ISSN: 2278 - 1323
International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)
Volume 2, Issue 6, June 2013

# Secure Policy Based Data Sharing for Dynamic Groups in the Cloud

**M. Kavitha Margret**

***Abstract–*** ***Major problem in public clouds is how to share documents based on fine-grained attribute based access control policies, sharing data in a dynamic groups while preserving data and identity privacy from an un trusted cloud is still a challenging issue, due to the frequent change of the membership., encrypting documents with different keys using a public key cryptosystem such as attribute based encryption (ABE), and/or proxy re-encryption (PRE) approach has some weaknesses: it cannot efficiently handle adding/revoking users or identity attributes, and policy changes; it requires to keep multiple encrypted copies of the same documents; it incurs high computational costs. In this paper, I propose a secure multi-owner attribute authorities based data sharing scheme for dynamic groups in the cloud. Tha aim of my paper is secure data sharing in a dynamic group where the there is no fixed Attribute authorities where as multi – owner attribute authorities scheme is possible. key policy key policy attribute-based encryption (KP-ABE) method is used to select dynamic AA (Attribute authorities ) . By leveraging group signature , signed receipts and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. As the result the computation cost is reduced and storage overhead and encryption computation cost of our scheme are independent with the number of revoked users so the encryption cost is also reduced .***

***Index Terms— Cloud computing, data sharing, dynamic groups, attribute- based encryption***

## I. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology [1] due to its in-trinsic resource-sharing and low-maintenance characteristics. One of the most fundamental services offered by cloud providers is data storage.Such cloud providers cannot be trusted to protect the confidentiality if the data . In fact, data privacy and security issues have been major concerns for many organizations utilizing such services. Data often encode sensitive information and should be protected as mandated by various organizational policies and legal regulations. Encryption is a commonly adopted approach to protect the confidentiality of the data. Encryption alone however is not sufficient as organizations often have to enforce fine-grained access control on the data. Such control is often based on the attributes of users, referred to as*identity attributes*, such as the roles ofusers in the organization, projects on which users are working and so forth. These systems, in general, are called *attribute based systems*. Therefore, an important requirement is to support fine-grained access control, based on policy spicier using identity attributes, over encrypted data. However, it also posesa significant risk to the confidentiality of those stored files. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [2].Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. First, identity Second, it is recommended that any memberin a group should be able to fully enjoy the datastoring and sharing services provided by the cloud,which is defined as the multiple-owner manner. Compared with the single-owner manner [3], Third, member revocation and signed receipt e.g., new member participation and currentmember revocation in a group . The changes of membership make secure data sharing extremely difficult, it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership re-vocation mechanism without updating of the secret keys of the remaining users minimize the complexity of key management , signed receipt is collected after every member revocation in the group it minimizes the multiple copies of encrypted file and also reduces computation cost.

***Manuscript received June, 2013.***

***M. Kavitha Margret** , received B.E (CSE) in 2004 from RVS college of Engineering, M.E (CSE) in 2007 from Jayaram college of engineering . Since 2010 she has been working as Assistant Professor in the department of Computer Science & Engineering, SVS college of engineering*

## II. RELATED WORKS

[4] proposed a cryptographicstorage system that enables secure file sharing a n untrusted servers, named Plutus. By dividing file into file groups and encrypting each file group with a unique lock group key, the data owner can share the file groups with others through delivering the corresponding group key, where the lock group-key is used to encrypt the lock-group keys. However, itbrings about a heavy key distribution overhead forlarge-scale file sharing. Additionally, the Lock group keyneeds to be updated and distributed again for a userrevocation.

In [5] untrusted server has two parts of files to be stored those : file metadata and file data. The file meta-data implies the access control information that includes a series of encrypted key blocks, each of which isencrypted under the symmetric key of authorized users.

It is proportional to the number of authorized users. The user revoca-tion in the scheme is an intractable issue especially

for large-scale sharing, since the file metadata needsto be updated. In their extension version, the NNLconstruction [10] is used for efficient key revocation.

However, when a new user joins the group, theprivate key of each user in NNL system needs tobe recomputed, which may limit the application fordynamic groups. Another concern is that, the compu-tation overhead of encryption linearly increases with the sharing-scale.

[6] To ensure security in distributed storage. Specifically the dataowner encrypts blocks of content with unique andsymmetric content keys. For access control, theserver uses proxy cryptography to directly re-encrypt through dynamically encrypted keys the appropriate content key(s) from the AA,s dynamically derived symmetric key. Unfortunately,a collusion attack between the untrusted server andany revoked malicious user can be launched, whichenables them to learn the decryption keys of all theencrypted blocks.

