International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Enabling Secure Data Sharing Scheme in the Cloud Storage Groups

C.Pavani[1], S.Vasundra[2]

[1]*M.Tech, CSE Department, JNTUCEA, Ananthapuramu, AP, India.*
[2]*Professor, CSE Department, JNTUCEA, Ananthapuramu, AP, India.*

Abstract*--In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host the data. It helps clients to reduce economic overhead of data management by moving the local management system into cloud servers. However, security concern becomes the main constraint. To preserve data confidentiality, there is an approach to encrypt data files before the client upload the encrypted data into the cloud which is challenging task in active groups in the cloud. This paper proposes an Identity based ring signature for data sharing in the cloud storage groups. This system aims at offering forward security to massive amount of data sharing in the cloud. It also provides the authenticity and anonymity of the end users. The method can achieve secure key distribution, fine-grained access control, anti-collusion attack and secure user revocation.*

Keywords: Access control, privacy-preserving, key distribution, cloud computing, identity based ring signature.

1. INTRODUCTION

Now-a-days the internet has to support different technologies. One of the mainly popular technology is cloud computing. Cloud computing atmosphere provides the massive storages facility to the client. Now a days, cloud computing is a technology to allow the user accessing the data which stored in remote server. It can be easily and quickly accessible through the internet which has been pay per use on demand service. Cloud computing mainly used for business and organization and provide the huge amount of space for data sharing at low cost. Clouds are provided by many cloud computing service providers like Amazon, Drop box, Google app engine etc. Cloud provides one of the most essential services is data storage.

Data sharing between two members or group of members take several issues into account. They are efficiency, data integrity and privacy of data owner. Providing the privacy and the integrity are the most challenging tasks for dynamic groups.

The existing system provides a secure data sharing scheme for dynamic members [1]. Without using Secure Communication channels, this method uses key distribution in secure way such that group manager provides private keys to the users. The scheme can achieve fine-grained access control. It provides the security against collusion attack by using group signature which provides secure user revocation. Collusion attack means decryption of data by revoked user using his secret key and get secrete file by conspire with the cloud. Secure user revocation means the revoked users cannot get the original data file even if they conspire with the untrusted cloud. The scheme can achieve fine efficiency, which means previous users need not to update their private keys when either a new user joins in the group or a user is revoked from the group. Secure and efficient methods are needed to ensure integrity and privacy of data stored at the cloud [2].

Group signature [3] allows members of a specified group to sign message on behalf of the entire group that is without revealing their individual identities. Group signature has two properties 1) anonymity 2) traceability. Anonymity means that, it does not revel which specific group members form the signature. As in any privacy preserving applications, anonymity of the users is maintained as much as possible, but still need to be sure that there is a mechanism in place for misbehaving members of group to get caught. The group signature identifies the misbehaving users can be easily revealed with help of traceability property. But there are some security applications in which it's disagreeable for a signer identity to be revealed. It is violating the anonymity property of group signature. To overcome this drawback, this paper proposes the Identity Based Ring Signature [4]. This system aims at offering forward security to massive scale data sharing in the cloud.
Ring signature for data sharing inside the cloud provides secure data sharing using identity based ring signature within the group. It additionally provides the authenticity and anonymity of the end users. The proposed system avoids costly certificate keys for verification as in the conventional public key infrastructure setting which is a bottleneck. In Identity based ring signature, Leakage of secret key of any user doesn't make all preceding generated signatures invalid. The assets is especially important to any huge amount of data sharing system, as it is impossible to ask all data owners to re-authenticate their data even if a secret key of one single user has been revealed.

The remaining of the paper is organized as follows. In the section 2, related works are discussed. The proposed system is presented in detail in section 3 followed by results in section 4. Finally the conclusion is made in section 5.

