IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 8, August 2014 ISSN 2321-5992

Anonymous Data Sharing Scheme for Dynamic Groups in an Untrusted Cloud

P Lavanya[1], S Komala[2] and N Vikram[3]

[1]P Lavanya, II MTech, CSE, Vemu College of Engineering and Technology, Chittoor, Andhra Pradesh, India,

[2]S Komala, Assistant Professor, CSE, Vemu College of Engineering and Technology, Chittoor, Andhra Pradesh, India,

[3]N Vikram, II MTech, CSE, Vemu College of Engineering and Technology, Chittoor, Andhra Pradesh, India,

ABSTRACT

The motivation of this paper is to propose a secure multi-owner data sharing scheme, for dynamic group in the cloud. We proposed a One-Time Password is one of the easiest and most popular forms of authentication that can be used for securing access to accounts. One-Time Passwords are often referred to as secure and stronger forms of authentication, and allowing them to install across multiple machines. We provide a multiple levels of security to share data among multi-owner manner. First the user selects the pre-selected image to login. Then selects an image from the grid of images. Then OTP is generated automatically and sent to corresponding e-mail account.

Keywords: Access Control, Anonymous data, Cloud Computing, Data sharing, Multi owner.

1. 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 [1], 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 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 [2], [3], [4]. 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. 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 Image based authentication is providing a three levels of security. It is a unique and an esoteric study of using images as password and implementation of an extremely secured system, employing 3 levels of security.

Level 1

Level 1 security provides a simple text based Password.

Level 2

In this security level the user has to select an image from the grid of images. It can eliminate the shoulder attack and the tempest attack.

Level 3

After the successful entry of the above two levels, the Level 3 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.

2. RELATED WORK

S. Kamara et al.[5] 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. HoIver, 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.[6] 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.[7] 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 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.[8] presented a security one of the most often-cited objections to cloud computing; analysts and sceptical 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 [9]. 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.[10] focused on a Hierarchical Identity Based Encryption (HIBE) system where the cipher text 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 cipher texts), 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 sub linear size private keys at the cost of some cipher text expansion.

3. SYSTEM MODEL AND DESIGN GOALS

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 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 [1], [6], 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 [11], [12], 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.

Fig-1 System Model

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 re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

4. PROPOSED SYSTEM

4.1 Overview

To achieve secure data sharing for dynamic groups in the cloud, we expect to combine the group signature and dynamic broadcast encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users. Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the cipher text increase with the number of revoked users. Thus, the heavy overhead and large cipher text size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To tackle this challenging issue, we let the group manager 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 cipher text size. Specially, the computations overhead of users for encryption operations and the cipher text 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.

4.2 Admin or Group Owner

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.

User Registration

For the registration of user i with identity IDi, 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..

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 forget ability property, anonymous authentication, and tracking capability. 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.

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.

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. 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.

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, we check 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 checks 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.

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.

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. Generation of OTP Value The algorithm can be described in 3 steps: Step 1: Generate the HMAC-SHA value Let HMK = HMAC-SHA(Key, T) // HMK is a 20-byte string Step 2: Generate a hex code of the HMK. HexHMK=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.

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 GF(2_8)

Add Round Key

A Simple Bitwise XOR of the current block with the portion of the expanded key

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

5. 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 the 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] 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.

[2] 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.

[3] 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.

[4] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

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

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

[7]] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Intl Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[8] 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.

[9] 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.

[10] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Intl Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

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

[12] 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.

[13] First Author (Year), "Manuscript Title", Proceedings / Conference Name, Vol. 1, No. 1, Pp. 10–15.

[14] D.A. First Author & B.S. Second Author (Year), "Book Title", Chapter No. (If any), Editors: First Editor Name & Second Editor Name, Publisher Name, Edition, Press, Place, Pp. 10-15.

AUTHOR

P Lavanya Pursuing M.Tech., CSE (II Year), Vemu Institute of Technology, Chittoor, Andhra Pradesh. Completed M C A from Sri Vidyanikethan Engineering College in 2009, persuing M.Tech CSE in VEMU, Chittoor, after MCA having 3 Years teaching Experience in Vemu College of Engineering & Technology, Chittoor . Areas of Interest Cloud Computing , Cryptography, Algorithms Design and Analysis Process . Attended one National Conference at SVCET Chittoor in the topic of Recent Trends in Computing.

S Komala, Asst. Prof., Vemu College of Engineering and Technology, Chittoor. B.Tech from JNTU in 2008, M.Tech from JNTU in 2011. Having 3 Years of experience in teaching in Vemu from 2011 to till date, Area of Interesting Data Mining, Cloud Computing, Big Data,Computer Networks. Attended 2 National & International Conferences, 2 journals.

Vikram Neerugatti Pursuing M.Tech., CSE (II Year), Global College of Engineering and Technology, Kadapa. B.Tech from JNTU in 2009, M.S from BRAINWELLS UNIVERSITY, UK. in 2010. MSc Psychology from SVU Thirupathi. Having 4 Years of experience in teaching in SVCE from 2010 to till date, Area of Interesting Data Mining, Computer Networks, Android Operating systems. Attended 3 National & International Conferences. 3 international Journals, attended 4 workshops, organized 3 workshops. Guided 5 UG level projects and 3 PG level projects.