International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Secure Private Key Distribution for Dynamic Groups in the Cloud

Miss. Sonali S Goral[1]
[1]*Computer Department, Savitribai Phule Pune University*

Abstract: ***To achieve a functional and low-budget approach for sharing data within groups with group members in the cloud with not only low maintenance but also low management cost, the system can be proposed. So, this proposed system must provide assurance of security while sharing data files since they are outsource. Due to continuous change of membership for sharing data which provide security protection is still challenging task, especially for an untrusted because of collusion attack. Secure key distribution is based on the secure communication channel in existing system but to have this secure channel is not only strong expectation but also hard to practice. We propose in this system, a sharing of data for dynamic group members securely. We propose a key distribution without secure communication channel first and group manager provide private keys to the user in a very secure manner. The system can achieve fine grain access control which means user cannot access the data stored on the group after revocation of the particular group, so that it can utilize the source in the cloud. This gives the protection from the collusion attack that means user cannot get original data files even if they join with untrusted cloud.***
Keywords: Cloud computing, Access control, Fine grain access, Key distribution, Data confidentiality.

I. INTRODUCTION

Cloud computing is with dynamism accessible and virtualization resources are provided as a service on internet. Cloud providers give us data storage service. Let's consider one practical data application. A company made their staff to store and share their data on the cloud. And this will go to affect the confidentiality of the data uploaded by the staff. Cloud servers handled by the cloud providers, and clients does not trust them, to store their files on cloud, for their security and privacy. And to provide clients the data privacy, the only way is data encryption, encrypt files before you upload on server. In cloud computing, the identity privacy is the most important obstacle. Until cloud providers do not get the trust of clients, about their identity is does not going to revealed, if they upload anything on cloud, clients do not going to ready to upload files on server. On other hand not reviling identity can becomes more dangerous. For example, some staff may misuse this privacy policy, and send unauthorized files on cloud, this may became difficult for company, and he will not get find because of this policy.

The best example of Internet based application is the cloud computing. It provides sharing of computer processing resources and information to computers and other devices on our requirements. The cloud computing plays an important role which provides futures of Internet of Services, enabling on demand provisioning of applications, platforms, and computing infrastructures.

By changing membership, sharing of data securely is very difficult. On other hand before part of the group or participation in the group user can not learn the content of the data files in a unknown system because it is not possible for the new granted users to communicate with unknown data owners and obtain corresponding decryption keys. We also propose an efficient user revocation with updating the secrete key of other users is desired to maintain the complexity of key management. We can share the data by using several security schemes in the proposed system. Data owner store the encrypted data file in untrusted storage and provide the corresponding decryption.

In the proposed work we can achieve secure key distribution as well as data sharing in dynamic groups in the cloud. So the contribution of the scheme includes:

1) Key distribution without any secure communication channels. The group manager provides private keys to the participant users without any certificate authorities due to the verification of the public key of the user.
2) We provide fine grain access control in which revoke user can not able to access the data again.
3) We also achieve memory management while uploading data files on a cloud.

II. REVIEW OF LITERATURE

To save information security, a fundamental arrangement is to encode information documents, and afterward transfer the scrambled information into the cloud. Shockingly, outlining a proficient and secure information sharing plan for gatherings in the cloud is not a

simple assignment. In the current System information proprietors store the encoded information documents in untrusted stockpiling and circulate the relating decoding keys just too approved clients. In this way, unapproved clients and additionally stockpiling servers can't take in the substance of the information records since they have no learning of the decoding keys. Be that as it may, the complexities of client support and repudiation in these plans are directly expanding with the quantity of information proprietors and the quantity of denied clients, individually.

The author proposed two novel strategies for secure appropriation of the gathering key. The methods proposed in this paper makes utilization of the cross breed key trees which permit the entire disposal of the safe channels for the dissemination of the key material not at all like a considerable lot of the prior proposed plans, least stockpiling prerequisites at every part, end of the odds of era of week keys, less number of rounds and least computational overhead. Be that as it may, cross breed cloud, might miss three key pieces: security, network and convenience. MONA proposed a new secure multi-owner data sharing scheme, for multiple groups in the cloud. They applied the group signature as well as dynamic broadcast encryption techniques, any cloud user can secretly share data with others. The storage overhead and encryption computation cost of our scheme are not dependent with the number of revoked users. Also they analyze the security of scheme with difficult proofs, and demonstrate the efficiency of scheme in experiments. First complete group key management scheme which can supports all these functions yet preserves efficiency. The proposed scheme is based on the new concept of access control polynomial (ACP) that efficiently and effectively support full dynamics, flexible access control with fine-tuned granularity, and concealment .New scheme is protected from various attacks from both external and internal malicious parties [2].

Achieving secure role based control on encrypted data in cloud achieved through RBAC. RBE scheme allows RBAC policies to be apply for the encrypted data stored in public clouds. RBE-based hybrid cloud storage architecture provides facility of an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organizations structure in a private cloud [3]. One approach to encrypt documents satisfying different policies with different keys using a public key cryptosystem such as attribute-based encryption, and proxy re-encryption is called broadcast group key management (BGKM), and then give a secure construction of a BGKM scheme called ACVBGKM. BGKM scheme iprovide an adding users/revoking users can be performed efficiently by updating only some public information. Fne-grained encryption-based access control for documents which are stored in an untrusted cloud, BGKM is used and make approach efficient [4]. This the most important advantage of the BGKM scheme.