2. RELATED WORK

Liu et al. [5] proposed a secure multi-owner data sharing scheme, named Mona. This scheme can attain fine-grained access control and revoke users will not be able to access the sharing data again once they are revoked. However, the scheme will easily suffer from the collusion attack by the revoked user and the cloud [6]. The revoked user can use his personal key to decrypt the encrypted data and get the secret data after his revocation through conspiring with the cloud. In the phase of document access, the revoked user sends his request to the cloud, and then the cloud responds the corresponding encrypted records file. After that, the revoked user can compute the decryption key with the help of the attack algorithm. At last, this attack can cause the revoked users getting the sharing data and disclosing other secrets of legitimate members.

Zhou et al. [7] proposed a secure access control scheme on encrypted data in cloud storage space by invoking role-based encryption technique. This method can achieve well-organized user revocation that combines role-based access control policies with encryption to secure huge data storage space in the cloud. Unfortunately, the verifications between entities are not afraid. The method easily suffers from attacks, for example, collusion attack. At last, this attack can direct to disclosing sensitive data files.

Zou et al. [8] proposed a realistic and flexible key management system for trustworthy collaborative computing. It is designed to achieve efficient access control for dynamic groups. Regrettably, the secure approach for sharing the personal permanent portable secret between the member and the server is not supported and the secret key will be disclosed once the personal permanent manageable secret is obtained by the attackers.

Nabeel et al. [9] proposed a privacy preserve procedure based data sharing scheme in public clouds. But, this scheme is not secure for the reason that of the weak protection of commitment in the phase of identity token issuance.

3. PROPOSED METHOD

In order to achieve better security by providing fine grained access control and reducing key generation overhead, Identity Based Ring Signature proposed. Ring signature is group oriented signature with privacy concerns [10]. It is one of the digital signatures. This method provides the authenticity and anonymity of the end user. As opposed to conventional approaches Identity based ring signature doesn't allow certificate verification. Identity based ring signature combines the identity based cryptosystem and ring signature.

The ring signature scheme consists of three algorithms: KeyGen, Sign and Verify. Each user will run KeyGen individually in this algorithm, on input the security parameter 1^k, will output a key pair (p^k, s^k). The Sign algorithm, on input takes a secret key sk, a ring R contains list of public keys belonging to members of ring, a signature θ and a message m, the output is a signature σ on m. Finally, the Verify algorithm, on input takes the ring R, a signature σ, and a message m, then the output is 1 if some member of R created the signature σ on m and otherwise the output is 0.

Framework

An ID-based ring signature scheme consists of the following four algorithms: Setup, KeyGen, Sign, and Verify.

Setup: Taking a unary input string 1^k where k is a security parameter, it produces the master secret key s and the common public parameters params, which include a description of a finite signature space and a description of a finite message space.

KeyGen: It returns Signer's secret key SID by taking the input of the signer's identity ID ∈ $\{0,1\}^*$ and the master secret key s. (The corresponding public verification key QID can be computed easily by everyone.)

Sign: On input of a message m, a group of n users' identities S{IDi}, where $1 \le i \le n$, and the secret keys of one members SIDs, where $1 \le s \le n$; it outputs an ID-based ring signature σ on the message m.

Verify: It take input as ring signature σ, a message m and the group of signers' identities S{IDi}, it outputs 1 for "true" or 0 for "false", depending on whether σ is a valid signature signed by a certain member in the group S{IDi} on a message m. These algorithms must satisfy the standard consistency constraint of ID- based ring signature scheme, i.e. if σ = Sign(m,S{IDi},SIDs), and IDs ∈ S{IDi}, we must have Verify(σ,S{IDi},m) = 1 and otherwise output is 0.

A secure ID-based ring signature scheme should be enforceability and signer-ambiguous.

Figure 1: Architecture of cloud data Sharing Scheme

The system model consists of 3 different entities: 1.The cloud server, 2. A Group Admin (i.e., group manager) and 3.A set of group members.

Cloud Server: Cloud is the huge storage of resources. Cloud is responsible for storing all members of data and access to the file within a group to other group members based on publically offered revocation list which is maintained by Group Admin. We imagine that the cloud server is honest but curious. That is, the cloud server will not unkindly delete or alter user data, due to the security of data auditing schemes

Group Admin: The Group Admin is acted by the administrator of the company. Therefore we imagine that the Group Admin is fully trusted by the other parties. Group Admin perform various operations such as system parameters generation, user registration, group creation, assign ring signature, generation of private key using bilinear mapping and assign to the requested user, maintain revocation list and migrate this list into cloud for public use, and traceability.

