ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 4, April 2016

ANTI-COLLUSION DATA SHARING POLICY FOR REGULARLY VARYING GROUPS USING CLOUD COMPUTING

M.USHA, DR. K. KAVITHA

***Abstract*— Cloud computing is the computing sample which supports earning resources like software, hardware, services over the internet. Most of the users store their data on cloud for data security and integrity is crucial. But the users in day to day changing groups can make the data sharing very tough. In order to establish the anti-collusion data sharing methods, special schemes are introduced through this paper. In this article, the problem of guaranteeing the integrity and of data storage security in cloud computing with the asymmetric encryption algorithm is done here. A secure key dispersion without any safe communication channels is provoked. Also, the group user can obtain the private key without any certificate authorities. Moreover, proposing a scheme of fine-grained access control and safe user revocation procedure. The new user joins the group is independent of the revoked users in the group. By the influence of group signature, signed account receipts and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. As the report the computation cost is reduced. The storage overhead and encryption computation cost of our schema are independent with the number of revoked users from the group, so the encryption cost is also reduced.**

***Index Terms*— Cloud service provider, key dispersion, dynamic groups, anti-collusion**.

I. Introduction

Cloud computing is possibly more secure than old-fashioned PC computing for most of the users. Within the cloud, the experts are in charge of maintaining the security of information and data being controlled by the servers. Most persons do not have the proficiency or are not willing to apply the maximum latest security features on their home PC. For this reason, many discuss that cloud computing and cloud operating are truly safer than traditional computing. A user should be alert of the level of required confidentiality of the data existence used to regulate what services should be used. . If the user is planning to only use cloud computing for social occasions and not post anything that should be kept away from the public then there should not any panic using the cloud computing. But still, if the information and the data are needed to be locked and delicate, then yet additional evaluation of the security presented by the cloud service should be classified.

A. Security Threats of Cloud Computing

The most security threat for cloud computing are stated as [18]

- Data breaches, which usually result from a defect in an application's design or other dangers.
- Data loss as a result of a mischievous attack, an unintentional deletion or a physical material problem in the data centers.
- Account hijacks, including the use of fraud techniques to obtain a user's private login information.
- Insecure interfaces, as in the cloud services depend on APIs to provide secure authentication, access control, encryption and other key functions. Vulnerabilities in these interfaces can raise the risk of a security breach.
- Rejection of service attacks, in which a malicious hacker prevents users from log on a targeted application or database.
- Mean insiders, such as employees or contractors, who use their spot to advantage access to private information warehoused in the cloud.
- Exploitation of services, which involves hackers who use the infinite resources of the cloud to break and bang an encryption key that would be not possible with limited hardware.
- Mutual vulnerabilities, containing platforms or applications accessed by different users in a multi-tenant environment.

To overcome these existing security threat issues in the cloud computing, there came solution such as [19]

1. Solution based on cryptography
2. Solution based on data partitioning schema
3. Solution based on machine learning
4. Solution based on multi-agent system

Here, the solution based on cryptography is highlighted in this paper.

M. Usha, *M.Phil Research Scholar, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, India.*
Dr.K. Kavitha*, Assistant Professor, Department of Computer Science, Mother Teresa Women's University, Kodaikanal. India.*

II. LITERATURE REVIEW

In 2003, the E.Goh, H. Shacham, N. Modadugu and D. Boneh projected a system named as SIRIUS. In that, the files stored on the untrusted server include two parts. They are file metadata and file data. In the file metadata, it contains a sequence of encrypted key-blocks and each one is encrypted by the public key of the official users. Here also, the user revocation is an inflexible question of the large amount of file sharing. Meanwhile, every time the file's metadata also needs to be updated. Whenever a new user joins the group, there is no need to calculate the private keys of the every user[14].

