International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2172846

Attribute-Based Privacy-Preserving Data Sharing for Dynamic Groups in Cloud Computing

K. V. Uma Maheswari[1], Dr. Dhanaraj Cheelu[2]

[1]M.Tech Student, Department of CSE, Dr. K. V. Subba Reddy Institute of Technology, Kurnool, Andhra Pradesh, India

[2]Professor, Department of CSE, Dr. K. V. Subba Reddy Institute of Technology, Kurnool, Andhra Pradesh, India

Article Info
Volume 7, Issue 2
Page Number: 585-590

Publication Issue :
March-April-2021

Article History
Accepted : 25 April 2021
Published : 30 April 2021

ABSTRACT

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource sharing and low maintenance characteristics. Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, when sharing the data in a group while preserving data, identity privacy is still a challenging issue due to frequent change in membership. In overcome this problem, a secure data sharing scheme for dynamic groups is proposed so that any user within a group can share the data in a secure manner by leveraging both the group signature and dynamic broadcast encryption techniques. It should enable any cloud user to anonymously share data with others within the group and support efficient member revocation. The storage overhead and encryption computation cost are dependent on the number of revoked users.

Keywords : Cloud Computing, Data Sharing, Privacypreserving, Access Control, Dynamic Groups

I. INTRODUCTION

Attribute-based encryption (ABE) is a talented cryptographic come up to that achieve a fine-grained data access control. It provides a way of major access policy based on different attributes of the requester, environment, or the data object. Especially, ciphertext policy attribute-based encryption (CP-ABEenable an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher text, and implement it on the contents. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy. This successfully eliminates the need to rely on the data storage server for prevent unauthorized data access, which is the traditional access control approach of such as the reference monitor. however applying CP-ABE in the data sharing systemhas several challenge. In CPABE, the key cohort center (KGC) generates private keys of users by applying the KGC's master secret keys to users' linked set of attributes. Thus, the major benefit of this approach is to largely reduce the need for dispensation and storing public key certificates under traditional public key infrastructure (PKI).

However, the advantage of the CP-ABE comes with a major drawback which is known as a key escrow trouble. The KGC can decrypt every ciphertext addressed to specific users by generating their attribute keys. This could be a potential threat to the data confidentiality or privacy in the data sharing systems. Another challenge is the key revocation.

Since some users may change their relate attributes at some time, or some private keys power be compromised, key revocation or update for each attribute is needed in order to make systems secure. This issue is even more difficult especially in ABE, since each attribute is imaginably shared by multiple users (henceforth, we refer to such a set of users as an attribute group). This imply that revocation of any attribute or any single user in an quality group would affect all users in the group. It may result in traffic jam during rekeying procedure or security dreadful conditions due to the windows of susceptibility.

We proposed a secure provenance scheme based on the ciphertext-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. unhappily, the single owner manner hinders the adoption of their scheme into the case, where any user is granted to store and share data. Our donations. To solve the challenges presented above, we propose Mona, a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this paper include:

1. We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.

2. Our proposed scheme is able to support active groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their sharing without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoke users.

3. We provide secure and privacy-preserving access control to users, which guarantee any member in a group to secretly utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when dispute occur.

4. We provide exact security analysis, and perform extensive simulations to show the efficiency of our scheme in terms of storage and computation overhead.

II. RELATED WORK

In, Kallahalla et al. proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the filegroups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key sharing overhead for largescale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation. In files stored on the untrusted server include two parts: file metadata and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the public key of authorized users. Thus, the size of the file metadata is proportional to the number of authorized users. The user revocation in the scheme is an intractable issuem specially for large-scale sharing, since the file metadata needs to be updated. In their addition version, the NNL construction is used for efficient key revocation. However, when a new user

