ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Enable Data Sharing Scheme for Dynamic Groups in the Cloud

Jyoti Pingat[1], Prof P. R. Ugale[2]

M.E. Student, Department of Computer Engineering, SPCOE, Otur, India[1]

Assistant Professor, Department of Computer Engineering, SPCOE, Otur, India[2]

ABSTRACT: With the fast advancements happening in cloud computing and administrations, there has been a developing method to utilize the cloud for substantial scale data storage. This has raised the vital security issue of how to control and prevent unapproved access to data stored in the cloud. With the character of low support, cloud computing gives a conservative and productive answer for sharing gathering asset among cloud clients. But, sharing data in a multi-proprietor way while saving data and character security from an untrusted cloud is as yet a challenging issue, because of the continuous change of the participation. To start with, we propose a safe proprietor data sharing plan, for dynamic gatherings in the cloud. By utilizing group signature and dynamic communicate encryption strategies, any cloud client can secretly impart data to others. Then, the storage overhead and encryption calculation cost of our plan are autonomous with the quantity of revoked clients. Likewise, we break down the security of our plan with verifications, and show the effectiveness of our plan .

KEYWORDS: Cloud Storage; Sharing Data; Group signature; Multi-Proprietor.

I. INTRODUCTION

The cloud provider provides one of the best services is data storage the security and privacy issue have major concern for organization for utilizing such service. It is a greatest platform that provides data storage in very lesser cost and all time it should be available over the internet. The security must be important in the cloud computing. The encryption technique is commonly adopted by the cloud computing that means the encrypted data should be stored on the storage of cloud to protect the data. Encryption is no sufficient as organization obtain have to enforce fine-grained access control on data. Such control is based on the attribute that system is known as the attribute based system. For the data privacy it is important to encrypt the data and upload the encrypted data on the cloud. In cloud it is not easy to design efficient and secure data sharing scheme in multiowner system due to the following challenging issues. Identity, revocation and new member participation i.e. the changes of membership make securely data sharing extremely difficult. On the other hand an efficient member revocation without updating the secret key of remaining user to minimize the complexity of key management. Signed receipt is caused after every member revocation in group that minimizes multiple copy of encrypted file it can help to minimize computation cost.

In this paper, we propose a protected information sharing plan, which can achieve secure key requisition and information sharing for element bunch. The principle commitments of our plan include:

1. We give a safe approach to key transport with no protected correspondence channels. The clients can safely obtain their private keys from gathering chief with no Certificate Authorities because of the confirmation for people in general key of the client.
2. Our plan can accomplish fine-grained access control, with the assistance of the gathering client list, any client in the gathering can make use of the source in the cloud and disavowed clients can't get to the cloud again after they are denied.
3. We propose a safe information sharing plan which can be protected from agreement attack. The denied clients cannot have the capacity to get the first information records once they are rejected regardless of the fact that they contrive with the untrusted cloud. Our plan can accomplish secure client rejection with the assistance of polynomial capacity.
4. Our plan can encourage dynamic gatherings effectively, when another client join in the gathering or a client is renounced from the gathering, the private keys of alternate clients don't should be recomputed and renovate.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

5. Security investigation to demonstrate the security of our plan. In expansion, performance of reenactments to exhibit the effectiveness of our plan.

II. RELATED WORK

In this section, the reference are collected from all conferences, sites, articles, books from the internet which helps to implement the project. For development of this project we referred some of the base papers, ideas which helps in development, testing and deployment phase. For good understanding of the advanced authentication system there are some work on the IEEE international journal that we have referenced are:

Boyang Wang, Baochun Li, and Hui Li, has proposed a paper on ”Public Auditing for Shared Data with Efficient User Revocation in the Cloud”. Where it gives information of Shared data with efficient user revocation in the cloud. The cloud can improve the efficiency of user revocation. But it has disadvantage as ”Network Connections Dependency. Cost is more”**.** Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H Deng proposed a paper on ”Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.”. More flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges. Allows efficient and flexible key delegation. ”Network Connections Dependency. here also has disadvantage that Cost is more and algorithm used are Key aggregate Encryption, Decryption.

Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student Member, IEEE, and Elisa Bertino, Fellow, IEEE” proposed a paper on ”An Efficient Certificate less Encryption for Secure Data Sharing in Public Clouds”. Securely share sensitive data in public clouds. Improve efficiency. here also has disadvantage that Network Connections Dependency and Cost is more” algorithm used are public key encryption algorithms.

Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed a paper on” Privacy Preserving Delegated Access Control in Public Clouds”. Decomposition ACPs used to privacy preserving fine-grained delegated access control to data in public clouds. The Owner has to handle a minimum number of attribute conditions while hiding the content from the cloud here also has disadvantage that Network Connections Dependency. Cost is more algorithm used are optimization algorithms, gen graph, random cover, policy decomposition.

Kaitai Liang, Man Ho Au, Member, IEEE, Joseph K. Liu, Willy Susilo, Senior Member, IEEE, Duncan S. Wong” proposed a paper on ”A DFA Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing”. Here also has disadvantage that ”Network Connections Dependency. Cost is more” algorithm used are DFA-based functional proxy re-encryption. KaipingXue and Peilin Hong proposed a paper on ”A Dynamic Secure Group Sharing Framework in Public Cloud Computing”. ”Dynamic secure group sharing framework in public cloud computing environment The sharing files are secured stored in cloud servers and all the session key are protected in the digital Envelopes. Here also has disadvantage that ”Network Connections Dependency. Cost is more” algorithm used are Proxy signature algorithm Diffie-Hellman.

Tao Jiang, Xiaofeng Chen, and Jianfeng Ma IEEE. proposed a paper on ”Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation”. it has Secure data integrity auditing for share dynamic data. Provide data confidentiality for group users. Here also has disadvantage that ”Network Connections Dependency. Cost is more” algorithm used are Randomized Key generation, RSA, SHA. Jiawei Yuan and Shucheng Yu proposed a paper on”Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification”. Efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation. Systematically construct a novel secure search protocol, which not only enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors, but also allows data owners to encrypt keywords with self-chosen keys and allows authenticated data users to query without knowing these keys. -Additive Order and Privacy Preserving Function family (AOPPF) which allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately. Here also has disadvantage that Network Connections Dependency. Cost is more algorithm used are Randomize Key generation, AES 128.

Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE, Jie Wu, Fellow, IEEE, and Siwang Zhou” proposed a paper on ”Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing”. Xinyi Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou” proposed a paper on ”Cost-Effective Authentic and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Anonymous Data Sharing with Forward Security". "Xinyi Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou" ID Based Ring Signature here also has disadvantage that Key exposure Network Connections Dependency. Cost is more" algorithm used are RSA/ElGamel/SHA.

III. PROBLEM STATEMENT

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue. Specifically, revoked users are unable to decrypt the stored data file after the revocation.

IV. EXISTING SYSTEM

A cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key. Key policy attribute-based encryption, proxy re-encryption and lazy re encryption to achieve fine-grained data access control without disclosing data contents.

Drawbacks of Existing System:

1. The file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead.
2. The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.
3. The single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others.

V. SIMULATION RESULTS

In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user. Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function. Our scheme is 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. We provide security analysis to prove the security of our scheme.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

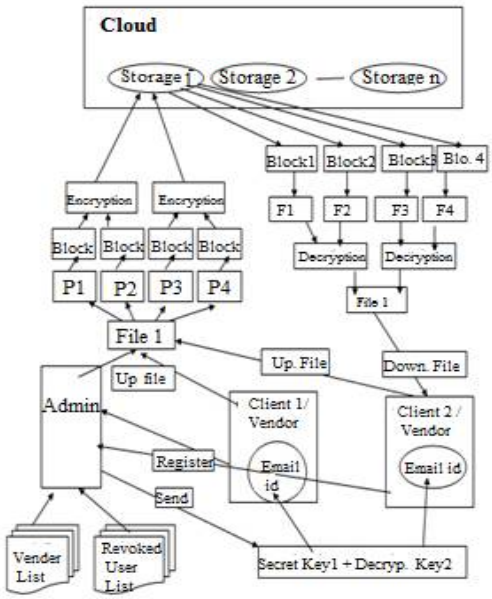

Fig. 1. Architecture of Anti-Collusion Data Sharing Scheme

Advantages of Proposed System:

1. The computation cost is irrelevant to the number of revoked users in RBAC scheme. The reason is that no matter how many users are revoked, the operations for members to decrypt the data files almost remain the same.
2. The cost is irrelevant to the number of the revoked users. The reason is that the computation cost of the cloud for file upload in our scheme consists of two verifications for signature, which is irrelevant to the number of the revoked users. The reason for the small computation cost of the cloud in the phase of file upload in RBAC scheme is that the Verifications between communication entities are not concerned in this scheme.
3. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is 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.