In 2005, Ateniese, K. Fu, M. Green and S. Hohenberger scheduled the proxy re-encryptions for the safe distributed storage. In this the concept of encryption calculation overhead is rising with the data sharing rate. The data holder translates the data with the two kinds of keys similar to unique and symmetric content keys. These two keys are again encrypted by a master public key. For the fine grained access-control, the server uses proxy cryptography method to directly re-encrypt the keys with the master public key granted to the public key of the user. But when any revoked users can be thrown, the users will be able to acquire the decryption keys[15].

In 2010, S. Yu, C. Wang, K. Ren and W. Lou considered an accessible and fine grained data access control schema in the cloud computing by by means of the KP-ABE technique. In this scheme, the data owners encrypt the file and the data with a rand-key where this random key is again encrypted with a group of attributes using the KP-ABE .The secret keys to the authorized users. Then the user can able to decrypt the cipher text if the data file attributes match with the access structure. To accomplish the user revocation, the cloud servers take the responsibility from the manager of the tasks such as file reencryption and the secret private key updates. Here in this, the single owner manner may create the problem with the execution of applications where all the users can share data with the others [20].

During 2010 Lan Zhou, V. Varadharajan and M. Hitchens suggested a scalable and selective fine-grained data access control schema by essential access policies based on data attributes and KP-ABE technique. The arrangement of attribute-based encryption (ABE), proxy re-encryption and lazy re-encryption allow the data owner to allot the calculation tasks to an untrusted server without enlightening the crucial contents of data. Data files are encoded using random key by the data owner. Using the Key Policy Attribute-Based encryption techniques, the random key is furthermore encrypted with a conventional of attributes. Then, the authorized users are allotted an access arrangement and equivalent secret key by the Admin. Hence, only the user with data file attributes that fulfill the access structure can break a cipher text. This system has particular restriction such as numerous- owner method is not supported by this system so that individual single holder manner makes it less flexible as only Admin are responsible for modifying the data file shared. And the user secret key needed to be updated after each revocation[20].

In 2010 R. Lu, X. Lin, X. Liang and X.Shen proposed secure derivation outline which registers ownerships and process history of a data object. This scheme is made on the bilinear pairing techniques which depend on upon group signatures and cipher text-policy attribute based encryption (CP-ABE) algorithms. The simple feature of this scheme is to suggest the unknown authentication for user retrieving the files, information privacy of documents stored in the cloud and tracing the beginning on unclear documents for illuminating the identity. Mostly, the arrangement has a single attribute. After the registration, each user in this schema obtains two keys and that is, a group signature key and an attribute key. Using Attribute-based encryption (ABE), any user can encode a data file. For decryption of the encoded data, an attribute keys is used by others in the group. To complete privacy preserving and trace ability, the user marks encrypted data with group signature key. Besides, the disadvantage of this scheme is that user revocation is not supported [4].

III. EXISTING SYSTEM

Wang, B. Li and H. Li focused on cloud computing and storage services, data is not only stored in the cloud, but also usually shared among a large number of users in a group. The author proposes Knox, a privacy-preserving checking mechanism for data stored in the cloud and shared among the group. Now particularly, the author utilizes group signatures to construct, so that a third party auditor (TPA) is capable to validate the shared data integrity. Until then, the uniqueness of the signer on each file block in shared data are saved private from the TPA. The original user can powerfully increase new users to the group and release the uniqueness of signers on all blocks. Through Knox, the information quantity is used for verification. Along with the time it takes to investigate with it. They are not altered by the number of users in the group[7].

Yong Cheng, Jun and Zhi-ying anticipated a security for users to store and share their complex data in the cloud storage. It provides a basic encryption and decryption for security and data confidentiality. So, the cloud storage still has some faults in its behavior. Primarily, it is ineffective for data owners to allot the symmetric keys one by one, particularly when there are a large number of files shared online. Also, the access policy revocation is expensive, since the data owner has to reclaim the data, and once again publish it. The initial problem can be resolved by consuming ciphertext policy attribute-based encryption (CP-ABE) algorithm. To adjust the revocation procedure, they are existing a new, capable revocation scheme. In this schema, the unique data are first distributed into a number of slices, and then issued to the cloud storage. When a revocation occurs, the data owner requests only to retrieve one slice, and re-encrypt and re-publish it. So, the revocation process is affected by only one slice in its place of the whole data[5].

