Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (135-139), Month: January-April 2016, Available at: www.noveltyjournals.com

Data Integrity and Efficient User Revocation for Dynamic Groups in the Cloud

Ms. R. Arthi[1], Ms. R. Jeevitha[2], Ms. S. Keerthanalakshmi[3], Mr. R. Sivaramakrishnan[4]

[1 2 3]UG Scholar, [4]Assistant Professor, Department of Computer Science and Engineering KPR Institute of Engineering and Technology- Arasur, Coimbatore

Abstract: **Cloud computing is the way of sharing the computer resource over the Internet and hence it is termed as the Internet based computing. But the problem with cloud is that many user store their data in cloud it has some security issues like collusion attack, loss of data. In existing system, they used the concept of user revocation to secure the data and to avoid collusion of the data using ECC algorithm which uses elliptical equations and complex calculations. In proposed system, we are using AGKA(Asymmetric Group Key Agreement) algorithm for encryption and decryption. For efficient user revocation we are using verifier local group signature method. And to maintain the integrity of the data TPA (Third Party Auditor) is used for checking the data. Our scheme provide some properties, such as confidently, efficiency, countability and traceability of secure group user revocation. Finally our scheme achieve the integrity and security.**

Keywords: **Group signature, Third Party Auditor, AGKA, Key generation, User revocation.**

I. INTRODUCTION

Cloud computing is the technology that provides scalability, efficiency and it deliver the resources over the Internet. It provides the information to the end to end user whenever and wherever they needed. Many users store their important data in the cloud, security risks may occur in this. So it is important to provide more security and data should not modified. Cloud provide unlimited storage and cost effective.

There are 2 types of model are there:

1. Deployment model- It define the type of access to the cloud, i.e. how the cloud is located? Cloud can have any of the four types of access: Public, Private, and Hybrid.

2. Service model- It reference models on which the Cloud Computing is based. There are 3 categories are there. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

Deployment model

1. Public cloud- It allow services to easily accessible to the general public. This may cause less secure because it is open to all. Ex: e-mail.

2. Private cloud - It allow the users to access the data with that organizations or with in that group. It offers increased security because it is private.

3. Hybrid cloud - It is mixture of public and private cloud. It provide scalability, security, flexibility.

Our proposed system is to maintain the integrity of data and user revocation part. In the Dynamic group due to frequent change of membership privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Revoked user means user removed from the cloud. In order to protect from collusion attack revoked user should not get the data. For efficient user revocation we are using group signature by this collusions are avoided. To maintain the integrity of data we are using TPA. TPA checks the data stored in the cloud whether any modification occurred in that data.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (135-139), Month: January-April 2016, Available at: www.noveltyjournals.com

II. LITERATURE SURVEY

When there is a multi owner environment sharing the data between the user is a challenging issue,because of the frequent change in the membership. To secure this *Xuefeng Liu et.al proposed* a multi owner data sharing scheme with the concept of group signature [1] and dynamic broadcast encryption techniques. In this group signature scheme,a signature is been sent along with the message using that signature we can identify the user,who has sent the message, which brings traceability in them. Broadcast encryption works fast and the calculations are done using simple symmetric encryptions and it involves three steps like setup,broadcast and decrypt. The advantages of this will be,without participation in the cloud any user can decrypt the files and without updating the key user revocation is performed.

In the existing system, user cryptographic method for viewing the data by decrypting it to authorize the user was used. By doing this, introduces heavy computational overhead on the data owners during key distribution. So, *L.Zhou et.al proposed* a method to address this challenge by using the techniques like attribute based encryption(ABE)) [2],proxy(PRE) and lazy re-encryption. ABE are associated with attribute for each and public key is defined . Encryptor uses these attribute information in the message for encrypting the message. PRE converts cipher text encrypted under public key into another cipher-text that can be opened by private key without viewing the underlying plain text. It also provides confidentiality and accountability property. And key generation algorithm is used in this scheme and hence it provides high efficiency.