System Architecture:

The system model consists of three different entities: the cloud, a group manager and a large number of group members. The cloud, maintained by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner. However, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the content of the stored data. Group manager takes charge of system parameters generation, user registration, and user revocation.

In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties. Group members (users) are a set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

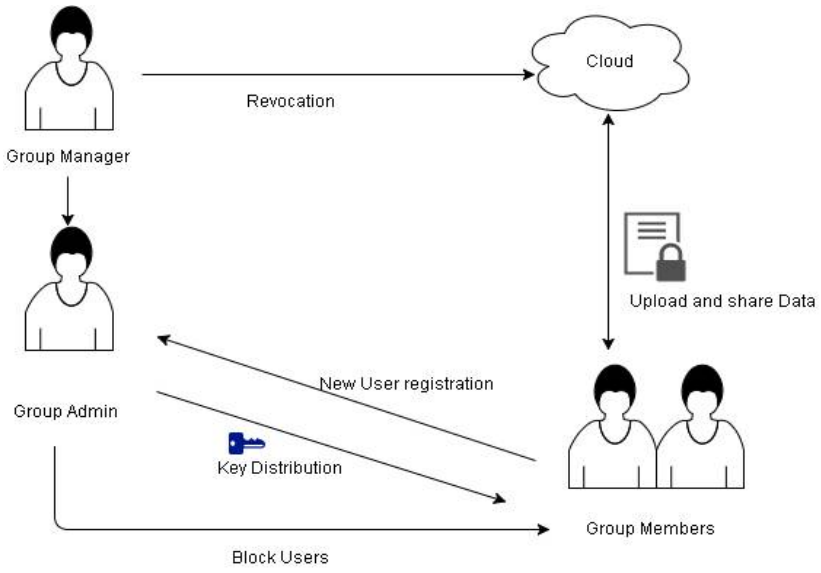

Fig. 2. System Architecture

VI. IMPLEMENTATION

a) Group Manager:
Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties.

b) Group members:
Group members (users) are a set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

c) Key Distribution:
The requirement of key distribution is that users can securely obtain their private keys from the group manager without any Certificate Authorities. In other existing schemes, this goal is achieved by assuming that the communication channel is secure, however, in our scheme, we can achieve it without this strong assumption.

d) Access control:
First, group members are able to use the cloud resource for data storage and data sharing. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud resource again once they are revoked.

e) Data confidentiality:
Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. To maintain the availability of data confidentiality fordynamic groups is still an important and challenging issue. Specifically, revoked users are unable to decrypt the stored data file after the revocation.

f) Efficiency:
Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the others, which means that the remaining users do not need to update their private keys.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

g) Cloud module:

Cloud module plays an important role ,group managers upload some files into cloud those files are stored in encrypted format because a secure access control scheme on encrypted data in cloud storage by invoking role-based encryption technique. It is claimed that the scheme can achieve efficient user revocation that combines role-based access control policies with encryption to secure large data storage in the cloud.

Unfortunately, the verifications between entities are not concerned, the scheme easily suffer from attacks, for example, collusion attack. Finally, this attack can lead to disclosing sensitive data files. The cloud, maintained by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner. However, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the content of the stored data.

VII. PROPOSED ALGORITHM

Implementation is the stage of the project when the theoretical design is turned out into a working system. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing, designing of methods to achieve change over and evaluation of change over methods.

Algorithm/Technique used

Advanced Encryption Standard (AES)

Algorithm Description

AES is an iterated symmetric block cipher, which means that:

- AES works by repeating the same defined steps multiple times.
- AES is a secret key encryption algorithm. AES operates on a fixed number of bytes.

