



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

Automated Security Providence for Dynamic Group in Cloud

V.Sathana^{#1}, J.Shanthini^{*2}

[#] M.E(Final Year), Department of CSE, Info Institute of Engineering, Coimbatore, Anna University, Chennai, India.

^{*}AP, Department of CSE, Info Institute of Engineering, Coimbatore, India.

ABSTRACT: Data sharing among group resource in the cloud server is a major problem, so cloud computing provides an efficient and economical solution. Due to the change of membership frequently, data sharing in a multi-owner manner to an untrusted cloud is a challenging issue. This proposal provides a secure data sharing scheme for dynamic group in the cloud, by providing AES encryption while uploading the data, any cloud user can securely share data with others. Meanwhile, the computation cost of encryption and storage overhead scheme are independent with the number of revoked users. In addition, this proposal analyze the security of this scheme with rigorous proofs. One-Time Password is the most popular and easiest forms of authentication that can be used for securing access to accounts. OTP are often referred to as a secure and stronger forms of authentication, and it installed across multiple machines. It provides a multiple levels of security to share data among multi-owner manner. First the user selects the text based password. Then the One-Time Password is automatically generated and sent to the corresponding e-mail account.

KEYWORD: Cloud computing, Broadcast encryption.

I. INTRODUCTION

Cloud computing is Internet ("cloud") based development and use of computer technology ("computing"). It is a style of computing in which dynamically scalable and often virtualization resources are provided as a service over the internet. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud.

First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable. Second, it is highly 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 [3], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company. Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

users to learn the content of data files stored before their participation, because 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 revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management. Several security schemes for data sharing an untrusted servers have been proposed [4], [5], [6]. 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

Our contributions. To solve the challenges presented above, we propose a secure multi-owner data sharing scheme for dynamic group in the cloud. The main contribution of this paper include:

To provide security for dynamic group we integrates Image based authentication and one time password to achieve high level of security.

The main Objective of providing a two levels of security is a unique and an esoteric study of implementation of an extremely secured system, employing 2 levels of security.

Level 1: Level 1 security provides a simple text based Password.

Level 2: After the successful entry of the above level, the Level 2 Security System will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his e-mail.

II. RELATED WORK

S. Kamara et al.[9] 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.

E. Goh et al.[7] 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 Ill 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.

A.Fiat et al.[6] proposed a system on multicast communication framework, various types of security threat occurs. As a result construction of secure group communication that protects users from intrusion and eavesdropping are very important. In this paper, They propose an efficient key distribution method for a secure group communication over multicast communication framework. In this method, They use IP multicast mechanism to shortest rekeying time to minimize adverse effect on communication. In addition, They introduce proxy mechanism for replies from group members to the group



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

manager to reduce traffic generated by rekeying. They define a new type of batching technique for rekeying in which new key is generated for both leaving and joining member. The rekeying assumption waits for 30 sec so that number time's key generation will be reduced.

M. Armbrust et al.[2] presented a security one of the most often-cited objections to cloud computing; analysts and skeptical companies ask “who would trust their essential data ‘out there’ somewhere?” There are also requirements for auditability, in the sense of Sarbanes-Oxley azon spying on the contents of virtual machine memory; it’s easy to imagine a hard disk being disposed of without being wiped, or a permissions bug making data visible improperly. There’s an obvious defense, namely user-level encryption of storage. This is already common for high-value data outside the cloud, and both tools and expertise are readily available. This approach was successfully used by TC3, a healthcare company with access to sensitive patient records and healthcare claims, when moving their HIPAA-compliant application to AWS [1]. Similarly, auditability could be added as an additional layer beyond the reach of the virtualized guest OS, providing facilities arguably more secure than those built into the applications themselves and centralizing the software responsibilities related to confidentiality and auditability into a single logical layer. Such a new feature reinforces the Cloud Computing perspective of changing our focus from specific hardware to the virtualized capabilities being provided