The data stored in untrusted cloud may get the security issues one user place their data in the stored system, multiple users read and update the same data. By this actual owner of the data may not be known. So, *Kallahalla et.al proposed* a method plutus. It is cryptographic storage by this files can be shared security in the untrusted cloud. In this they are using the prototype openAFS [3], this achieves the security. In this paper plutus provide security features to detect and prevent unauthorized data modification, handle the user revocation, distinguish read and write access. Instead of encrypt and decrypt file each time over the network plutus that encrypt the data when data is updated, decryption cost is distributed among separate users

However sharing the data in the public cloud leads to leakage of data. Confidentiality of the data and preserving the privacy of users is difficult *E.Bertino et.al proposed* a method of privacy preserving policy-based content sharing in public cloud. For this a new key management scheme, called broadcast group key management (BGKM)[4] is used in this paper. The idea is to give some secrets to users based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets and some public information. The advantage of the BGKM scheme is that adding users/revoking users or updating can be performed efficiently by updating only some public information.

III. SECURING COLLUSION ON DYNAMIC CLOUD GROUPS IN THE CLOUD

Sharing the data in the cloud will be insecure because of the frequent change in the membership due to collision attack. so, in the existing system to avoid collusion they used secure way of key distribution without using secure communication channel and the private key is issued by the manager for each and every user. In this scheme any user in the group can access the cloud and even if the revoked user cannot access the cloud and even if the revoked user are there in the untrusted cloud they cannot get the original data files. Finally, if the user enters are removed from the cloud, it is necessary to update the private keys. In this system they have used the algorithm called ECC, Elliptical Crystal Cryptography which uses the graph for representing a problem. Since it deals with complex mathematical operations, then it is tedious.

A. EXISTING USER REGISTRATION:

If the user needs to join in a group, the group manager only add or remove the user in the group. For that, the user should give their identity, public key, account user and random number to the Group Manager. For each and every user have an identity and public key. Random number is used to indicate how many times the manager and users are communicating. Account user is used for to pay for registration. For the user response, manager will send some acknowledgement. After that, the private key which is distributed to the user from the group manager and then user can be used for the data sharing. Simultaneously,the manager will update the group user list.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (135-139), Month: January-April 2016, Available at: www.noveltyjournals.com

B. TO UPLOAD A FILE:

If the user wants to upload the data, along with the data file some parameters need to be sent. The message should be in the encrypted format. The parameters are id i.e) for each user have a unique data file, then time stamp value has to be sent to the manager and then manager will upload into the cloud.

C .USER REVOCATION:

The manager will perform the user revocation. If the user is going to revoke, first update to the manager. The manager will perform some operations like polynomial function and remove it in cloud. Then, the user is removed from the group, private key is removed and group user list is updated in cloud.

D. TO DOWNLOAD THE FILE:

If the user to download a file some verification has to be done. The user will send the group identity , identity of the user, encrypted format with his identity of an data. Then cloud will check the user list .if the verification is clear then only they can decrypt the data.

E. NEW USER REGISTRATION:

The new user is going to register, it performs same operation like an existing user.

IV. USER REVOCATION AND INTEGRITY CHECKING IN CLOUD

In order to provide a security against collusion attack in cloud, the user revocation is done effectively by using the group signature method. To show the integrity of data TPA (Third Party Auditor) is used.

The group user uses the AGKA (Asymmetric Group Key Agreement)[5] protocol to encrypt/decrypt a message. The algorithm works as follow:

Setup: The group controller X generates the parameters. Then X generates tuple $Y = (G_1 , G_T , e , H , g , q)$. X chooses the cryptographic hash function $H=\{0,1\}_* \rightarrow G_1$ where $G_1$is a group with prime order q, e: G_1 X $G_1 \rightarrow G_T$ is a bilinear map and g is the generator of G_1. Then generate public key P_UK, Private key PK_i to the each user in the group.

