S1, A1, U1, F1, GS, K1, ttlf, RL1, Es, SD }

Where,
S1 = Start state i.e. Establishing connection between client and cloud server,
A1 = Group Admin who create group and add members into Group.
U1 = User called as registered group member.
F1= File that user want upload on the cloud server and share within group.
K1 = Private key of each group members.
GS= Group signature assigned by group admin.
ttlf = time to live of the uploaded file.
RL 1= is the revocation list maintained by group admin.
DE F= Encrypted data file.
SD= is the copy of the server database.
Es = End state.i.e User query ran successfully on encrypted database and user get the accurate result in minimum time.

Functionality

A1 = Create(GS, K1)
U1 = Register(uid , password)
RL1 = RevocationList(GSID, MID)
DEF = Ek(F1)
SD = StoreData (DEF, RL1, ttlf)

5. METHODOLOGY

6.1 Dynamic Broadcast Encryption

The dynamic Broadcast Encryption [7] techniques enabling the group manager to dynamically add new user and at the same time preserves the previously computed information. That is, newly joining users can directly decrypt data files without contacting with data owners. So that there is no need to update user decryption keys.

5.2 Group Signature

Group Signature will be used to achieve privacy of group member against potential verifiers. Group signature scheme allows any group member to issue a signature on behalf of the whole group [10]. Any verifier can publicly check the validity of this group signature using the group public key. The important property of group signatures is that the group manager can open group signatures and identify their signers using the information collected during the admission process when a dispute occurs, which is denoted as traceability. Thus as compare to ordinary digital signatures, group signatures have provide extended security.

6. RESULT AND DISCUSSION

6.1 Security Analysis

Table 1: Security performance comparison

	Secure key distribution	Access control	Secure user revocation	Anti-collusion attack	Data confidentiality
RBAC scheme		√			
Mona	√	√			√
Proposed scheme	√	√	√	√	√

since evaluated with Mona planned scheme can accomplish secure key distribution, security from collusion attack and secure user revocation.

7.2 Performance Analysis

We evaluated the MODOC style on the foundation of the total time inspired to upload and download a file to/from the cloud. The entire time is collected time from the time of submission of request to the cloud server to the point of time at which the file is uploaded/downloaded to/from the cloud.

Table 2: Comparison of Turnaround Time

File Size (KB)	MONA		MODOC	
	Upload	Download	Upload	Download
148	12.9	11.6	12.4	7.5
520	35.8	40.3	34.3	33.6
876	66.6	68.1	64.6	44.4
1050	80.1	84.6	77.2	50.8
1516	98.8	121.5	81.9	51.5

The above Table 2 reveals the turnaround times for upload and download. In regular, the time to upload and download the data improved with the raise in the file size. This table reveals that the MODOC technique outperforms the existing techniques MONA outstanding to the lack of profound calculations and memory transparency.

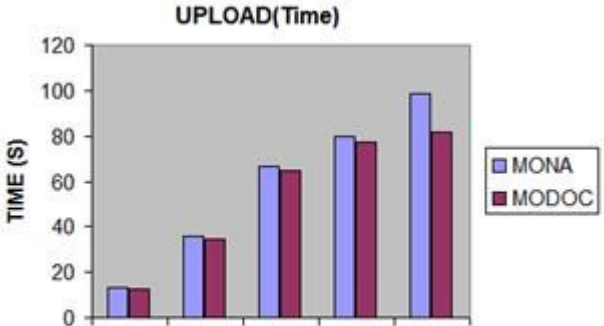


Figure 2: Performance of File Upload.

Figure 2 demonstrates consequences for upload time. X axis signifies the file size and Y axis signifies the time. In existing system MONA 1.5mb was uploaded in 98.8s, where as in proposed system MODOC it takes 81.9s to upload a 1.5mb file. This graph obviously shows that as evaluate to the existing system the performance of proposed system is higher.

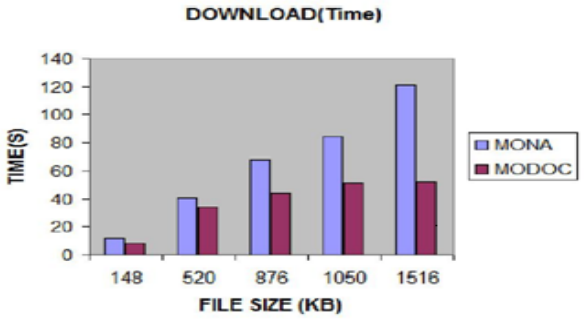


Figure 3: Performance of File Download.

Figure 3 demonstrates the result for download time. X axis symbolizes the file size Y axis symbolizes the time. In existing system MONA 1.5mb was downloaded in 121.5s, where as in proposed system MODOC it takes 51.1s to upload a 1.5mb file. The graph obviously explains that as compare to the existing system the presentation of proposed system is higher.

7. CONCLUSION

This paper gives a note that a cloud information distribution plan assuring security for regular modification of enrollment which consists of the mix of assembling signature and element telecast encryption systems. Proposed framework supports different clients to distribute basic information over the individuals and every part can include in information elements. Framework offered in this paper is able to give highlights like security and protection saving access control, insignificance and traceability. This framework gives high security and ability. As a result planned framework maintains required output, security and adaptability.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions On Parallel and Distributed Systems, Vol.24, No. 6, June 2013.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[3] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of /Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[4] Yong CHENG, Jun MA and Zhi-ying "Efficient revocation in cipertext-policy attribute-based encryption based cryptographic cloud storage" Zhejiang University and Springer-Verlag Berlin 2011

[5] Prasad et al., International Journal of Computer Engineering In Research Trends, Volume 2, Issue 10, October-2015, pp. 889-895

[6] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53,no. 4, pp. 50-58, Apr. 2010.

[7] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[8] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and

[10] Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[11] D. Boneh, X. Boyen, and H. Shacham, Short Group Signature, Proc. Intl Cryptology Conf. Advances in

Cryptology (CRYPTO), pp. 41-55, 2004.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

ABOUT THE AUTHORS

Mrs. K.PRASANTHI is pursuing M.Tech degree in, Computer Science and Engineering from Jagruti Institute of Engineering and Technology, Telangana State, India.

Mr. P.GIRIDHAR, presently working as Assistant Professor in, Department of computer science and engineering, Telangana State,India.