IV. PROPOSED SYSTEM ARCHITECTURE

A. *Preliminaries: [1]*

1. The bilinear maps in pairings resolve by moving the central systems P to mere mathematics. With pairings, the central system P still exists, but it need not invoke for every action. In the sense,

The central system P has a private key, and the corresponding public key is known to every user.

Each user i obtain the private key from P.

When user wants to communicate with another user *R*, he can compute *R*'s public key using the only *R*'s name may be an email address and the central system public key .Recipient *R* uses K_R to decrypt the message.

2. Diffie-Hellman Problem and its related assumptions shows the method for two parties to securely exchange keys across an untrusted medium here in the cloud. In our scheme, two parties wish to begin communicating between each other. DH allows the construction of a common secret key (here we specify KEY) over an insecure communication channel[1].

B. *Techniques Used:*

The technique used here is Asymmetric Encryption algorithm. In order to widespread data sharing for dynamic groups in the cloud, the combination of the group signature and dynamic broadcast encryption techniques are implemented. Particularly, the group signature pattern enables users to namelessly use the cloud resources, and the dynamic broadcast encryption technique allows the data owners to tightly share their user's data files with others including new joining users.

C. *System Model*

The System model consists of the Group Manager, Group Users and Cloud Service Provider.

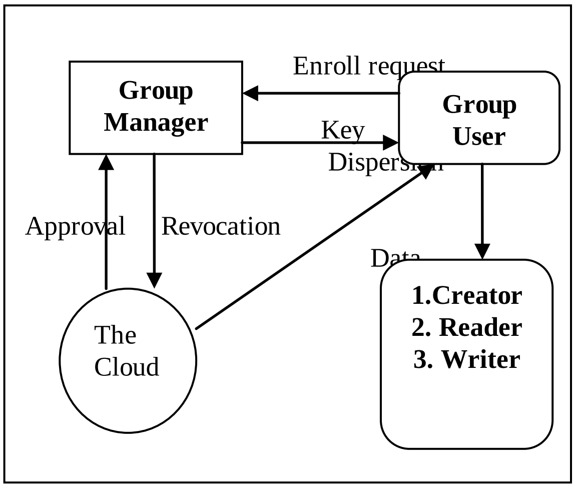

Fig. 1 System Model

As the group is frequently changing, the data sharing between the entities are very tough.Although, the user issue a request for login and the group manager accept the request and present a key. Then, the group manager adds the user in to the Active User List and sends to the cloud along with the current time stamp.

The users in the group can login as creators, writers and readers by the group manager. The users in a creator can create a file, writer may edit the data and reader can only read the file.

The Group Manager can revoke the user. The details of the revoked user can add to Revocation List and send to the cloud along with the time stamp.

D. *Steps For Setting System Privileges:*

The system setting of privileges are described in the figure.