D. Boneh et al.[4] focused on a Hierarchical Identity Based Encryption (HIBE) system where the ciphertext consists of just three group elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth. Encryption is as efficient as in other HIBE systems. They prove that the scheme is selective-ID secure in the standard model and fully secure in the random oracle model. The system has a number of applications: it gives very efficient forward secure public key and identity based cryptosystems (with short ciphertexts), it converts the NNL broadcast encryption system into an efficient public key broadcast system, and it provides an efficient mechanism for encrypting to the future. The system also supports limited delegation where users can be given restricted private keys that only allow delegation to bounded depth. The HIBE system can be modified to support sublinear size private keys at the cost of some ciphertext expansion.

III. PRELIMINARIES

A. Group Signature

The concept of group signatures was first introduced in [15] by Chaum and van Heyst. In general, 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.

B. Dynamic Broadcast Encryption

Broadcast encryption [16] enables a broadcaster to transmit encrypted data to a set of users so that only a privileged subset of users can decrypt the data. Besides the above characteristics, dynamic broadcast encryption also allows the group manager to dynamically include new members while preserving previously computed information, i.e., user decryption keys need not be recomputed, the morphology and size of ciphertexts are unchanged and the group encryption key requires no modification. The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique in [14], which will be used as the basis for file sharing in dynamic groups.

IV. SYSTEM MODEL

We consider a cloud computing architecture by combining with an example that a company uses a cloud to enable its staffs in the same group or department to share files. The system model consists of three different entities: the cloud, a group



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

manager (i.e., the company manager), and a large number of group members (i.e., the staffs) 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 [3], [7], 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 [17], [18], but will try to learn the content of the stored data and the identities of cloud users. Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given 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. Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

A. Design Goals

In this section, we describe the main design goals of the proposed scheme including access control, data confidentiality, anonymity and traceability, and efficiency as follows:

Access control: The requirement of access control is to fold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, 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 after the revocation.

Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners.

Efficiency: The efficiency is defined as follows: 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. That is, the remaining users do not need to update their private keys or reencryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

V. PROPOSED SYSTEM

A. Overview

To achieve secure data sharing for dynamic groups in thecloud, we expect to combine the group signature anddynamic broadcast encryption techniques. Specially, thegroup signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryptiontechnique allows data owners to securely share their datafiles with others including new joining users.Unfortunately, each user has to compute revocationparameters to protect the confidentiality from the revokedusers in the dynamic broadcast encryption scheme, whichresults in that both the computation overhead of theencryption and the size of the ciphertext increase with thenumber of revoked users. Thus, the heavy overhead andlarge ciphertext size may hinder the adoption of thebroadcast encryption scheme to capacity-limited users.To tackle this challenging issue, we let the groupmanager compute the revocation parameters and makethe result public available by migrating them into the cloud.Such a design can significantly reduce the computationoverhead of users to encrypt files and

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

the ciphertext size. Specially, the computation overhead of users for encryption operations and the ciphertext size are constant and independent of the revocation users.

Secure environments protect their resources against unauthorized access by enforcing access control mechanisms. So when increasing security is an issue text based passwords are not enough to counter such problems. Using the instant messaging service available in internet, user will obtain the One Time Password (OTP) after image authentication. This OTP then can be used by user to access their personal accounts. In this paper I one time password to achieve high level of security in authenticating the user over the internet.



Fig. 1. System Architecture.

The main Objective of 2 Level Security system is a unique and an esoteric study of using OTP and implementation of an extremely secured system, employing 2 levels of security.

Level 1: Security at level 1 has been imposed by simple text-based password.

Level 2: After the successful clearance of the above level, the Level 2 Security System will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his email id.

B. Admin or Group Owner

1. Group Creation

Groups are creating by admin. A company allows its staffs in the same group or department to store and share files in the cloud. 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.

2. User Registration

For the registration of user i with identity ID_i , the group manager randomly selects a number and characters for generate random key. Then, the group manager adds into the group user list, which will be used in the traceability phase. After the registration, user i obtains a private key, which will be used for group signature generation and file decryption.

