Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 2, February 2016, pg.192 – 198

Security and Privacy Challenges in Large-Scale Cloud Computing using Signature Generation Algorithm

Gayathri.R[1], Subaira.A.S[2], Shanmugapriya.P[3]

[1]Assistant Professor, Department of Information Technology, Mahendra College of Engineering, Salem
[2]Assistant Professor, Department of Computer Science and Engineering, Mahendra College of Engineering, Salem
[3]Assistant Professor, Department of Information Technology, Mahendra College of Engineering, Salem

Abstract: In this paper, the secure data storage in clouds for a new decentralized access is proposed. Concerns like data leakage are common and can influence the original data owners drastically. Encrypting every data over the cloud which is a huge collection of data is not economically feasible. Signature Generation Algorithm (SGA) is proposed to authenticate the data access from the cloud to ensure the security of the data over cloud and their data sets. Evaluation results express that the secrecy and privacy of the data stored over the network is achieved efficiently and successfully.

Keywords— Security, data storage, decentralized access, encryption, Signature Generation Algorithm (SGA).

I. INTRODUCTION

Cloud computing is a computing environment, where resources such as computing power, storage, network and software are abstracted and provided as services on the internet in a remotely accessible fashion. With the rapid development of Internet and Cloud computing, there are more and more network resources. Sharing the resources, management and on-demand allocation of network resources are particularly important in Cloud computing. The Cloud has become a new vehicle for delivering resources such as computing and storage to customers on demand. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Considering a practical data application where a company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. But, 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 [21]. 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. The issues include preserving identity privacy, issues due to single ownership and maintaining dynamic groups.

A. Issues in secure data sharing:

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 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.

II. RELATED WORK

In [2], Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the KPABE technique. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager 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. However, 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.

In [3], Kallahalla et al. proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation. key needs to be key needs to be updated and distributed again for a user revocation updated and distributed again for a user revocation

Lu et al. [5] proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique [8], 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. [2] presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique [9]. Unfortunately, the single owner manner hinders the adoption of their scheme into the case, where any user is granted to store and share data.

Several security schemes for data sharing on untrusted servers have been proposed [3], [4], [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 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.

III. PROPOSED SYSTEM

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

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

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

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

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

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) as illustrated in Fig. 1.

Fig. 1. System model.

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.

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 computation overhead of users for encryption operations and the cipher text size are constant and independent of the revocation users.

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 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 nformation, 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.

Algorithm (1). Signature Generation

Input: Private key (A; x), system parameter (P;U;V ;H;W) and data M.
Output: Generate a valid group signature on M.

Algorithm (2). Revocation Verification

Input: System parameter (H0;H1;H2), a group signature g, and a set of revocation keys A1; :::;Ar
Output: Valid or Invalid.

begin
set *temp* = e(T1,H1) e(T2,H2)
for i= 1 to n
if e(T3,A, H0)=*tempr*
Return Valid
end if
end for
Return Invalid
End

IV. PERFORMANCE EVALUATION

In this section, we first analyze the storage cost of this scheme, and then perform experiments to test its computation cost.

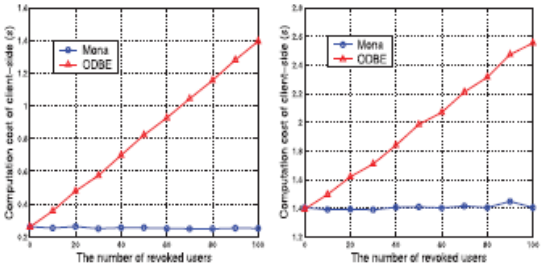
A. Simulation

To study the performance, we have simulated this scheme by using C programming language with GMP Library [22], Miracl Library [23], and PBC Library [24]. The simulation consists of three components: client side, manager side as well as cloud side. Both client-side and manager-side processes are conducted on a laptop with Core 2 T7250 2.0 GHz, DDR2 800 2G, Ubuntu 10.04 X86. The cloud-side process is implemented on a machine that equipped with Core 2 i3-2350 2.3 GHz, DDR3 1066 2G,Ubuntu 12.04 X64. In the simulation, we choose an elliptic curve with 160-bit group order, which provides a competitive security level with 1,024-bit RSA.

