



# Secure Data Sharing For Manifold Users in the Cloud

A.Mercy<sup>1</sup>, C.Hariram<sup>2</sup>

P.G Scholar, Department of IT, Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, India<sup>1</sup>  
Asst. Professor, Department of IT, Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, India<sup>2</sup>

**Abstract:** Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Cloud computing has a character of low maintenance which will provide an effective solution to share resource among group of users in the cloud. Major problem in public cloud is how to share data's and documents based on fine grained access control policies, due to frequent change of the membership data sharing in dynamic groups to preserve data and identity privacy from a cloud which is a untrusted one is still a challenging issue. Encrypting the Document with different key such as Attribute Based Encryption and Proxy Re-Encryption has many draw backs. In this paper, we propose a privacy preserved multi owner data sharing scheme by leveraging group signature, signed receipts and Advance Encryption Standard techniques, any cloud user can anonymously share data with others. At the same time overhead in the storage and computation cost for encryption of our scheme for the number of users revoked are independent additionally, we also analyze schemes security with rigorous proofs.

**Keywords:** Cloud computing, Data sharing, Dynamic group, Group signature, AES.

## I. INTRODUCTION

Cloud computing is a class of the next generation highly scalable distributed computing platform in which computing resources are offered 'as a service' leveraging virtualization and Internet technologies. Cloud computing can also be defined as "a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers". Cloud-based services include various commercial models are developed that are described by "X as a Service (XaaS)" where X could be Infrastructure, Software, Platform or Education etc . Amazon's Elastic Compute Cloud (EC2) and IBM's Blue Cloud are examples of cloud computing services. These cloud service providers allow users to instantiate cloud services on demand and thus purchase precisely the capacity they require when they require based on pay-per-use or subscription-based model.

Although cloud computing provides a number of advantages that include economies of scale, dynamic provisioning, increased flexibility and low capital expenditures, it also introduces a range of new security risks. The biggest concerns about cloud computing are security and privacy. A client can log into Cloud from any location to access data and applications. Cloud computing will need to

find ways to protect client privacy. One way is to use authentication techniques such as user names and passwords. Another is to employ an authorization format -- each user can access only the data and applications relevant to his or her job. Cloud has centralized server administration system. Centralized server administers the system, balances client supply, adjusts demands, and monitors traffic. In Cloud Computing it is very common to store data of multiple customers at one common location. Another concern is data access in cloud. These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of users. Cloud computing should have provide proper techniques for data security and confidentiality.

Several security schemes for data sharing on untrusted servers have been proposed [1], [2], [3]. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, a secure provenance scheme based on the ciphertext-policy attribute-based encryption technique [5], 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. [4] presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case, where any user is granted to store and share data.

In this paper we address, First, identity Second, it is recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner [4], Third, member revocation and signed receipt e.g., new member participation and current member 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.

## **II. RELATED WORKS**

### **A. Plutus: Scalable Secure File Sharing on Untrusted Storage**

M. Kallahalla et al.[1] presented the Plutus a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. They explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. They have built a prototype of Plutus on Open AFS. Measurements of this prototype show that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.

### **B. Sirius: Securing Remote Untrusted Storage**

E. Goh et al.[2] presented a Sirius, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. Sirius assumes the network storage is untrusted and provides its own read-write cryptographic

access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by Sirius using hash tree constructions. Sirius contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to Sirius include large scale group sharing using the NNL key revocation construction. Our implementation of Sirius performs well relative to the underlying file system despite using cryptographic operations. Sirius contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Using cryptographic operations implementation of Sirius also possible. It only uses the own read write cryptographic access control. File level sharing are only done by using cryptographic access.

### **C. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing**

S. Yu et al.[4] presented a scalable and fine-grained data access control scheme in cloud computing based on 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 further encrypted with a set of attributes using KP-ABE. Then the AA's for the group assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file re-encryption and user secret key update to cloud servers. The single-owner 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.

### **D. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing**

C. Wang et al.[6] proposed a cloud storage system, consisting of a collection of storage servers, provides long-term storage services over the Internet. Storing data in a third party's cloud system causes serious concern over data confidentiality. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. They propose a threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user





without retrieving the data back. The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. Our method fully integrates encrypting, encoding, and forwarding. They analyze and suggest suitable parameters for the number of copies of a message dispatched to storage servers and the number of storage servers queried by a key server.

