Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secured Multi-Owner Data Sharing for the Dynamic groups in the Cloud

P. Kiranmai, Y. Ramu
Department of Computer Science and Engineering,
SVECW, Bhimavaram, AP, India

Abstract — Now-a-days the cloud computing became a leading edge for the traditional information technology by its characteristics like low maintenance and the resource sharing. Along with its advantages it also brings some challenging issues for securing the data files. Here we are proposing a new scheme MONA for the secure sharing of data files among the users in the un trusted cloud by using the group signature and the broadcast encryption scheme. But in this scheme also some limitations in terms of reliability and scalability. Hence in this paper we are further extending the basic concept of MONA by increasing the reliability and scalability by increasing the group managers dynamically.

Keywords:-Cloud computing, dynamic groups, data sharing, access control, reliability and scalability, integrity.

I. INTRODUCTION

A. What is Cloud Computing?

The cloud is a group of machines and web services that implement the cloud computing. Cloud computing is accessing the computers and their functionalities via the internet or a local area network [2]. Cloud computing is one of the major platform where we have the facilities such as data storage and the data available in any time because the cloud computing is an internet-based computing. The cloud service providers such as Amazon are providing various services to the cloud users by maintaining a powerful data centres. Generally the Cloud computing is simply saving on IT implementation costs. In cloud computing the users can request access for a group of web services .when the permission is granted, a group of resources will be given to the requested user. After working with the resources the users get released.

B. Basic concept of MONA

Data storage is the one of the major services provided by the cloud providers. Now consider a practical application. one organization allow all its staff members to store and share data files in the cloud .By using the cloud, the staff become free from the maintenance of data in a local system. But it may create a problem for the data confidentiality. Particularly, the cloud servers that are managed by the cloud providers are not trusted by the users while the data files stored in the cloud are may be sensitive and confidential, that are may be business plans. To maintain the data privacy, one of the solution is t encrypt the data files and then the encrypted files are uploaded into the cloud. Unfortunately, it is not an easy task to design an efficient and secure data sharing method for the groups in the cloud .It has some challenging issues like as follows.

First of all in the cloud computing the identity privacy is one of the major obstacle. Without giving guarantees to the users, the users are not interested to participate in the cloud computing system. Because whenever the dispute occurs the real identities are disclosed to cloud providers. On the other hand, unconditional identity privacy may create the problem to privacy. For example, the misbehaved staff can produce some fake information to the others in the company without being identified. Therefore, identification which enables the group manager to reveal the real identification of the user is also highly adorable.

The second thing is the multiple owner manner, that is nothing but the all group members can efficiently share the data files with all the others and can store the data files in the cloud .in single owner manner the group manage can only store and change update the data present in the cloud but the multiple –owner manner is more flexible for the practical applications additionally the each and every user in the group not only permitted for reading the data but they was shared by the company.

The last one is the dynamic groups in an organization. The staff can join in the company or the current working employee can vacate the company. But this may create problem for the data security. Here we have two major issues. One thing is the newly joined members can directly decrypt the files without contacting the data owners the second thing is there is no need to update the others secret keys when ever any user is revealed from the company. It will minimize the complexity of the key management. Up to now, there are several security schemes are developed for the data sharing on the un trusted cloud servers. In those the data owners store the encrypted data files in the unauthorized users cannot know the contents of files because of they don't have the knowledge of the keys.

In this if with the no. of data owners and the no. of revoked users linearly increasing the complexity of the user

participation and the revocation also increases respectively. In lu. et al proposed system, he designed the scheme by using a provenance scheme based on the cipher text policy ABE technique, which allows all the members to share the data with the group members. But in this scheme, the user revocation is not mentioned. In Yu et al proposed scheme, the KP-ABE technique is used for the scalable and fine grained data access control in the cloud computing systems. In this method the single owner manner is presented, where the user can store and share data. By combining all these technologies we can create a new system which is the multi-owner, secure sharing of data for the dynamic groups in the un trusted clouds.

II. LIERATURE SURVEY

In 2003, Kallahalla proposed a system named PLUTUS enables the secure file sharing on the un trusted cloud servers by using the cryptographic storage system.[5] In this method, the files are divided into the file groups and encrypting each group with a unique file block key. Now the data owner can share the file groups with the others by delivering the corresponding lock box keys, where the lock box key is used for encrypting the file-block keys. But this brings a heavy key distribution for the large amounts of file sharing and more additionally the file-block keys need to be updated every time when ever the user revocation occurs and the updated keys has to be distributed.

In 2003, the E.Goh and his team proposed a system named "SIRIUS" [6]. In that the files stored on the un trusted server include two parts: file metadata and file data. In the file meta data it include a series of encrypted key blocks and each one is encrypted by the public key of the authorized users. Here also the user revocation is an intractable issue for the large-scale file sharing. Since every time the file's meta data also need to be updated. In the next version , the NNL construction is used for the efficient key revocation .But in this also whenever a new user joins in the group, there is no need to recomputed the private keys of the every user.

In 2005, Ateniese et.al proposed the proxy re encryptions for the secure distributed storage [7]. Here in this the concept of encryption computation overhead increases with the data sharing rate. In this the data owner encrypts the data with the two types of keys like unique and symmetric content keys. These two keys are further encrypted by a master public key. Here for the access control, the server uses proxy cryptography to directly re encrypt the keys with the master public key granted user's public key. But when any revoked users can be launched they will be able to learn the decryption keys.