joins the group, the privatekey of each user in an NNL system needs to be recomputed, which may limit the
application for dynamic groups. Another concern is that the computation overhead of encryption linearly increases with the sharing scale. Ateniese et al. leveraged proxy re encryptions to secure distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly reencrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launch, which enables them to learn the decryption keys of all the encrypted blocks.
In, Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the KPABE technique. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KPABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a ciphertext if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file reencryption and
user secret key update to cloud servers. However, the singleowner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others. Lu et al. proposed a secure provenance scheme, which is built upon group signatures and ciphertext-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs encrypted data with her group signature key for privacy preserving and traceability. nevertheless, user revocation is not supported in their scheme. From the above analysis, we can view that how to securely share data files in a multiple-owner
manner for dynamic groups while preserving identity privacy from an untrusted cloud remains to be a challenging issue. In this paper, we propose a novel Mona protocol for secure data sharing in cloud compute. Compared with the accessible works, Mona offers unique features as follows:
1. Any user in the group can store and share data files with others by the cloud.
2. The encryption complication and size of cipher texts are independent with the number of revoked users in the system.
3. User revocation can be achieved without updating the private keys of the remaining users.
4. A new user can directly decrypt the files stored in the cloud before his participation.

III. PROPOSED SCHEME

The proposed scheme is to secure the data against unauthorized access by enforcing access control mechanisms. Basic solution to secure the data over the untrusted cloud is to encrypt the data using attribute-based encryption to achieve secure data sharing for dynamic groups in the cloud by combining both the group signature and dynamic broadcast encryption techniques. The short group signature introduced by Chaum and van Heist scheme, which enables users to anonymously use the cloud resources provided by cloud service providers is used; it also supports efficient user revocation and provides secure and privacy-preserving access control to users, which guarantee any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur within the group through the group signature.

Only the members of the group can create valid group signatures. Figure 1 show how the group members register with the group owner and how the data is shared between the group members from the cloud server.

Figure 1: System Architecture

The dynamic broadcast encryption technique allows data owners to securely share their data files with other users within the group including newly joined users. Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme such that revoked users cannot access the data after their revocation from the group. This results in both computation overhead of the encryption and the size of the cipher-text increases with the number of revoked users. Thus, the heavy overhead and large cipher-text size may hinder the adoption of the broadcast encryption to the limited users.

The group manager is allowed to compute the revocation parameters, which includes the list of revoked users and make this revocation list available to public by migrating them into the cloud. Each time when users request for the data cloud service provider verifies the revocation list and provide access to data only to active users in the group.

Such a design can significantly reduce the computation overhead of users to encrypt files and the cipher-text size.

IV. ALGORITHMS USED

The algorithms used in the proposed system are as follows:

Algorithm 1: Signature Generation

This algorithm is used to generate the signature for group users.Each individual user within the group must generate a valid signature.

Step1: start

Step2: Input: Private keys (Ai, xi), system parameter (P, U,V,H,W) and data M.

step2: Output: Generate a valid group signature on M.

step3: begin

step4: Select random numbers Set (t1, t2, t3, r1, r2, r3) And set x1=a and x2= b

Step5: Compute the following values t1, t2, t3, r1, r2, r3.

Step6: compute the challenging c c=h (m, t1, t2, t3, r1, r2, r3, r4, r5) using Hash function.

Step7: using c construct the Values s, s2, s3, s4, s5

Step8: Output the signature computed as gsp=(t1,t2,t3,c,s1,s2,s3,s4,s5)

Step9: stop

Algorithm 2: Signature Verification

This algorithm is used to verify the group sign and individual user sign during the data sharing from the cloud server.

Step1: start

Step2: perform the verification for P and q

Step3: verify that Q is a factor of p-1, if Any of the checks fail then the Signature cannot be verified.

Step4: verify that r and s are in the range [1,q-1]

Step5: compute w=(s^-1) modq

Step6: compute u1=m*w modq

Step7: compute u2=r* w modq

Step8: compute

v = (g^u1,y^u2) modp)modq

Step9: compare v and r if they are matched signature verified

Step10: stop

Algorithm 3: Revocation Verification

This algorithm is used by the active users to check if any users within the group revoked from the group.