In [3], Yu *et al.* presented a scalable and fine-graineddata access control scheme in cloud computing basedon the key policy attribute-based encryption (KP-ABE) technique. The data owner uses a random key to encrypt a file, where the random key is furtherencrypted with a set of attributes using KP-ABE. Thenthe AA's for the group assigns an access structure andthe corresponding secret key to authorized users, suchthat a user can only decrypt a cipher text if and only if the data file attributes satisfy the access structure.

Toachieve user revocation, the manager delegates tasksof data file re-encryption and user secret key updateto cloud servers. The single-owner mannermay hinder the implementation of applications withthe scenario, where any member in a group should beallowed to store and share data files with others.

[7] proposed a secure scheme,which is built upon group signatures and policy attribute-based encryption techniques. The system in their scheme is set with a singleattribute. Each user obtains two keys after the registration:a group signature key and an attribute key. Thusany user is able to encrypt a data file using attributebasedencryption and others in the group can decryptthe encrypted data using their attribute keys. Meanwhile,the user signs encrypted data with her groupsignature key for privacy-preserving and traceability.

However, user revocation is not supported in theirscheme.From the above analysis, we can observe that howto securely share data files in a multiple-owner mannerfor dynamic groups while preserving identityprivacy from an untrusted cloud remains to be a challengingissue. The proposed scheme uses a protocol for secure data sharing in cloud computing.Compared with the existing works the new protocol offers

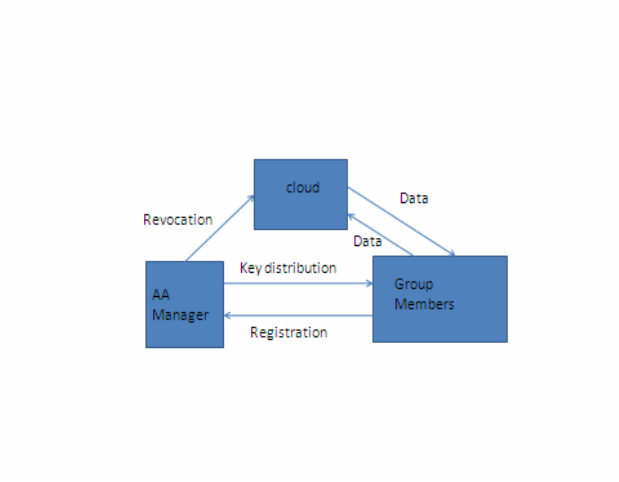
1) the user in the group can share and store data files with others by the cloud;

2) the complexity and size taken for encryption is 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 and signed receipts will be collected after any revocation that reduces duplication of encrypted copies ;

## III. PROPOSED SCHEME

### *A.System model*




*The system model consists of threedifferent entities: the cloud, a AAmanager and a large number of groupmembers as illustrated in Fig.1.*

Cloud is operated by Cloud Service Providers(CSPs) which provides abundant storage services.However, the cloud is not fully trusted Similar to [7], we assumethat the cloud server is honest-but-curious. That is, thecloud server will not maliciously delete or modifyuser data due to the protection of data auditing schemes[8], but will try to learn the content ofthe stored data and the identities of cloud users.AA Manager for group takes charge of system parametersgeneration, user registration, user revocation and revealingthe real identity of a dispute data owner. Inthe given example, the AA manager is acted by the administrator of an organization . Therefore, we assumethat the AA manager is fully trusted by the otherparties.

Group Members are a set of registered users thatwill store their private data into the cloud server andshare them with others in the group. In my example,

Each group has a members. Note that,

the group membership is dynamically changed, dueto the

member resignation and new member participationin an organization

*B. Design goals*

The main design goals ofthe proposed scheme including access control, dataconfidentiality, anonymity and traceability and efficiencyas follows.

Access Control: The requirement of access controlis two-fold. First, group members are able to use thecloud resource for data operations.

Second, unauthorizedusers cannot access the cloud resource at anytime, and revoked users will be incapable of usingthe cloud once again they are revoked.

Data Confidentiality: Data confidentiality requiresthat unauthorized users including the cloud are incapableof learning the content of the stored data . Animportant and challenging issue for data confidentialityis to maintain its availability for dynamic groups.New users should decrypt the data storedin the cloud before their participation, and revokedusers is unable to decrypt the data moved into thecloud after the revocation.

Anonymity and Traceability: Anonymity guaranteesthat group members can access the cloud withoutrevealing the real identity it enables effective protection for user identity itposes a potential inside attack risk to the system.

To tackle the inside attack, the group managershould have the ability to reveal the real identities ofdata owners.