B. Client Computation Cost

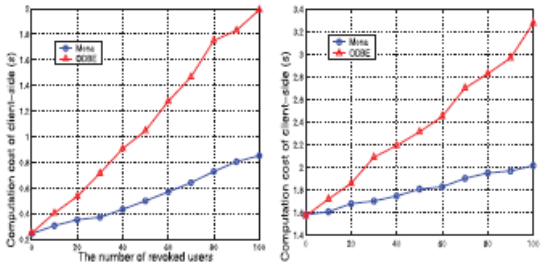
In Fig. 2, we list the comparison on computation cost of clients for data generation operations between Mona and the way that directly using the original dynamic broadcast encryption (ODBE) [14]. It is easily observed that the computation cost in Mona is irrelevant to the number of revoked users. On the contrary, the computation cost increases with the number of revoked users in ODBE. From Figs. 2a and 2b, we can find out that sharing a 10-Mbyte file and a 100-Mbyte one, cost a client about 0.2 and 1.4 seconds in our scheme, respectively, which implies that the symmetrical encryption operation domains the computation
cost when the file is large.

The computation cost of clients for file access operation with the size of 10 and 100 Mbytes are illustrated in Fig. 3. The computation cost in Mona increases with the number of revoked users. Therefore, Mona is still superior than ODBE in terms of computation cost. Similar to the data generation operation, the total computation cost is mainly determined by the symmetrical decryption operation if the accessed file is large, which can be verified from Figs. 3a and 3b. In addition, the file deletion for clients is about 0.075 seconds, because it only costs less.



(a) Generating a 10 MB file (b) Generating a 100 MB file

Fig. 2. Comparison on client computation cost for file generation between this scheme and ODBE.



(a) Accessing a 10 MB file (b) Accessing a 100 MB file

Fig. 3. Comparison on client computation cost for file access between this scheme and ODBE.

C. Cloud Computation Cost

To evaluate the performance of the cloud in Mona, we test its computation cost to respond various client operation requests including file generation, file access, and file deletion. Assuming the sizes of requested files are 100 and 10 MB, the test results are given in Table 3. It can be seen that the computation cost of the cloud is deemed acceptable, even when the number of revoked users is large. This is because the cloud only involves group signature and revocation verifications to ensure the validity of the requestor for all operations. In addition, it is worth noting that the computation cost is independent with the size of the requested file for access and deletion operations, since the size of signed message is constant.

Computation Cost of the Cloud (s)

Request	The number of revoked users		
	0	50	100
File generation (100 MB)	0.065	0.154	0.271
File generation (10 MB)	0.045	0.125	0.226
File access (100 MB)	0.045	0.150	0.237
File access (10 MB)	0.045	0.151	0.240
File deletion (100 MB)	0.041	0.153	0.240
File deletion (10 MB)	0.042	0.156	0.238

TABLE 1

V. CONCLUSION

In order to avoid the problem of data security, a secure data sharing scheme is designed for dynamic groups in an untrusted cloud. Each and every 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. The encryption complexity and size of cipher texts are independent with the number of revoked users in the system. 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] Xuefeng Liu; Yuqing Zhang; Boyang Wang; Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,", IEEE Transactions on Parallel and Distributed Systems , vol.24, no.6 Page(s)1182-1191, 2013.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, Page(s): 534 – 542, 2010.

[3]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, Page(s): 29 – 42, 2003.

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

[5] 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, Page(s):282-292, 2010.

[6]G. 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), Page(s):29-43, 2005.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), Page(s): 89-98, 2006.

[8] 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, Page(s): 507-525, 2012.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Page(s): 523-533, 2010.

[10] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, Page(s):46-50, 2008.

[11]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), .Page(s): 440-456, 2005.

[12]C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, Page(s): 39-59, 2007.

[13]D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), Pages 257-265, 1991.

[14]Nomir, O.; Abdel-Mottaleb, M.(2008), "Fusion of Matching Algorithms for Human Identification Using Dental X-Ray Radiographs", in IEEE Transactions on Information Forensics and Security, Volume: 3, Issue: 2 , Page(s): 223 – 233

[15]D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532, 2001.Pages 514-532, 2001.

[16]D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, Page(s): 361-396, 2000.

[17]S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), Page(s): 136-149, 2010.

[18]The GNU Multiple Precision Arithmetic Library (GMP), http:// gmplib.org/, 2013.

[19]D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), Page(s): 41-62, 2001.

[20]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.

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