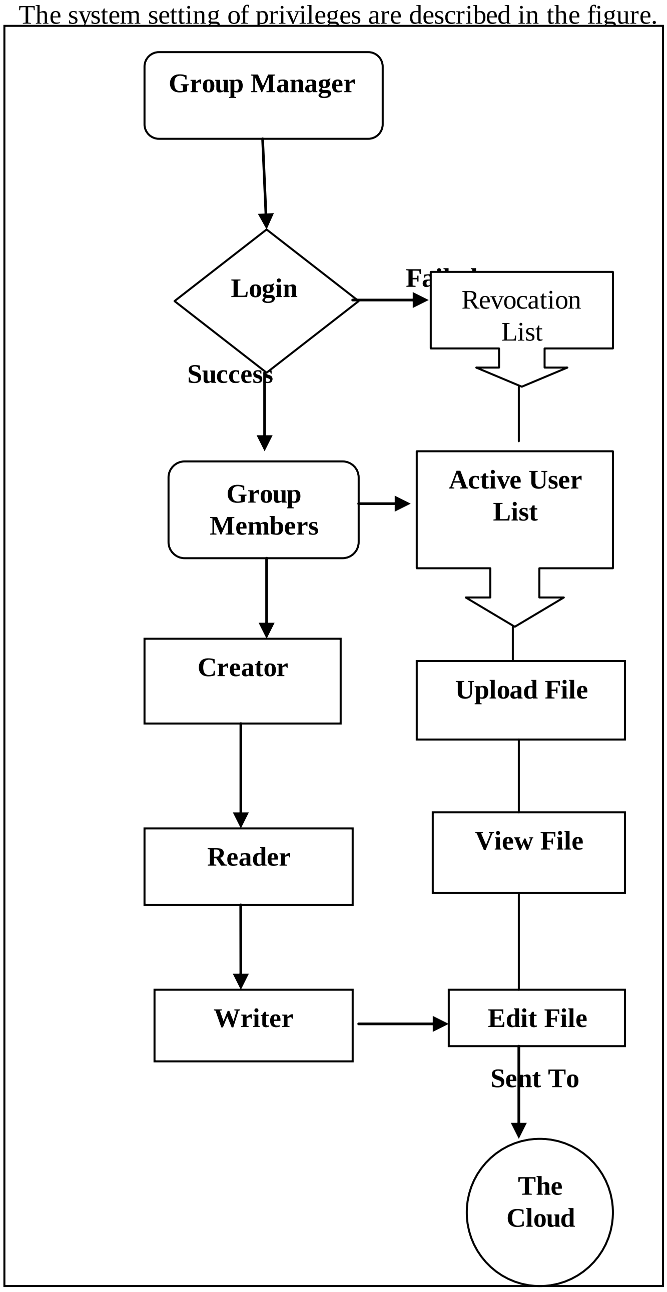

Fig 2. Work flow proposal

E. Design goals:

The Design goals of the proposed system are [1]

1. Secure key dispersion within insecure channels.
2. Granting fine-grained access control of the group users
3. The revoked user cannot get original data of the group even from the cloud, in order to preserve anti-collusion
4. For higher efficiency, the private key of the group user is independent of the number of the revoked user.
5. Revocation of the group user is done safely by leveraging a polynomial.

V. METHODOLOGY

a. Notations:

ID_i = the identity of a single group member i

Pub-k = public key of the user. Help to communicate with group manager.

Pri-k= private key of the user corresponding to the public key pub-k

KEY (xi,Ai,Bi) = private key which is distributed to user from group manager and used for data sharing.

ENC_k( ) = symmetric encryption algorithm used the encryption key k

$AENC_k$( ) = Asymmetric encryption algorithm used the encryption key k

GM = group manager or Admin

sign ( ) = signature of the group manager GM.

UL = Group User list

DL = Group Data list

t_{ul} = time stamp for User group list

ac= account user pay for registration.

v1, v2 $\in$ Z_q^* are random numbers.

CE = Cipher text

EK = re-encryption key

b. Algorithm for generation KEY:

The group manager GM generate the KEY when the IDi message matches the identity in calculation of the following equations

$$Ai = 1/(\gamma + xi) \,.\, P \in G1$$
$$Bi = xi/(\gamma + xi) \,.\, G \in G1$$

So the KEY will be KEY(xi, Ai, Bi)

Thus, this KEY [1] generated is used for data sharing.

VI. SCHEME DESCRIPTION

A. Registration for Existing User:

This operation is done by user IDi, group manager, GM and the cloud.

