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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in Cloud Computing

Shubham Narandekar, Sagar Lambture, Vishal Kadam, Prasoon Kushwah

School of Computer Engineering, MIT Academy of Engineering, Pune, Alandi, India

School of Computer Engineering, MIT Academy of Engineering, Pune, Alandi, India

School of Computer Engineering, MIT Academy of Engineering, Pune, Alandi, India

School of Computer Engineering, MIT Academy of Engineering, Pune, Alandi, India

ABSTRACT: This system provides many to many data sharing paradigm for multiple users of a group in the cloud, it will be an economical and effective approach of data sharing with the characters of low maintenance and little management. Proposed system will provide security of data since they are outsourced and third party cloud service providers cannot be trusted. Each dynamic group can accomodate data upto certain limit and consists of several group members managed by a group manager, here the data is shared among the group members only using their keys provided securely by manager, also the system prevents collusion attack which means when a user revokes from the dynamic group then that particular user will not be able to access data related to that group. It also allows multiple users to upload multiple files with same name.

KEYWORDS*:* Access Control, Cloud Computing, Key Distri-bution, Privacy-Preserving

I. INTRODUCTION

Cloud computing has attracted the interests of many firms because of its low energy consumption and resource sharing characteristics. Cloud computing provides users with limitless storing and computing resources. Storage is one of the most important service which it provides because of which various forms of data information can easily flow with respect to the cloud storage service, for instance, social networks, video viewing, video sharing etc. Although cloud has been used for many purposes, little significance has been given to group data sharing in the cloud, which refers to the situation in which ,multiple users want to achieve data sharing in a group manner for cooperative purposes.

Group data sharing has many practical applications, such as sharing within project groups in an organization, electronic health networks, electronic literature in libraries. Primarily, there are two ways to achieve data sharing in cloud- the first case refers to the situation where one client grants access to his/her data for many clients in a one-to-many pattern and the second case refers to the situation wherein many clients grant access to their data to many clients in a many-to-many pattern.

Despite of the above advantages of cloud storage, there still remain various challenging obstacles, among which, the privacy and security of users data have become two major issues. Traditionally, the data owner stores his/her data in the trusted servers, which are generally controlled by a fully trusted administrator. However, the cloud is usually maintained and managed by a semi-trusted third party (Cloud provider). As a result, traditional security storage technologies cannot be directly applied in the cloud storage scenario. While it is desirable for the data owner to share his/her private data with intended recipients, it presents an even more challenging problem since we have to make sure that except the intended recipients, nobody, including the cloud providers, can obtain any useful information from the encrypted data.

DOI: 10.15680/IJIRCCE.2019. 0702045

A. Main Contributions

To address the above challenges, we present a secure anti-collusion data sharing scheme for dynamic groups in cloud computing . The main contributions of this paper include the following.

1) Arbitrary Number of Users and Dynamic Changes Are Supported: To address an arbitrary number of users in real applications, such that the number of users can be arbitrary rather than restricted. Moreover, in real cloud storage applica-tions, users may join or leave freely. The proposed scheme can efficiently support dynamic changes of users with respect to the access control and the many-to-many data sharing pattern.

2) The Confidentiality of the Outsourced Data Is Preserved: In our scheme, the outsourced data are encrypted with a common conference key prior to being uploaded. Attacks or the cloud having no access to the common conference key cannot reveal any information of the data stored in the cloud. The security of the encryption key is based on Advanced Encryption Standard (AES) and Blowfish algorithm. Consequently, users can safely exchange data with others.

3) Traceability Under an Anonymous Environment Is Achieved by Our Scheme: With respect to the key agreement,every user in the cloud is able to freely share data with other users. Moreover, users can exchange information in the cloud anonymously with respect to the group signature. When-ever a dispute occurs, the group manager has the authority to reveal the real identity of the data owner.

4) Authentication Services Are Provided: During the key agreement during data sharing, each member exchange mes-sages along with the group number to ensure whether the identity of the members is valid. Furthermore, the group signature will be bound with the uploaded data file to verify the validity of the file.

B. Related Works

The cloud supplier one amongst the most effective ser-vices is knowledge storage the safety also as privacy issue have a major concern for folks for utilizing this services. To protect the privacy of information held on within the cloud, cryptographical role-based access management (RBAC) schemes are developed to confirm that knowledge will solely be retrieved by folks that are allowed by access policies. However, these cryptography strategies don't address the prob-lems of trust. during this paper [1], they planned trust models to reason regarding and improve the safety for a hold on knowledge in cloud storage systems that use cryptographical RBAC schemes. The trust models provide AN means for the homeowners and roles to determine the trustiness of individual and users severally within the RBAC system. The planned trust models monitor role hierarchy within the analysis of exactitude of roles. we have a tendency to gift a style of a trust-based cloud storage system that shows, however, the trust models is joined into a system that uses cryptographical RBAC. we have also considered practical application scenarios and described how these trust evaluations are wont to reduce the error and enhance the standard of higher cognitive process by data owners and roles of cloud storage service.