#### *E. Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud*

B. Wang et al.[7] focused on cloud computing and storage services, data is not only stored in the cloud, but routinely shared among a large number of users in a group. It remains elusive, to design an efficient mechanism to audit the integrity of such shared data, while still preserving identity privacy. In this paper, they propose Knox, a privacy-preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group. In particular, they utilize group signatures to construct homomorphic authenticators, so that a third party auditor (TPA) is able to verify the integrity of shared data. Meanwhile, the identity of the signer on each block in shared data is kept private from the TPA. With Knox, the amount of information used for verification, as the time it takes to audit with it, are not affected by the number of users in the group. In addition, Knox exploits homomorphic MACs to reduce the space used to store such verification information. Our experimental results show that Knox is able to efficiently audit the correctness of data, shared among a large number of users. Scalable and rising trend which prompts a number of interesting security issues, many of which have been extensively investigated in the past. Provable Data Possession (PDP) is a topic that has only recently appeared in the research literature

#### *F. Cryptographic Cloud Storage*

S. Kamara et al.[8] proposed a security for customers to store and share their sensitive data in the cryptographic cloud storage. It provides a basic encryption and decryption for providing the security. However, the revocation operation is a sure performance killer in the cryptographic access control system. To optimize the revocation procedure, they present a new efficient revocation scheme which is efficient, secure, and unassisted. In this scheme, the original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. Thus, the

revocation process is accelerated by affecting only one slice instead of the whole data. They have applied the efficient revocation scheme to the cipher text-policy attribute-based encryption based cryptographic cloud storage. The security analysis shows that the scheme is computationally secure.

From the above analysis, we can observe 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. 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

Providing rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead. Tackle this challenging issue, we let the server compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the ciphertext size. Specially, the computation overhead of users for encryption operations and the ciphertext size is constant and independent of the revocation users.

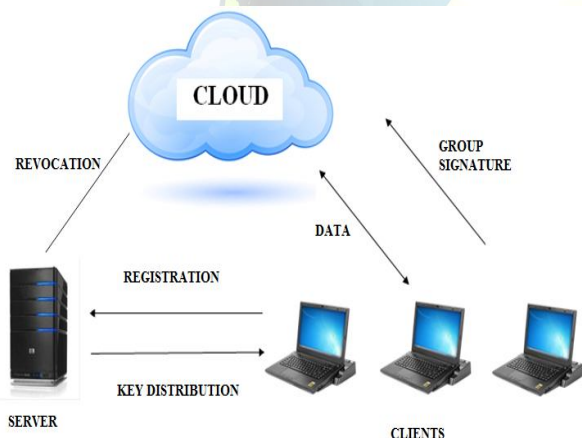
### **III. EXISTING SYSTEM**

To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task. In the existing System data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. The drawback of existing system is that only the group manager can store and modify data in the cloud. The changes of membership make secure data sharing

extremely difficult the issue of user revocation is not addressed.

#### IV. PROPOSED SYSTEM

A secure multi-owner data sharing scheme is proposed in this paper. It implies that any user in the group can securely share data with others in the untrusted cloud and has the ability to support dynamic groups efficiently. Specifically, newly participated users can directly decrypt data files uploaded before their participation without contacting the corresponding data owners. The size and computation overhead of encryption are considered to be constant and are independent with the number of revoked users. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. Group manager distributes and efficiently allocates the public keys and authenticate by using digital signature process. User revocation from a group is easily achieved by a revocation list without updating the secret keys of the remaining users. Thus the system provides secure and privacy-preserving access control to users and also guarantees that any member in a group can utilize the cloud resource.



**Figure 1. System Design**

To solve the above challenge, we propose a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this paper include a secure sharing scheme for multi-owner. It implies that any user in the group can securely share data with others by the untrusted cloud. Our scheme will support dynamic groups efficiently. Specifically, decryption can be done directly without contacting the data owner. A Novel revocation list which contains the secret keys without updating is used for

user revocation. The size and computation overhead of encryption remains constant and independent with the number of revoked users.

##### A. Components

**Cloud** is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to [4], we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

**Server** takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. For example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties.

**Client** are a set of registered users that will store the private data into the cloud server and share them with others in the group. They are responsible for selecting the group owner as well the group manager if needed. For example the staff will play this role. The membership is dynamic so that any staff can resign and new employee can participate in the company.

##### B. Design goals

**Access Control:** The group members are able to use the cloud resource for data operations. Unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud once again they are revoked.

**Data Confidentiality:** An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. New users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud.

**Anonymity and Traceability:** Anonymity guarantees that group members can access the cloud without revealing the real identity it enables effective protection for user identity.

**Efficiency:** Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users.

**Data sharing:** To achieve privacy preserved data sharing for dynamic groups in the cloud, the scheme combines the



group signature, signed receipt and Advance Encryption Standard techniques.