Begin

1. The user i send IDi, pub-k, ac, v1 for signing in.
2. For verification, group manager sends U, R to a user.
3. On confirmation, user sends IDi, v2, $AENC_{pri\text{-}k}$(IDi, v1, ac)
4. Then GM checks received IDi, message with identity IDi, computed by decrypting $AENC_{pri\text{-}k}$(IDi, v1, ac).
5. Also, check the random number v1 same as such given in the first step.
6. After all, successful verification, the GM generates the KEY.
7. GM adds the user IDi in UL along with the t_{ul}.
8. GM signs his signature sign (UL) and finally sends UL to the cloud.
9. The cloud verifies and stores as active UL.
10. User i become an active group member with IDi.

End

As soon as the authorized user i login, GM categories i into creator, reader, writer.

B. File Upload:

The Steps for file upload in the cloud done by group manager, the cloud and the user i.

Begin

1. Compute C1 = k.Y $\in$ G1
   Compute C2 = k.P $\in$ G1
   K = $Z^k \in G_2$
   C = ENC_k(M)
2. User encrypts
   ENC_{Bi}(IDdata, C1,C2,C, tdata)
   along with its private key Bi
3. GM decrypts it and gets
   I. Random re-encryption key EK
   = { K_r,W_0,…….,W_m}
   II. Cipher text CE = { C1,C2,C}
4. GM sends data file DF ={IDgroup, IDdata, CE,EK,tdata } with sign(DL)
   to the cloud.

End

C. User Revocation:

The user revocation is done by group manager and the cloud.

Begin

1.Removing user i from UL in the local storage space and updating the UL in the cloud

2. GM constructs a polynomial function along with the new UL

$$f''_p\,(x)= \Pi_{j\neq i \quad j=1\text{to } m}(x - Vj) = \Sigma_{\,j=0 \text{ to}(m-1)}\ a_jx^j \ (\text{mod } q\,)$$

3. Select new random re-encryption key K_r' and construct new EK
4. Compute Ciphertext CE = { C1,C2,C} $_{Kr'}$

```
5. Along with GM sign (DF) along with new time stamp
   tdata send to cloud.
End
```

D. *File Download:*

File Download is performed by the group member or users and the cloud.

```
Begin
    1. User i encrypts IDgroup, IDi, $ENC_{Ai}$( IDdata ) to
       cloud
    2. Cloud decrypts and compares with Ai along
       with UL.
    3. If checking is ok then data file DF will send to
       user i.
End
```

VII. Conclusion

In this paper, the proposed system describes the secure anti-collusion data sharing strategy for dynamic groups in cloud computing. Our schema deals with effective key dispersion based on the safe communication channel. Also, new user joining is independent of the number of the revoked user leaves the group. As the group manager is having the active user list and revocation list, there is a minimum possibility of misuse. By the use of influencing a polynomial, the user is revoked from the group. So, the proposed system is satisfying the requirement of anti-collusion data sharing and provides superior efficiency. The computation cost is less and key dispersion overhead is minimized.

REFERENCES

[1] Zhongma Zhu and Rui Jiang, "A secure anti-collusion data sharing scheme for dynamic groups in the cloud", IEEE Transactions on parallel and distributed systems, vol.27, no.1, January 2016

[2] 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.

[3] 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.

[4] 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.

[5] 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

[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. Co

[13]M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[14] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems
Security Symp. (NDSS), pp. 131-145, 2003.

[15] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed
Storage," Proc. Network and Distributed Systems Security Symp.(NDSS), pp. 29-43, 2005.

[16] 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.

[17] http://techterms.com/definition/cloud_computing

[18]http://www.blackstratus.com/overcome-security-issues-cloud-computing/

[19] Y. Ghebghoub, S. Oukid, and O. Boussaid
"A Survey on Security Issues and the Existing Solutions in Cloud Computing"International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013

[20] Shobha D. Patil, Dr. Sulochana B. Sonkamble, " A Dynamic Secure Group Sharing in Cloud Computing", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438