ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

An Efficient Anti-Collusion Data Sharing Mechanism for Data Confidentiality for Dynamic Groups

Nivedita P.Regundwar [1], Prof.Prema Desai [2]

M.E. II year Student, Department of Computer Engineering, SKNCOE, Pune, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering, SKNCOE, Pune, Maharashtra, India[2]

ABSTRACT: In this framework users can achieve an effective and economical approach for information sharing among gathering individuals in the cloud with characters of low maintenance and little management cost. Because of the consistent change of the membership sharing information while giving security ensuring is as yet difficult, especially for a untruth cloud because of the collusion attack. In existing framework the secure key distribution depends on the secure communication channel, however to have such a channel is strong assumption and is difficult for practice. In this framework ,a protected information sharing plan for dynamic members. In proposed framework first propose is secure route for key distribution without utilizing any safe communication channels, and user can safely acquire their private keys from gathering managers. The framework can finishes fine grained get to control any customer in the social event can use the source in the cloud and refused customers can't get to the cloud again after they are denied. Additionally the framework can secure the framework shape conspiracy attack, which implies that clients can't get unique information records regardless of the possibility that they plan with depended cloud. In this propose system, the file is fragmented into fragments and then uploaded to the cloud where the authentic users can download the file using its private key.If a user leaves the group, the private keys of other members is changed.If a user wants to change the group from one group to other group it can change it.

KEYWORDS: Access control, Private key distribution, cloud computing, Blowfish algorithm, RSA algorithm, DSS, Fragmentation.

I.INTRODUCTION

Cloud computing denotes to applications and services distributed done on the Internet. These services are present from data centers all over the existence, which joints are referred to as the "cloud." The hint of the "cloud" streamlines many networks and computer systems, complicated in linked online services. This symbolizes the Internet's wide-ranging reach, while streamlining its complexity. Any user with an Internet connection can contact the cloud and enjoy the services it provides to them. Since these services are oftentimes coupled, users can share information between several systems and with other users. The examples of cloud computing include available backup services, dynamic social networking services, and individual data services, etc. The Cloud computing also includes online applications, such as those accessible through Microsoft Online Services. The hardware services, similar as redundant servers, mirrored websites or files, and Internet based clusters are also examples of cloud computing. Identity privacy is one of the most coming obstacles for the wide deployment of cloud computing. Users may be unwilling to join in cloud computing because their own identities may be revealed to the intruders.The information can be disclosed by the intruders. For example, a misbehaved staff can deceive others in the company by sharing false files without being known to the intruder. The group members should be able to fully enjoy the data storage and services which are shared provided by the cloud. As compared with the one group manager level, where only the group manager can store and change data in the cloud, the more than one owner manner is more flexible in practical applications. More concretely, each user in the group cannot access data. At last, groups are normally active in practice, like new member addition and current member deletion in a company. The revocation and addition of the group members in the group makes it more difficult. On the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

other hand, the unknown system challenges grant the group members to learn the content of data files stored before their participation, because it is impossible for new group members to contact with unknown data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users reduces the complexities. Several security schemes for data sharing an untruth servers have been proposed . In these approaches, data owners store the encrypted data files in entrusted storage and distribute the corresponding decryption. In this proposed scheme, we propose a scheme that provides the anti-collusion data sharing in multiuser cloud. Firstly the user registration user can register in the system in which user provides the information about him and complete the registration process system provides the user id and password to access the cloud.

II.RELATED WORK

In 2003 the authors S.Kamara and K.Lauter [2], proposed paper which describes secure multi-owner information sharing theme. It implies that any user within the group can firmly share information with others over a trustworthy cloud. This supports dynamic groups over a cloud. Specifically, new granted users will directly rewrite information files uploaded before their participation while not contacting with information group owners. User revocation will be simply achieved through a completely unique revocation list while not change the key. Keys of the remaining users the scale and computation overhead of coding are constant and independent with the amount of revoked users. However, the problem is about a heavy key distribution overhead for large file sharing. Again, the file-block key needs to be updated and distributed again for a user revocation.