AES as well as most encryption algorithms is reversible. This means that almost the same steps are performed to complete both encryption and decryption in reverse order. The AES algorithm operates on bytes, which makes it simpler to implement.

This key is expanded into individual sub keys, a sub keys for each operation round. This process is called Key Expansion.

VIII. EXPERIMENTAL RESULT

In general, our proposed plan can accomplish secure key appropriation, fine get to control and secure client repudiation. For obviously seeing the upsides of security of our proposed plan, as represented in Table 1, we list a table contrasted and Mona, which is Liu et al's. plan, the RBAC plan, which is Armbrust plan and ODBE plan, which is Delerablee et al's scheme. The √ in the clear means the plan can accomplish the comparing objective and also simulate in java platforms using an IDE Eclipse.

Scheme	Secure Key Distribution	Access Control	Secure User Revocation	Anti-Collus -ion Attack	Data Confe- dentiality	Block User	Key Recov -ery Attack
Mona		Yes					
RBAC Scheme		Yes					
ODBE		Yes	Yes	Yes			
Base Paper	Yes	Yes	Yes	Yes	Yes		
Our Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Fig. 3. Security Performance Comparisons

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

IX. SNAPSHOTS

Fig. 1. User Login

Fig. 2. User Registration

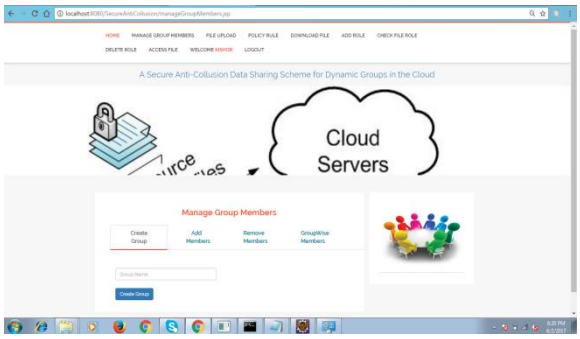

Fig. 3. Create Group

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

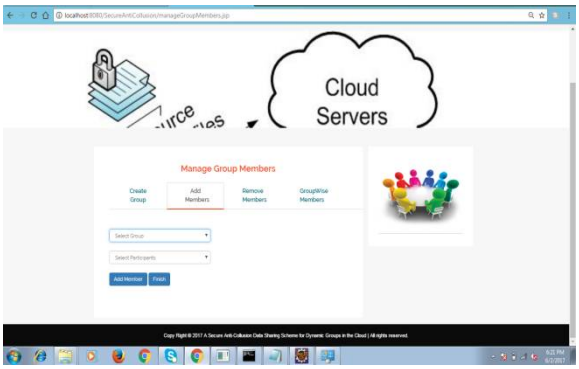

Fig. 4. Add Member

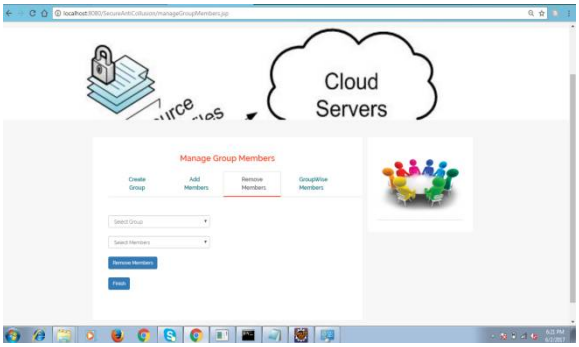

Fig. 5. Remove Member

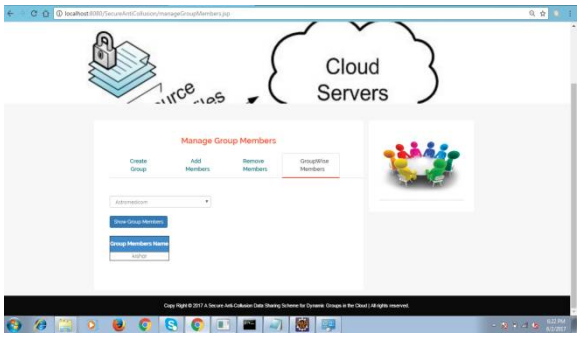

Fig. 6. GroupWise Members

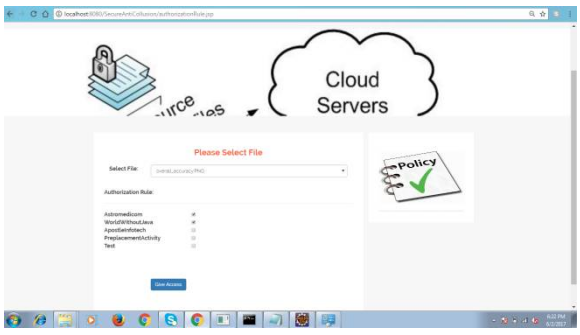

Fig. 7. Select File to Upload

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Fig. 8. Download Files

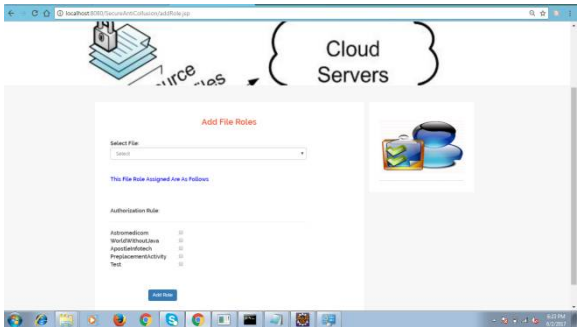

Fig. 9. Add File Roles

Fig. 9. Check File Roles

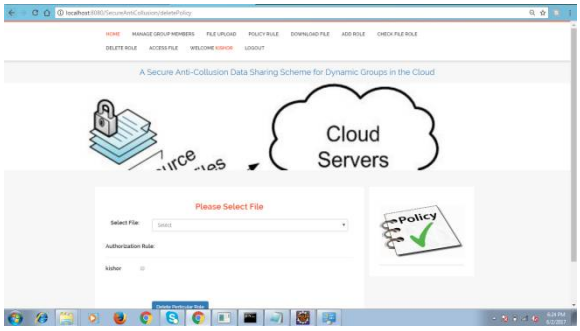

Fig. 10. Please Select File

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Fig. 11. Access File

X. CONCLUSION

We design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is 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. Moreover, our scheme can achieve secure user revocation; the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

XI. ACKNOWLEDGEMENT

I express my sincere thanks to my project guide Prof. P. R. Ugale who always being with presence & constant, constructive criticism to made this paper. I would also like to thank all the staff of computer department for their valuable guidance, suggestion and support through the paper work, who has given co-operation for the project with personal attention. Above all I express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during paper work. At the last I thankful to my friends, colleagues for the inspirational help provided to me through a paper work.