Cloud is the new platform. It provides data storage with low cost and it should be available over the Internet all the time. The security is the most important factor 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 un-sufficient as organization uses fine-grained access control on data. This system is known as the attribute based system. Because the control is based on the attribute. It is important to encrypt the data and upload the encrypted data on the cloud for the data privacy. In cloud it is difficult to design efficient and secure data sharing scheme in multi-owner system due to the many challenging issues such that Identity, revocation and new member joining i.e. the changes of membership make securely data sharing extremely difficult. On the other side an efficient member revocation without updating the secret key of remaining user which reduces the complexity of key management. Signed receipt is caused after every member revocation in group. It minimizes multiple copy of encrypted file as well as minimize computation cost [5].

RekMolva et al. proposed another structure for multicast security in view of disseminated calculation of security changes by middle of the road hubs. The contribution of transitional hubs in the security procedure causes another kind of reliance between gathering enrollment and the topology of the multicast organize. The control of security exposures in substantial multicast gatherings is guaranteed. The system additionally guarantees both the versatility for extensive element bunches and the security of individual individuals. Two distinctive key circulation conventions consenting to the system are presented. Data distribution in cloud infrastructure provides an effective approach called Secure-Split-Merge (SSM) is introduced for the security of data. The proposed SSM scheme was it uses unique mechanism for performing splitting of data using AES 128 bit encryption key. The chunks of encrypted splits are being maintained on various group servers of different types of cloud zones. The relative analysis denotes that the proposed system gives effective throughputs as compared to other existing and traditional security standards [6].

III.EXISTING SYSTEM

Private key distribution is based on secure communication channel in the existing system but to have such type of communication channel is not only strong hypothesis but also difficult for practice. To provide privacy while sharing data is still challenging issue for untrusted cloud due to collusion attack.

A. Attribute-based encryption:

Cipher text and secret key of user are depend on attributes such that country in which he lives or the kind of contribution he has is nothing but the Attribute based encryption which is a type of public key.In this type of encryption the set of attributes are very important because if the one of the attribute in the set is missing then the decryption is impossible or if the set of attribute of the user have to match with attribute of the cipher text then only decryption is possible.

B. Disadvantages:

1) Data are not secure while data sharing in a group.

2) Revoked users will be able to access the data after they revoked.

IV. PROPOSED SYSTEM

The proposed system is introduced to share the data files as well as secure key distribution by using a dynamic group in the cloud.

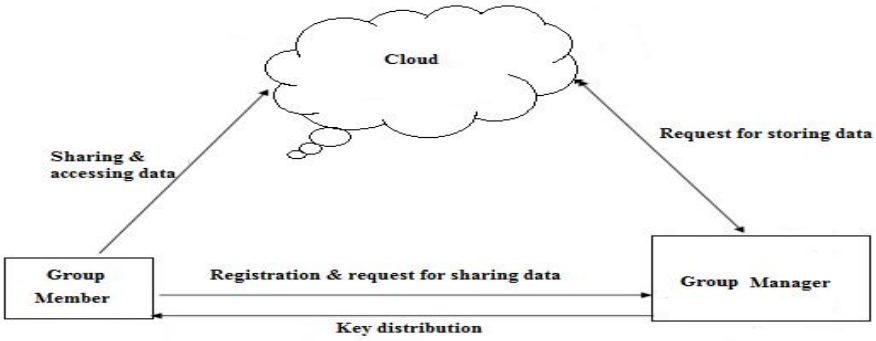

Fig. 1 Proposed system architecture

The system provides 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.

The system 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.

In proposed system there are three models included like Group member, Group manager and Cloud server. Every modules have their own responsibility provided they are as follows:

A. Group member

As shown in Figure 1, group member is important factor for the system.The user or group member can store the data, share the data with other group members. For sharing the data files on the cloud the user have to first register to the group manager.After that group manager doing the verification of the registerd user for security.If the group manager approve the request which is send by user then only he can get access to that group otherwise he can not store any data or download data on that cloud storage.

B. Group manager

Group manager is frontrunner of the system. Activate and deactivate user, managing system parameters these functions can be performed by the group manager. Group manager can view all details of activities carried on cloud storage. He can provide as well as denying access permissions to the group members.

C. Cloud

Cloud can not only provide access but also deny the permission for data file storage.

If the user joins new group or revoked from one group to another group, the private keys of other group members will updated by the respective group manager. From this method proposed system provide the dynamic group efficiency as well as security to the group.

To provide Access control, data confidentiality, anonymity, traceability and efficiency are the main aim of the proposed system. These features can be as follows:

1) *Access control:* To share the data and store the data group members can use their resources in cloud. Unauthorized user can not access the resources in the cloud at any situation or at any time. After revocation, the revoked user can not use the resources in the cloud.
2) *Data confidentiality:* It is important to a person who is unauthorized are not proficient of learning the data which is stored on cloud. A challenging issue is to maintain data securely in dynamic groups in the cloud. Revoked user cannot decrypt the data which is stored on cloud after revocation.