3. Group Access Control

When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner. The employed group signature scheme can be regarded as a variant of the short group signature, which inherits the inherent unforgeability property, anonymous authentication, and tracking capability.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

4. File Deletion

File stored in the cloud can be deleted by either the group manager or the data owner (i.e., the member who uploaded the file into the server). To delete a file ID data, the group manager computes a signature ID data and sends the signature along with ID data to the cloud.

5. Revoke User

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. The admin can only have permission for revoke user and remove revocation.

C. User Or Group Member

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group.

1. File Upload

To store and share a data file in the cloud, a group member checks the revocation list and verify the group signature. First, checking whether the marked date is fresh. Second, verifying the contained signature. Uploading the data into the cloud server and adding the ID data into the local shared data list maintained by the manager. On receiving the data, the cloud first to check its validity. It returns true, the group signature is valid; otherwise, the cloud stops the data. In addition, if several users have been revoked by the group manager, the cloud also performs revocation verification, the data file will be stored in the cloud after successful group signature and revocation verifications.

2. File Download

Signature and Key Verification

In general, 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.

3. OTP (One Time Password)

OTPs avoid a number of shortcomings that are associated with traditional passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize.

OTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

Generation of OTP Value

The algorithm can be described in 3 steps:

Step 1: Generate the HMAC-SHA value Let $HMK = \text{HMAC-SHA}(\text{Key}, T)$ // HMK is a 20-byte string

Step 2: Generate a hex code of the HMK. $\text{HexHMK} = \text{ToHex}(HMK)$

Step 3: Extract the 8-digit OTP value from the string

OTP = Truncate (HexHMK) the Truncate function in Step 3 does the dynamic truncation and reduces the OTP to 8-digit.

4. AES Encryption

The input 16 byte Plain text can be converted into 4×4 square matrix.

The AES Encryption consists of four different stages they are

Substitute Bytes: Uses an S-box to perform a byte-by-byte substitution of the block

Shift Rows: A Simple Permutation

Mix Columns: A substitution that makes use of arithmetic over $\text{GF}(2^8)$

Add Round Key: A Simple Bitwise XOR of the current block with the portion of the expanded key

5. AES Decryption

The Decryption algorithm makes use of the key in the reverse order. However, the decryption algorithm is not identical to the encryption algorithm

VI. CONCLUSION

In this paper, I 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, It 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. A new type authentication system, which is highly secure, has been proposed in this paper.

This system is also more users friendly. This system will definitely help thwarting Shoulder attack, Tempest attack and Brute-force attack at the client side. Though 3-Level Security system is a time consuming approach, it will provide strong security where we need to store and maintain crucial and confidential data secure. Such systems provide a secure channel of communication between the communicating entities. The ease of using &remembering images as a password also support the scope of these systems.

REFERENCES

- [1] X.Liu, B.Wang, Y.Zhang, and J.Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Computer Society, 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] G.Ateniese, R. Burns, R.urtmola, J.Herring, L. Kissner, Z. Peterson, and D.Song, "Deduplication in cloud storage using side channels in cloud services," Oct 2008.
- [4] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.
- [5] K. D. Bowers, A. Juels, and A. Oprea, "Hail: A high-availability and integrity layer for cloud storage," in Proc. Of CCS'09, 2009, pp. 187-198.
- [6] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.
- [7] 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.
- [8] 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.
- [9] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

- [10] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, pp. 46-50, 2008.
- [11] 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.
- [12] 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.
- [13] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Services Computing, pp. 1939-1974, 2011.
- [14] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and secure sensor data storage with dynamic integrity assurance," in Proc. of IEEE INFOCOM'09, Rio de Janeiro, Brazil, April 2009.
- [15] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in Proc. of IWQoS'09, July 2009, pp. 1-9.
- [16] 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.
- [17] 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.