REFERENCES

1. Zhongma Zhu, Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems, 2015.
2. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp. 2003, pp. 131–145.
3. 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.
4. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc.Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.
5. 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.
6. 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.
7. 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.
8. D.Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Cipher text," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp.440-456, 2005.
9. C. Delerablee, P. Paillier, and D. Pointcheval, "FullyCollusionSecure Dynamic Broadcast Encryption with Constant-SizeCi-phertexts or Decryption Keys," *Proc.*First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.
10. Zhongma Zhu, Zemin Jiang, Rui Jiang, "The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," Proceedings of 2013 International Conference on Information Science and Cloud Computing(ISCC 2013), Guangzhou, Dec.7,2013,pp. 185-189.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

11. 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.
12. X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans.Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182– 1191, Jun. 2013.
13. 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.
14. B. Dan and F. Matt, "Identity-based encryption from the weil pairing," in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol., 2001, vol. 2139, pp. 213–229.
15. B. Den Boer, "Diffie–Hellman is as strong as discrete log for certain primes," in Proc. Adv. Cryptol., 1988, p. 530.
16. D. Boneh, X. Boyen, and H. Shacham, "Short group signature," *in* Proc. Int. Cryptology Conf. Adv. Cryptology, 2004, pp. 41–55.
17. D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," *in* Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 440–456.
18. 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.
19. X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," in Proc. IEEE Conf. Comput. Commun., 2008, pp. 1211–1219.

BIOGRAPHY

Jyoti Pingat is a Student in the Computer Engineering Department, SharadChandra Pawar College of Engineering, Savitribai Phule Pune University. Her research interests are Cloud Computing, Communication, Security etc.