Cloud Computing, the long-held dream of cloud computing as a utility, has the potential to remodel an outsized a part of the IT trade, creating code even a lot of engaging as a service and shaping the method IT hardware is intended and purchased. Developers with innovative ideas for brand spanking new net services not need the big capital outlays in hardware to deploy their service or the human expense to work it. they have not to worry regarding over-provisioning for a service whose popularity doesn't meet their predictions, so wasting expensive resources, or underneath provisioning for one that becomes wildly in style, so missing potential customers and revenue. Cloud computing refers to the uti-lization of net (cloud) based mostly technology for a spread of services. it is a computing model during which virtualized resources square measure provided as a service over the web. The construct incorporates infrastructure as a service (IaaS), platform as a service (PaaS) and code as a service (SaaS) that have the common theme for satisfying the computing desires of the users. Cloud computing services sometimes give common business applications online that square measure accessed from an internet browser. This paper [2] pays a lot of attention to the Grid paradigm because it is usually confused with Cloud technologies. They also describe the relationships and distinctions between the Grid and Cloud approaches.

In this paper [3] they have concentrated on building a secure cloud storage service on a cloud infrastructure, where the service provider is entrusted by the user.they have surveyed the benefits of the architecture provided to both user and service provider and talks about recent advances in cryptography dedicated to cloud storage.

In this paper [4] they devised Sirius, it is a secure file system designed to cover over or layer over the insecure networks and other P2P file systems like NFS, CIFS. In this paper, they assumed that the network storage is not trusted and provides its own cryptographic control for file level sharing.revocation and key management is simple with minimal out of band communication and it also uses a hash tree constructions.

In this paper [5] they proposed associate application referred to as atomic proxy re-encryption wherever a semi-trustworthy proxy converts a ciphertext for one person into a ciphertext for one more person without seeing the underlying plaintext.they also foreseen that a secure and quick encryption trend can become celebrated and common for managing encrypted file systems. By the longer term works of the author, they gift a replacement re-encryption theme that gives a lot of security and Access management to secure classification system.

This paper [6] puts forward a replacement economical constructions for public key broadcast encryption that has following properties receivers and unsettled.here the encryption is collusion-secure for big collusions of users and secures also new users will be part of cluster dynamically.they also planned the way to for good revoke subgroup of users. Also, they achieved the optimum sure of O(1) size for ciphertexts or decryption keys.

It is the greatest platform that gives data storage in terribly lesser price and everyone time it ought to be offered over the net. In this paper [7] it is stated that the protection should be vital within cloud computing. The encryption technique is usually adopted by cloud computing which means the encrypted data ought to behold on on the storage of the cloud to guard the information. Encryption isn’t any sample as an organization gets ought to enforce fine-grained access management on data. Such management relies on the attribute that a system is understood because of the attribute-based system. For the information privacy, it is vital to encode the information and transfer the encrypted data on the cloud. In the cloud, it is challenging to style economical and secure data sharing a theme in the multi-owner system because of the subsequent challenging problems. Identity, revocation and new member participation i.e. the changes of membership build firmly data sharing extraordinarily tough. On the opposite hand associate degree, economical member revocation while not change the key of remaining user to attenuate the quality of key management. A signed receipt is caused once each member revocation in the cluster that minimizes multiple a copy of the encrypted file

In this paper [8] they try to overcome the problem in a Presented cryptographic storage system that enables secure data sharing.This technique involves dividing the file into the file group and encrypt each file group with a file block key. In this scheme, at the time of user revocation, the file block key had to be updated again and distributed to the user, therefore, causes a heavy key distribution overhead. Also, they talk about plutus which is a cryptographic storage system which provides secure file sharing without trusting file servers, it provides highly scalable key management also allow users to retain direct control. here they have explained the mechanism of plutus to reduce the number of cryptographic keys exchanged between users with using filegroups and also distinguish file read and write access.

This paper [9] focuses on attribute primarily based coding with the delegation, as throughout the delegation the cloud servers may replace or change/tamper the delegated ciphertext and supply a cast computing answer with infectious intent. They may also cheat authentic users by responding to them that they are not authentic so as to avoid wasting price, here they considered construction for realizing circuit cipher text pol-icy at-tribute primarily based hybrid coding that provides verifiable computation, data confidentiality, fine gained access management and correctness at the same time and their theme also achieves security against plaintext attacks below k- multilinear decisional Diffie-hellman assumption.

During this paper[10] they Introduced a replacement fine-grained 2FA issue authentication access system for cloud computing services.specifically in their proposed system asso-ciate attribute based mostly access management mechanism is implemented with the necessity of each a light-weight security device and a user secret key, and a user cannot access the system if they dont have each, this mechanism will enhance the safety of the system, especially in scenarios wherever several users share the same pc for web-based cloud services. Their system also allows the cloud server to limit the access to those users with the same set while preserving user privacy and they have also carried out a simulation to demonstrate the ability of 2FA system.