Step1: Input: System parameter (p, q, r), a group signature M and a set of revocation keys A1..Ar.

step2: Output: Valid or Invalid.

Step3: begin

Step4: set temp = e = (T1,Q)

e2 = (t2.R)

For i=1 to n

If e (t3-Ai,p) Return null

Step5: else return temp

Step6: stop

V. EXPERIMENTAL ANALYSIS

In the proposed system, the group manager needs to store the user list and shared data. A system with 200 users with an assumption that each user shares 50 files on an average is considered. Then, the total storage of the group manager could be not more than 28.5Kbytes, which is acceptable. Group members need to store only their individual private key which is about 60 bytes. The extra storage overhead to store the file in the cloud is about 248 bytes only.

Therefore, the analysis on the proposed approach shows that the utilization of storage space among different model is low. Thus, it is acceptable in real practical usage.

VI. CONCLUSION

A secure data sharing scheme, for dynamic groups in an un-trusted cloud scheme allows a user to share data with others within the group without revealing data and identity privacy to the cloud. Additionally, it supports efficient user revocation and new user joining. More specifically, efficient user revocation can be achieved through a public revocation list without updating the private keys of remaining users and new users can directly decrypt files from the cloud before their participation.

VII. REFERENCES

[1]. P. Junod and A. Karlov, "An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies in Tenth annual ACM workshop on digital rights management. ACM, 2010, pp. 13–24.

[2]. Lam, S.S-zebeni, and L.Buttyan, "Invitation-oriented: Key management for Dynamic groups in an asynchronous communication model," Submitted to 4th International Workshop on Security in CloudComputing, 2012.

[3]. N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.

[4]. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with large Groups in the Cloud," in the Proceedings of ACNS 2012, June 2012,

[5]. B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," Information Theory, IEEE Transactions on, vol. 57, no. 3, pp. 1786–1802, march 2011.

[6]. 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.

[7]. Mahesh, Bhasutkar, Maninti Venkateswarlu, and M.Raghavendra. "End-to-end congestion control techniques for Router." 2011 International Conference on Communication Systems and Network Technologies. IEEE, 2011.

[8]. Mahesh, B., and K. Shyam Sunder Reddy. "Router Aided Congestion Control

Techniques." Second International Conference on Information Systems and Technology.

[9]. Mahesh, B. "Dynamic Update and Public Auditing with Dispute Arbitration for Cloud Data." Journal of Advanced Database Management & Systems 4.3 (2017): 14-19.

[10]. Mahesh, B., et al. "A Review on Data Deduplication Techniques in Cloud." Embedded Systems and Artificial Intelligence. Springer, Singapore, 2020. 825-833.Chin-Su Ko, K.Kim, R.Hwang, Y. Kim and S.Rhee, "Robust Audio Watermarking in wavelet domain using PN sequences", Proc. of ICIS-2005 published by IEEE. 120

[11]. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557.

[12]. H. Abu-Libdeh, L. Prince-house and H. Weather-spoon, RACS: a case for cloud storage diversity, ACM, 2010, pp. 229-240.

[13]. Taka-bi , H.; Joshi, J.B.D.; Ahn, G.; , "Security and Privacy Challenges in Cloud Computing," Security& Privacy, IEEE, vol.8, no.6, pp.24-31, Nov-Dec.2010. doi:10.1109/MSP.2010.186.

[14]. Kamara, Seny and Lauter, Kristin, Cryptographic cloud storage, FC'10 Proceedings of the 14th international conference on Financialcryptograpy and data security, pp.136-149, 2010.

Cite this article as :

K. V. Uma Maheswari, Dr. Dhanaraj Cheelu, "Attribute-Based Privacy-Preserving Data Sharing for Dynamic Groups in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 2, pp. 585-590, March-April 2021. Available at doi : https://doi.org/10.32628/CSEIT2172846
Journal URL : https://ijsrcseit.com/CSEIT2172846