### C. Group Signature

A Group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group which introduced by David Chaum and Eugene van Heyst in 1991. For example, a group signature scheme could be used by an employee of a large company where it is sufficient for a verifier to know a message was signed by an employee, but not which particular employee signed it. Essential to a group signature scheme is a group owner and group manager, who is in charge of adding group members and has the ability to reveal the original signer in the event of disputes. A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability. In this paper, a variant of the short group signature scheme [12] will be used to achieve anonymous access control, as it supports efficient membership revocation.

### D. Advance Encryption Standard Algorithm

Encryption is the process of converting plain text into cipher text. Decryption is the process of converting cipher text to plain text. In our paper for both encryption and decryption uses Advance Encryption Standard Algorithm. AES is the Standard Algorithm. AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. Characteristic of AES is that, Resistance against all known attacks, Speed and code compactness on a wide range of platforms and Design Simplicity. The advantages of AES is that, prevent destruction of data by malicious writers, to detect and prevent unauthorized data modifications, prevent known plaintext attacks with different keys for different files, revoke readers and writers to differentiate between read and write access to files, minimize the number of keys exchanged between users.

#### a. Inner Workings of a Round

The algorithm begins with an **Add round key** stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the **Mix Columns** stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the **Inverse Mix Columns** stage. Each of these stages will now be considered in more detail.

## V. SCHEME DESCRIPTION

**Cloud Computing:** In cloud computing, the word cloud is used as a metaphor for "the Internet" so the phrase cloud computing means "a type of Internet-based computing," where different services -- such as servers, storage and applications -- are delivered to an organization's computers and devices through the Internet.

**System Initialization:** The group manager takes charge of system initialization as follows: Generating a bilinear map group system.

### Cloud Module

In this module, we provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

### Server Module

Server takes charge of followings,

1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of a dispute data owner.

Therefore, we assume that the server is fully trusted by the other parties. The Server is the admin. The server has the logs of each and every process in the cloud. The server is responsible for user registration and also user revocation too.





### **Client Module**

Clients are a set of registered users that will

1. Store their private data into the cloud server and
2. Share them with others in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it.

### **File Security Module**

1. Encrypting the data file.
2. File stored in the cloud can be deleted by the data owner (i.e., the member who uploaded the file into the server).

### **Group Signature Module**

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

### **User Revocation Module**

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

## **VI. CONCLUSION**

In this paper, we design a secure data sharing scheme, for dynamic groups in an untrusted cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Its supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

## **REFERENCES**

- [1]. 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.
- [2]. 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.
- [3]. 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.
- [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]. 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.
- [6]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.
- [7]. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.
- [8]. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.
- [9]. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.
- [10]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.
- [11]. 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.
- [12]. D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.
- [13]. N.Chandrakala Dr. P.Sivaprakasam " Analysis of Fault Tolerance Approaches in Dynamic Cloud Computing ", IJARCSSE, Volume 3, Issue 2, February 2013.
- [14]. Van den Bossche, R., Vanmechelen, K., Broeckhove, J.: —Cost Optimal Scheduling in Hybrid IaaS Clouds for Deadline Constrained Workloads. In: 3rd IEEE International Conference on Cloud Computing, Miami, July 2010.



- [15]. Wang, S. C., Yan, K. Q., Liao, W. P., Wang, S. S.: Towards a Load Balancing in a three level cloud computing network. In: Computer Science and Information Technology, pp. 108—113, 2010.
- [16]. R. M. Bryant and R. A. Finkel, "A Stable Distributed Scheduling Algorithm," in Proc. 2nd Int. Conf. Dist Comp., pp. 341-323, April 1981.
- [17]. D. Grosu and A. T. Chronopoulos, "Noncooperative Load Balancing in Distributed Systems," Journal of Parallel and Distributed Computing, vol. 65, no. 9, pp. 1022-1034, Sept. 2005.

#### About Author



**A. Mercy** received the B.Tech degree in Information Technology from Anna University, Chennai, in 2013. Currently, she is pursuing M.Tech degree in Information Technology from Anna University, Chennai. Her research areas of Interests include Data Mining, Cloud Computing, and Operating System.



**C. Hariram** has completed B.Tech in Information Technology from Sethu Institute of Technology, Madurai in 2006 and M.E in Computer Science Engineering from Manonmaniam Sundaranar University in 2010. He is now working as an Assistant Professor for 6 years in Dr. Sivanthi Aditanar College of Engineering, Tiruchendur. His research areas are Data Mining and Databases.