V. RESULT AND ANALYSIS

As illustrated in Fig. 2, here we compare the uploading data files on a cloud between existing and proposed system. In this we can observed that the speed of uploading data file in proposed system is much more than in existing system. Uploading speed is irrelevant to the revoked users.

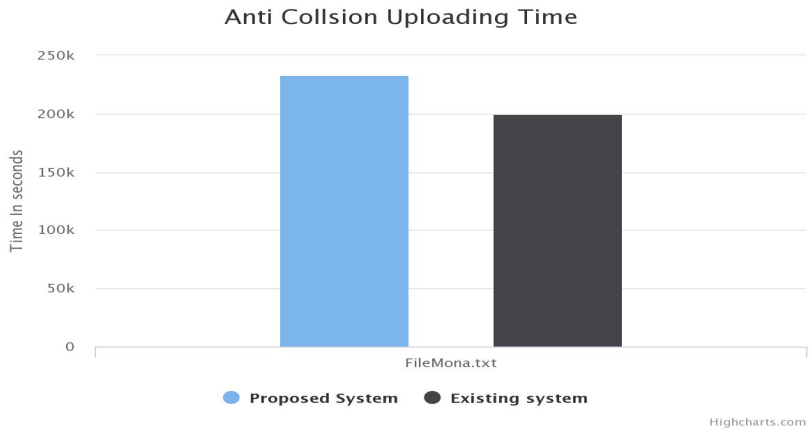

Fig. 2 Comparison between existing and proposed system's uploading data files.

In Fig. 3, we compare the downloading data files on a cloud in existing and proposed system. In this we can observed that the time required for downloading data file in proposed system is less than the existing system where downloading of the data file is irrelevant to the number of revoked users. So the computation cost is independent on the size of data file.

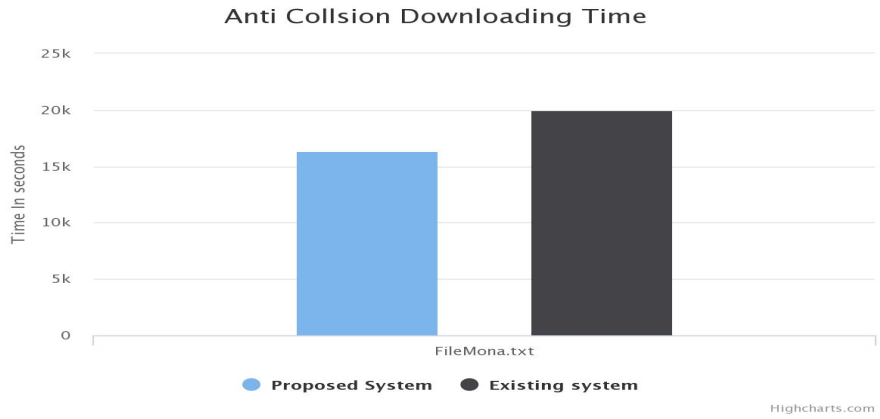

Fig. 3 Comparison between existing and proposed system's downloading data files.

VI. CONCLUSIONS

In this research work, we have reviewed literature on ways to provide a secure environment where a data owner can share data with members of his group while preventing any outsiders from accessing any data in case of malicious activities like data loss and theft. However, throughout this work we assume that members of the group will not carry out malicious activities on the data owners data. Here, we frame a secure anti collusion data sharing schema for dynamic groups in cloud computing. The scheme includes safe and secure key dispersion, fine grained access control , safe user revocation procedure and no change of the private key for the users are manipulated in the cloud computing environment. The system is design using dynamic groups in an untrusted cloud for secure data sharing scheme. Without releasing identity privacy to the cloud user can share data among other users in the group. It also supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation

list with no updation of the private keys of the other users. New users can directly decrypt files which is stored in the cloud before their participation. A new type authentication system, which is highly secure, has been proposed in this system.

VII. ACKNOWLEDGMENT

We extend our thanks to all the staff members and faculty from our college who has directly and indirectly helped us in designing and performing experiments for the proposed work.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang Boyang Wang, and Jingbo Yan. "MONA: Secure Multi-Owner Data Sharing for Dynamic Group in the Cloud", IEEE, 2013.
[2] X. Zou, Y.-S. Dai, and E. Bertino. "A practical and flexible key management mechanism for trusted collaborating computing", in Proc.IEEE conf.Comput.Commun.2008,pp 12111219.
[3] L. Zhou, V. Varadharajan, and M. Hitchens, "Achiving secure role-based access control on encrypted data in cloud storage", IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 19471960, Dec. 2013.
[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. 26022614, Nov. 2013.
[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy reencryption schemes with applications to secure distributed storage", in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 2943.
[6] Burhan Ul Islam Khan, Rashidah F. Olanrewaju, "SSM: Secure-Split-Merge Data Distribution in Cloud Infrastructure", in 2015 IEEE Conference on Open Systems (ICOS), August 24-26, 2015, Melaka, Malaysia.
[7] 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.