II. PROBLEM STATEMENT

In Cloud based Dynamic group sharing to maintain the data security the private keys of existing members of group need to be updated after the revocation of any group member , also to restrict the malicious members from accessing the data in group file accessing constraints will be introduced.Data confidentiality will be maintained using double encryption when uploading data on cloud.

A. Threat Model

We consider the following types of attack which may threat the security of the proposed scheme.
1) If a member try to access files from a group to which he doesn't belong to, then the group manager will face multiple requests which may lead to heavy traffic.
2) Any user irrespective of the domain, can register to any group to access files which may be used against the organisation.

3) A revoked member can share the keys of all the members with other external members.

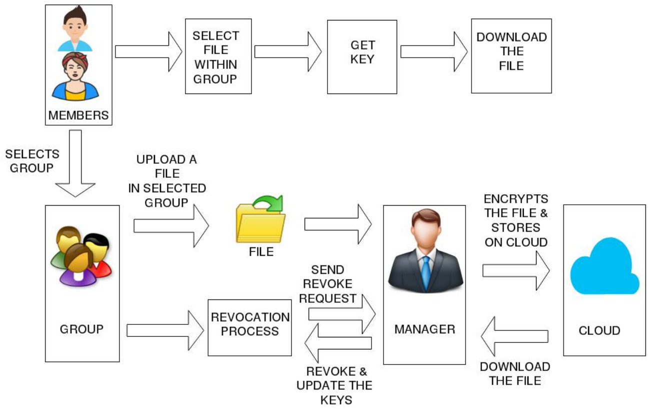
B. Design Goals

In order to overcome the problems above, the main design goals of the proposed scheme include the following.

1) Key Updation : Data sharing in dynamic groups should be handled carefully as the group members can dynamically switch groups. A member who no more belongs to that particular group cannot access files from that group. To achieve this, after revocation process the keys of all the members along with the revoked member will be updated.

2) Data Confidentiality : The data stored on the cloud should be protected from unauthorised access and ma-licious users. In an organisation, only the users with particular predefined domain id can register to the ap-plication. This will restrict fake users from registering.

3) Traceability : Although data are shared anonymously in the cloud, a well-designed scheme should be able to locate the owner of the controversial data in disputes.



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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

III. PROPOSED SYSTEM

Proposed scheme consists of following modules

1) Group Member: In our scheme, members are people with the same interests (e.g., bidder, doctors, and businessmen) and they want to share data in the cloud. The most worrying problem when users store data in the cloud server is the confidentiality of the outsourced data. In our system, users of the same group conduct a key agreement. Subsequently, a common conference key can be used to encrypt the data that will be uploaded to the cloud to ensure the confidentiality of the outsourced data. Attackers or the semi-trusted cloud server cannot learn any content of the outsourced data without the common conference key. In addition, anonymity is also a concern for users. Our scheme uses a technique called
group signatures, which allows users in the same group to anonymously share data in the cloud.

2) Group Manager: is responsible for generating system parameters, managing group members (i.e., uploading members encrypted data, authorizing group members) and for the fault tolerance detection.The group manager in our scheme is a fully trusted third party to both the cloud and group members. If an external user tries to access files from a different group more than three times then the manager will remove that particular user from the applications.

3) Cloud: provides users with seemingly unlimited storage services. In addition to providing efficient and convenient storage services for users, the cloud can also pro-vide data sharing services. However, the cloud has the characteristic of honest but curious. In other words, the cloud will not deliberately delete or modify the uploaded data of users, but it will be curious to understand the contents of the stored data and the users identity.

A. Methodology

Whenever a member uploads a file, group manager will assign a group to that member with a private key which will the unique key of that member. If the user wants to upload the file , it will go through encryption and stored on the cloud. When user A want to access user Bs file then user B will get a message asking for the permission. If user B grants the permission then manager will provide user A the key of user B by which user A can access the files and download them.If user wants to leave a group then he can request group manager for revocation. After revocation private keys of all the group members will be updated. The available space in the group will also get updated.Group manager also maintains the log of file uploaded by all the users of the group.

IV. CONCLUSION

The system is designed for secure data sharing scheme, for dynamic groups in an untruth cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, It supports efficient user revocation and new user joining. 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 of authentication system, which is highly secure, has been proposed in this system. Using all these modifications we have successfully overcome the drawbacks of previous applications.

REFERENCES

[1] SS.Kamara and K.Lauter,Cryptographic cloud storage, in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136149.

[2] MM.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.5058, Apr. 2010.

[3] MM.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.2942.

[4] EE.Goh, H.Shacham, N.Modadugu, and D. Boneh, Sirius: Securing remote untrusted storage, in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp.131145.

[5] GG.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. 2943.

[6] CC.Delerablee, P.Paillier, and D.Pointcheval,Fully collusion secure dynamic broadcast encryption with constant-size Ciphertexts or decryption keys, in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 3959.

[7] RR.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. 282292.

[8] Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud Xuefeng Liu,Yuqing ZhangBoyang Wang, and Jingbo Yan 2013 IEEE.

[9] BB.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. 5370.

[10] SS.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. 282292.