In 2010, Yu.et.al proposed a scalable and fine grained data access control scheme in the cloud computing [4] by using the KP-ABE technique. In this scheme, the data owners encrypt the file with a rand key where this random key is further encrypted with a group of attributes y using the KP-ABE and the respected secret keys to the authorized users, then the user can only decrypt the cipher text if the data file attributes match with the access structure. To achieve the user revocation the cloud servers takes the responsibility from manager of the tasks such as file re encryption and the secret key updates. Here in this scenario, the single owner manner may create the problem with the implementation of applications where all the users can share data with the others.

In 2010 the Lu.et.al proposed the secure provenance scheme [8]. In this they implemented the group signatures and the cipher text policy ABE techniques. In this scheme the system is set with a single attribute. In this method the user gets two keys after the registration. The two keys are group signature key and the remaining users in the same group can decrypt the data with their group signature key for the privacy preserving and traceability. But in this scheme the user revocation is not presented.

By Observing all this analysis we have a greater challenging issue that is how we can securely share data with the others by the multiple-owner manner for the dynamic groups in the un trusted cloud along with preserving identity privacy. Now in this project, we are proposing a new protocol MONA, for secure data sharing in the cloud computing along with the dynamic groups.

III. EXISTING SYSTEM

Up to now we have seen several methods for secure sharing of data in the cloud, but most of them failed in providing the required features. In all the methods the MONA[1] given the best solution for the existing problems. Here the MONA offers some unique features when compared with the others. Any group member can share data files with others and can also store the data files in the cloud. In this the number of revoked users is independent with the complexity of encryption and also the size of cipher texts. There is no need of updating the private keys of the remaining users whenever the user revocation occurs. The new users can directly access the files that are stored n the cloud without their participation. Here the storage overhead and the computation cost are constant.

Fig 1: Existing System Model

Disadvantage of MONA:-

In this the reliability and scalability decreases if the group manager fails to work whenever there are more number of requests or if the group manager is not available to give the access permissions to the group members.

IV. PROPOSED SYSTEM

In the proposed system for increasing the reliability and scalability in MONA, we are proposing the new model for MONA. In this method we are proposing a method, how we are managing the risks like the failure of group manager or hanging of group manager if there are more number of requests by sharing the workload in the multiple group managers. So that the reliability and scalability can be increased.

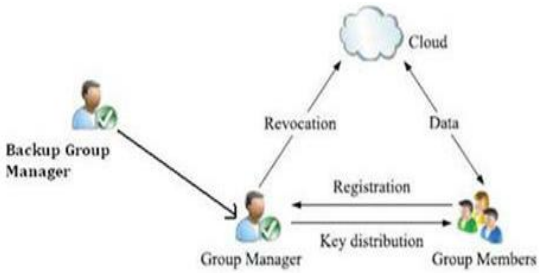

Fig 2.Proposed System Model

Advantage of Proposed System:-

To defeat the disadvantage of existing system MONA, here if the group manager fails to work with the large number of requests there is a backup group manager to share the work.

V. IMPLEMENTATION

Here in the implementation procedure of the proposed scheme starts with the group members registration. Whenever the group members request is accepted by the group manager or backup group manager. Here the group manager and the backup group manager work is same. If the group manager fails to work then backup group manager acts like the group manager. Whenever the group member registered with the group than a group signature is send to the group members mail. And whenever the group members uploaded a file the file key is generated. This file key generation and verification is done by using the Triple DES (3 DES) algorithm for security purpose.

Key Generation &Verification:-

The function of file key generation follows an encrypt-decrypt-encrypt (EDE) sequence.

Encryption

$$C = E_{K3}(D_{K2}(E_{K1}(P)))$$

first encrypt the plain text with the k1. $a= E_{K1}(P)$

Then decrypt the text by using the k2. $b=D_{K2}(a)$

Again perform the encryption by using k3. $C=E_{K3}(b)$

Decryption

$$P = D_{k1}(E_{k2}(D_{k3}(C)))$$

First decrypt the text by using the k3. $b= D_{K3}(C)$

Then encrypt the text by using the k2. $a=D_{K2}(b)$

Again perform the decryption by using k1. $C=E_{K3}(a)$

Where P=Plain text, C=Cipher text

VI. CONCLUSION

The cloud computing providing various services for the business environment in a cost effective manner. There is a method MONA a secure multiple user data sharing for the dynamic groups in the cloud. In this we are proposing a new approach in the MONA for achieving more reliability and scalability. In this method we are allowing the dynamic group managers for solving the risks like group manager failure to handle more no. of requests or the hanging of group manager .So that the efficiency, reliability and scalability increases more effectively.

REFERENCES

[1] Xuefeng Liu,Yuqing,Zhang,Boyang Wang, and Jingbo Yan,"Mona:Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,VOL.24,No.6,JUNE 2013

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53,no. 4, pp. 50-58, Apr. 2010.

[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,"Proc.IEEE INFOCOM,pp. 534-542, 2010.

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

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

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

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,"Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.

[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[11] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