Key establishment: In order to communicate with each user the message should be in Encrypted and Decrypted form. Let $Y_1, Y_2, \ldots Y_n$ are the users in the group. Each user has a identity ID_i for $1 \leq i \leq n$ in the group, following steps are performed:

1. Choose any value $h_i \epsilon G_1$, $r_i \epsilon Z_q$ then compute $X_i=g^{ri}$, $A_I=e(H(IDi)+h_i,g)$
2. For $1 \leq j \leq n$, compute $\Omega_{i,j}=h_i * H(ID_j)^{ri}$
3. Then signature β_i is generated on $X_i$using PK_I
4. Publish $(X_i A_I \beta_i ID_i)$ to all the users.

Encryption key derivation:

- for group encryption we need the parameters(P,Q,R)
- where $P = \prod_{i=1}^{n} x_i$, $Q = \prod_{i=1}^{n} A_i$, $R = \prod_{i=1}^{n} H(ID_i)$

If the message signature pair $(x_1,\beta_1) \ldots (x_n, \beta_n)$ is valid the encryption key is generated.

Encrypt format:

After knowing encryption key parameters then message m can be encrypted:

- Select a random number b € z_q
- Compute variable $C1=g^b$, $C2=W^b$, $C3=m*A^b$
- Send C(cipher text)=(C1,C2,C3) to the receiver.

Decryption key derivation:

Novelty Journals

ISSN 2394-7314

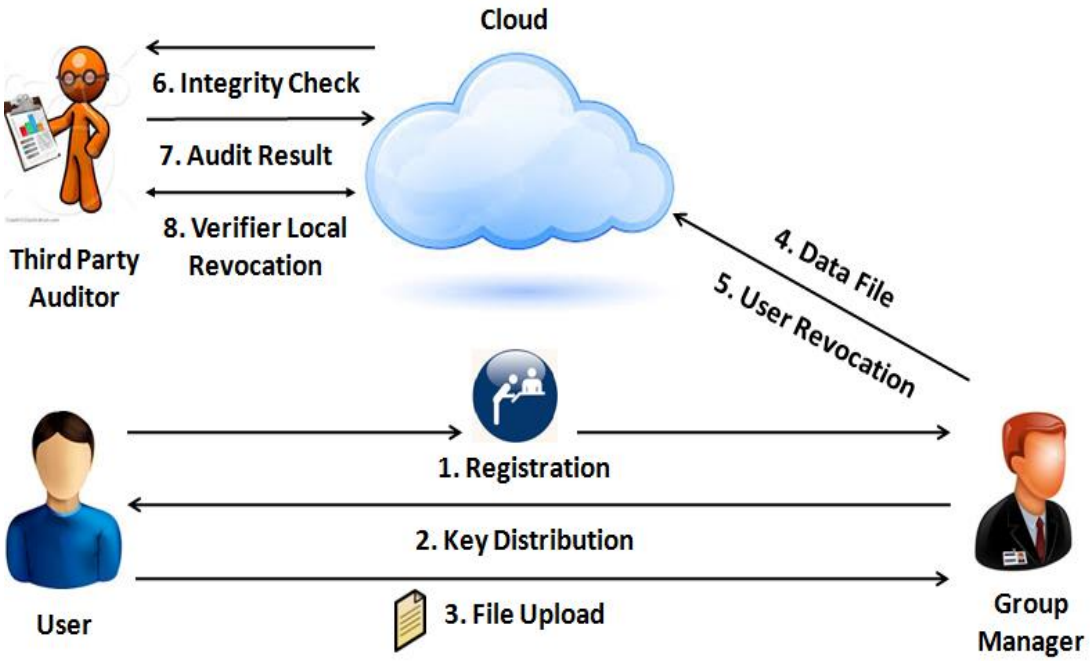
International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (135-139), Month: January-April 2016, Available at: www.noveltyjournals.com

- Decryption key $D_i=\prod_{l=1}^{n}\Omega_{i,j}$, If the message signature pair $(x_1, \beta_1)\ldots (x_n, \beta_n)$ is valid the decrypted key is generated

Decrypt Format:

Here the encrypted text get decrypt by $m = C3/(e(D_i,C1)*e(Q,C2)*e(H(ID_j)^{-1},C2))$

Group Manager will take part in the user Revocation phase[6]. In verifier local group signature scheme 3 process are there: Key Gen, Sign, Verify.