In 2003, Kallahalla et al [3] displayed a cryptographic storage framework that empowers secure information sharing on deceitful servers in view of the strategies that partitioning records into files bunches and encrypting every document amass with a document square key. Yu et al abused and consolidated methods of key approach quality based encryption, intermediary re-encryption and languid re-encryption to accomplish fine-grained information get to control without uncovering information substance. The record square keys should be upgraded and circulated for a client denial; accordingly, the framework had an overwhelming key conveyance overhead. The complexities of client cooperation and denial in these plans are straightly expanding with the quantity of
information proprietors and the revoked clients.

In 2003, the E.Goh, H. Shacham, N. Modadugu and D. Boneh [4] 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.

In 2010, S. Yu, C. Wang, K. Ren and W. Lou [6] 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 files are encrypted by the owner of the file and also the random key is encrypted with attributes group using 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 complete the user deletion from the group, the cloud servers take the responsibility from the manager of the tasks such as file re-encryption 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.

Liu et al. [10] introduced a safe multi- owner information sharing plan, named Mona. It is guaranteed that the plan can achieve fine-grained get to control and revoked clients won't have the capacity to get to the sharing information again once they are revoked. In this paper a new method was proposed for sharing the secure data in the Cloud computing for the Multiuser Groups. Data integration is the biggest problem with cloud data storage. To preserve data privacy, the data files are encrypted and the uploaded into the cloud. To resolve this problem of data theft, recently the efficient method MONA presented for secured multi owner data sharing in however there were some limitations in that same

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

approach in terms of reliability and scalability. In any case, the plan will effectively experience the ill effects of the arrangement assault by the disavowed client and the cloud .

D. Boneh, X. Boyen, and E. Goh [11], The authors have introduced exhibit a Hierarchical Identity Based Encryption (HIBE) framework where the ciphertext comprises of only three gathering components and unscrambling requires just two bilinear guide calculations, paying little mind to the hierarchical depth profundity the plan is particular ID secure in the standard model and completely secure in the arbitrary oracle model demonstrate .This framework has various applications: it gives exceptionally effective forward secure open key and character based cryptosystems with short ciphertexts.

Zhongma Zhu et al. [13] found that there are some collusion attack on Liu et al.'s protocols. Due to the presence of the collusion attack, the secure data access control has not been achieved and the sharing of data has not been taken into consideration and therefore poorly protected. Also, another security loophole existing user registration phase because of the unsecure communication channels. Thus the private key has to be securely given to users in this channel. This can also lead to revealing the data of the users in the group. Thus, the scheme will easily suffer from the collusion attack by the user which has been deleted and the cloud. The revoked user will be able to use his private key to get the secret data and will also be able to decrypt it after his revocation by conspiring with the cloud. client disapproval by joining part based get to control strategies with encryption to secure gigantic information stockpiling in the cloud.

During 2010 Lan Zhou, V. Varadharajan and M. Hitchens [14] suggested a scalable and selective finegrained 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 reencryption 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 management 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.

M.Nabeel, N.Shang,, and E.Bertino [16], presented view on the security of data on cloud is based on fine-grained encryption of the data. Under such approaches, data owners are in charge of encrypting the data before uploading them on the cloud and reencrypting the data whenever user credentials or authorization policies change. Data owners thus acquire high communication cost and the computation costs. In order to minimize the overhead at the data owners, while assuring data confidentiality from the cloud, a better approach should be implemented to enforce the secured access control to cloud. This paper proposes that there are two layers of encryption that addresses such requirement. Under this approach, the data owner performs a one layer encryption, and whereas the cloud performs a second layer of encryption on top of the owner encrypted data. The authors have used an effective group key management scheme for encryptions. This approach provides secrecy of the data and maintains the privacy of the user from the cloud while accessing the cloud. Such approaches requires high communication and computation cost to manage the private keys and encryptions whenever user credentials or organizational authorization data changes.