Efficiency: The efficiency is defined as follows. Anygroup member can store and share data files withothers in the group by the cloud . User revocation canbe achieved without involving the remaining users and signed receipts will be collected after secure content sharing. the remaining users do not need to update

Data sharing :

To achieve privacy preserved data sharing for dynamic groups in the cloud , the scheme combines the group signature, signed receipt and dynamic broadcast encryption techniques.Specially, the group signature and signed receipt scheme enables usersto anonymously use the cloud resources, and thedynamic broadcast encryption technique allows dataowners to securely share their data files with othersincluding new joining users.

Unfortunately, each user has to compute revocationparameters to protect the confidentiality from therevoked users in the dynamic broadcast encryptionscheme, which results in that both the computationoverhead of the encryption and the size of the cipher text increase with the number of revoked users. Thus the Large cipher text size may hinder the adoption of the broadcast encryptionscheme to capacity-limited users.To tackle this challenging issue, let the groupmanager compute the revocation parameters andmake the result public available by migrating theminto the cloud. Such a design can significantly reducethe computation overhead of users to encrypt filesand the ciphertext size. Specially, the computationoverhead of users for encryption operations and theciphertext size are constant and independent of therevocation users.

## IV. RESULTS AND DISCUSSION

The proposed scheme of storage into cloud server is demonstrated using the private cloud setup with open stack. The SQL server 2005 andvisual studio 2008 is used for building the ASPX pages that are used in demonstration of the proposed work.

Microsoft Visual Studio 2008 helps individual developers accelerate solution development. Deliver breakthrough user experiences for all the users. It effectively building solutions for the Web, Windows, the Microsoft Office system, and Windows Mobile.

Visual Studio is a complete set of development tools for building ASP.NET Web applications, XML Web Services, desktop applications, and mobile applications. Visual Basic, Visual C#, and Visual C++ all use the same integrated development environment, which enables tool sharing and eases the creation of mixed-language solutions. In addition, these languages use the functionality of the .NET Framework, which provides access to key technologies that simplify the development of ASP Web applications and XML Web Services.

Regardless of which platform is being targeted, Visual Studio 2008 delivers the productivity, performance, and stability required to help developers remain focused on the real business challenges, along with a broad ecosystem that helps ensure they can always find the partners, information, and other community members to help them deliver great software. Also included is SQL Server 2005 Compact

Edition, SQL Server 2005 Express Edition and MSDN Express documentation.

The following are the visual studio 8 run-time member functions that are involved in the proposed system.

Math Functions – math functions are used to implement RSA algorithms which is used to encrypt the data fields (attributes ) in the data base.

Conversion Functions – conversion functions are to implement KP- ABE , which ensures dynamic policy changes.

- Type Conversion Functions
- String Functions
- Math Functions
- CType Function

## V. CONCLUSION

In this paper, I design a secure data sharing scheme, for dynamic groups in an untrusted cloud. In this scheme a user is able to share data with others in thegroup without revealing identity privacy to the cloud. Secure policy supports efficient user revocationand new user joining. Efficient userrevocation can be achieved through a public revocation list without updating the private keys of theremaining users, and new users can directly decryptfiles stored in the cloud before their participation.Extensive analysesshow that the proposed scheme satisfies the desiredsecurity requirements and it guarantees efficiency aswell.

## REFERENCES

[1] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. of FC, January 2010, pp. 136-149.
[2][1] M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, andM. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, Apirl 2010.
[3] S. Yu, C. Wang, K. Ren, and W. Lou," Achieving secure, scalable,and fine- grained data access control in cloud computing," inProc. of INFOCOM, 2010, pp. 534-542.
[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Scalable secure file sharing on untrusted storage," in Proc. OfFAST, 2003, pp. 29-42.
[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius:Securing remote untrusted storage," in Proc. of NDSS, 2003, pp.131-145.
[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improvedproxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS, 2005, pp. 29-43.
[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance:The Essential of Bread and Butter of Data Forensics in CloudComputing,", in Proc. of AISIACCS, 2010, pp. 282-292.
[8] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-SizeCiphertexts or Decryption Keys," in Proc. of Pairing, 2007, pp.39-59.
[9] D. Chaum and E. van Heyst, "Group Signatures," in Proc. Of EUROCRYPT, 1991, pp. 257-265.
[10] A. Fiat and M. Naor, "Broadcast Encryption," in Proc. Of CRYPTO, 1993, pp. 480-491.

*Mrs. M.Kavitha Margret received B.E (CSE) in 2004 from RVS college of Engineering, M.E (CSE) in 2007 from Jayaram college of engineering . Since 2010 she has been working as Assistant Professor in the department of Computer Science & Engineering, SVS college of engineering . Her Research interests include Operating System, Virtualization Techniques, and Cloud Computing*