For generating the key this takes n number of members in the group and generate group public key, private key for each user and user revocation tokens. For sign it takes group public key, private key of user and message then it return a signature α. In verification part it take group public key, a set of revocation tokens and group signature with message then it returns either valid or invalid.

Data stored in cloud server may get corrupted or the cloud storage server (CSS) is semi-trusted so TPA is used [7]. Data owner could Encrypt and upload the data in the cloud storage server. TPA verify the integrity of the data stored in cloud storage. If any modification occurred in that data it show the result to the data owner. This will reduce the risk of the users.

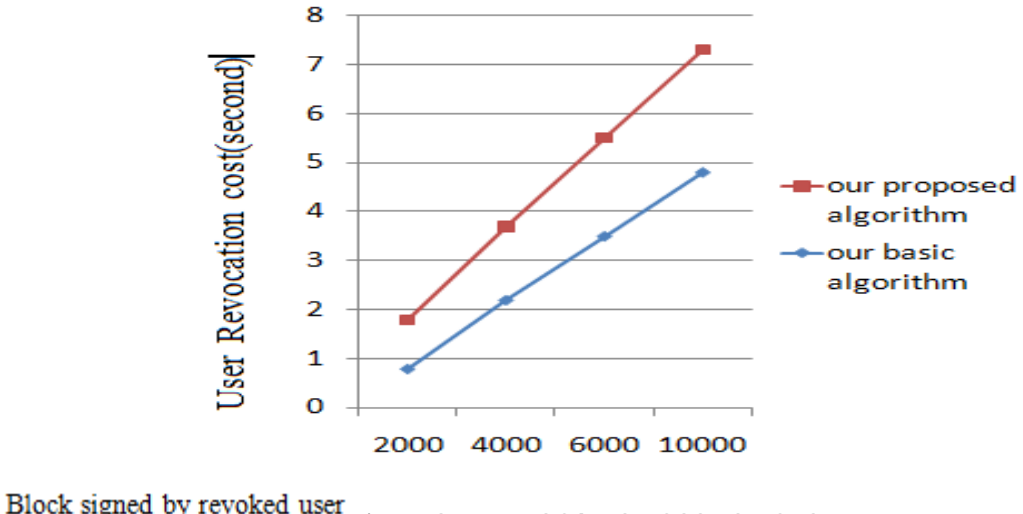


Fig: 1 USER REVOCATION COST ON CLOUD

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (135-139), Month: January-April 2016, Available at: www.noveltyjournals.com

V. CONCLUSION

In this paper, we design a data integrity and efficient user revocation of dynamic groups in the cloud. In our scheme, by using an AGKA, the group revocation is done effectively .so that user revocation is achieved. Third party auditor without knowing content checking the data by generating tokens, if the tokens gets matched integrity is achieved.

REFERENCES

[1] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multi owner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[2] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[4] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602–2614, Nov. 2013.

[5] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo- Ferrer, \Asymmetric group key agreement," in Proceedings of EUROCRYPT'09, LNCS 5479, pp. 153-170, 2009.

[6] D.Boneh and H.Shacham, "Group signatures with verifier local revocation,"IEEE Trans. security and cryptography Oct. 2004

[7] Renuka Goyal, Navjot Sidhu, "Third Party Auditor: An Integrity Checking Technique for Client Data Security in Cloud" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014.