Zhongma Zhu and Rui [17] proposed a paper in which a secure way of key distribution is used by using secure communication channels, and the users can securely obtain their private keys from group manager and the users can achieve fine-grained access control. But the limitation is that users do not recomputed and update their private keys for the situation where new users join the group or a existing user is revoked from the group. In this paper, the computation cost decreases with number of revoked users that means the member computation cost is dependent on number of revoked users.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

III.IMPLEMENTATION STATUS

Modules:
1. Member or User Module
2. Manager Module
3. Cloud or Admin Module

I. Member or User Module:
1. Every user needs to register with corresponding group for getting access permission using signature key.
2. The group admin consists of all the information such as vendor list and the list of revoked users.
3. The client that wants to register to the group requests to the admin. They can get access permission they can upload files to cloud.Members from same group can view the content of file over simultaneously they can download the file as well.

II.Manager Module:
1. Responsible for providing and denying access permission to the members of various groups.
2. Manager has the main access permission for maintaining the files over cloud. Manager can navigate through the group as well.
3. Manager can view the log details of activities carried on cloud file storage.
4. Manager achieve able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.

III.Cloud or Admin Module:
1. Responsible for providing and denying access activities related to manager module and user module.
2. Admin have the rights to maintain the all the permission.
3. Admin Can efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt.

IV .PROPOSED SYSTEM ARCHITECTURE

This system provides a very secure way for distributing the private keys without using secure communication channels. The users can get their private keys from group manager securely without any Certificate Authorities due to the verified for the public key of the user. As shown in the above fig.1. there are three actors in the architecture i.e. Group user, group manager and the group admin. The group admin consists of all the information such as vendor list and the list of revoked users. The client that wants to register to the group requests to the admin. After the registration the admin sends the admin secret key to its mail id. Then after the verification the client can upload or download the data. The files that are stored in the group are fragmented into blocks and those blocks are encrypted and then stored in the cloud. Previously, the data was encrypted completely and were not fragmented. This block encryption increases the security of the data. This process is during the uploading of a file. While downloading the data file, the blocks of the files are decrypted and then combined and given to the user to download the file. It uses two level security using OTP. In the first level is simply a text based password and at the level 2, after the successful clearance of level 1, security system will generate a onetime password that would be valid for just one session. The authentic user will be informed by the OTP on its email id. System supports active groups efficiently, when a new user joins in the group or a user is deleted from the group, the private keys of the other needs to be recomputed and updated.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

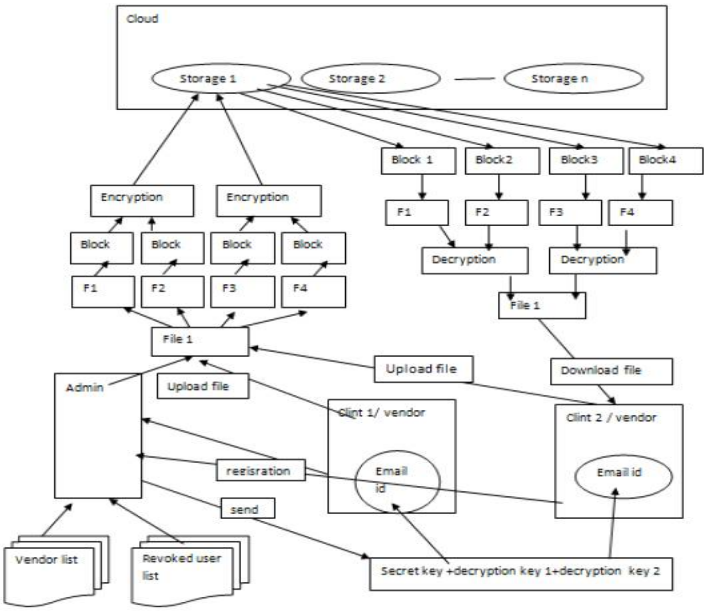

Fig.1.Proposed System Architecture

Algorithms:

I.SecureKey Distribution Algorithm DSS(Digital Signature Standard And Mail method):
Generating Random pre message value k where k<0<q. Calculate r=(gk mod q) mod q, q=N-bit prime number. If unlike case that r=0 and start again different random k .Calculate s=k-1 (H (m)+xr) mod q, x=choose secret key, s=public key.
If unlike uncase s= then again start with different random k . Sign(r,k).

II.Key Generation RSA (Ron Rivest, Adi Shamir and Leonard Adelman) :
1. Choose p = 3 and q = 11
2. Compute n = p * q = 3 * 11 = 33
3. Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
4. Choose e such that 1 < e <φ(n) and e and n are co-prime. Let e = 7
5. Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
6. Public key is (e, n) => (7, 33)
7. Private key is (d, n) => (3, 33)
8. The encryption of m = 2 is c = 27 % 33 = 29
9. The decryption of c = 29 is m = 293 % 33 = 2

III. Blowfish :
1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.
2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)
3. Encrypt the all-zero string with the Blowfish algorithm, using the data file described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified data .

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

6. Replace P3 and P4 with the output of step (5). Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

IV. PERFORMANCE MEASURES AND RESULT EVALUATION:

The above table gives the comparison between the existing systems like ODBE,RBAC etc. and the proposed system. In our system a user is able to share data with others in the group with revealing identity privacy to cloud. Table 1 gives the comparison between the existing system and the proposed systems.

Parameter	Exiting System	Proposed System
Cost	High	Low
Security access based	Low	High
ODBE	Yes	No
RBAC	No	Yes
Data Security	No	Yes
Access Control	Yes	Yes
User Revocation	No	Yes
Data Confidentially	No	Yes
Anti Collision attack	No	Yes

Table 1.Result evaluation.

V.CONCLUSION

From this system it is concluded that the data sharing is secure in this scheme, for dynamic groups in an untrusted cloud. A group member is able to share data securely with others in the group without revealing its own privacy to the untrusted cloud. Moreover, It supports efficient user deletion and new user addition in the group. It allows a user to change the group from one group to another. More specially, efficient user revocation can be achieved through a public revocation list with updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. A new type authentication system, which is highly secure, has been proposed in this system.

REFERENCES

[1] M. Armbrust, A.Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.
[2] S.Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.
[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] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote entrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.
[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw.Distrib. Syst. Security Symp., 2005, pp. 29–43.
[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp.Inf., Comput.Commun. Security, 2010, pp. 282–292.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer. Commun. Security, 2006, pp. 89–98.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput.Commun.Security, 2010, pp. 282–292.
[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.
[10] 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.
[11] D. Boneh, X. Boyen, and E. Goh, "The Hierarchical identity based encoded with the constant size ciphertext," in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn, 2012, pp. 440–458.
[12] Ca. Delerableae, P. Paillier, and D. Paointcheval, "Fully collusion of secure dynamic broadcast encoded with constant-size Ciphertext or encoded keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59.
[13] Z. Zhu, Z. Jsiang, and Rd. Jiang, "The attack on mona: safe multiowner information sharing for dynamic groups in the cloud," in Proc. Int. Conf. Inf. Sci. Cloud Comput., Dec,8, 2013, pp. 18-25.
[14] L. Zhou, V. Varadhaarajan, and M. Hitcheans, "To Achieving the secure role-based access control on encoded information in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2015.
[15] X. Zoxu, Y.-S.Dai, and E. Bertixno, "A practical and flexible key management mechanism for trusted collaborative computing," in Proc. IEEE Conf. Comput.Commun., 2008, pp. 1211–1219.
[16] 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.
[17] Zhongma Zhu, 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.