Group Members: 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. Both Group Admin and group member can login using their login details. After successful login, Group Admin activates newly added users of the cloud by generating keys for each member using bilinear mapping and send it to the corresponding group members. He can also check the group details, and assign group signature. After successful login, Group Members signature is verified. After successful verification, the member can upload, download and can modify the files. Group member must be encrypting data file before uploading to the cloud. The Group Members account can be revoked after he leaves the cloud by the Group Admin.

User Registration: After successful creation of cloud setup, members want to get registered with the system through user registration process. While registering, members have to submit their personal details for completion of registration process. User registered with their information such as identity (user name, mobile no and email-id). During registration process, user got unique identity and access structure. This generates secret key for the members. For registered users they will obtain private key, that secret key is used for file encryption and decryption.

User Authentication: The user can login successfully only if user id and password are entered correctly. The login is a failure if the incorrect user id or wrong password is enters by the user. This helps in preventing unauthorized access.

Key Distribution: Means of distribute secret keys through the Group Admin that is valid only if the group members are not revoked from the group. Key can be updated by generating new key from an old key.

User Revocation: User revocation is the method of removal of user from system user list which is performed by group admin. Group admin can directly revoke multiple users through public revocation list at every time without affecting any non revoked user. If the login credentials of the specified user matches with the details of revocation list then access denied.

File Upload: File upload is the method of storing specified data files into the cloud. Uploaded files remains in the cloud up to the time specified while uploading the file. Before uploading the file, file has to be encrypted and compacted to ensure security and privacy of the files. Then it is encapsulated with corresponding decryption key and time to live (TTL) value for the file and send it to cloud.

File Download: To access the data that are store in the cloud, group member will give request as group id, data id. Cloud server will verify their signature, if the group member in the same group then allow to access file. Group member have rights to access data, but not having rights to delete or alter the data that are store in the cloud.

4. RESULTS

Security Analysis

Table 1: Security performance comparison

	RBAC	Mona	Proposed method
Secure key distribution		✓	✓
Access control	✓	✓	✓
Secure user revocation			✓
Anti-collusion attack			✓
Data confidentiality		✓	✓

As compared with RBCA and Mona the proposed scheme can achieve secure key distribution, fine-grained access control, protection from collusion attack, data confidentiality and secure user revocation.

Performance Analysis

With the aid of identity based ring signature, on the basis of the total time consumed to upload and download a file to/from the cloud. The total time is composed of the time from the time of submission of ask for to the cloud server to the point of time at which the file is uploaded/downloaded to/from the cloud.

Table 2: Comparison of Turnaround Time

File size (KB)	Existing Method		Proposed method	
	Upload	Down-load	Upload	Down-Load
150	12.5	11.6	12	7.8
500	35	40.5	33.8	32.3
1000	80.5	85.6	77.4	50.8
1500	95.1	122.2	82.1	51.9

Table 2 shows that turnaround time for upload and download the file. In general, the time to upload and download the data increased with the increase in the file size This table reveal that the proposed method outperforms the existing method appropriate to the absence of heavy computations and memory overhead.

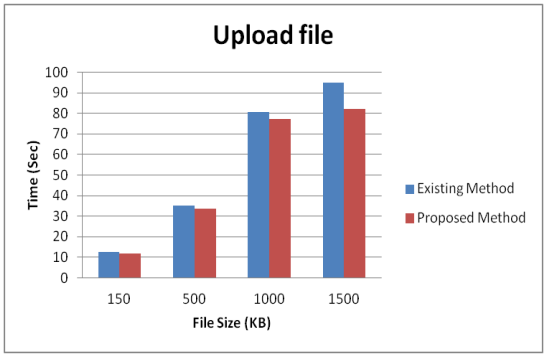

Figure 2: Performance of File Upload

In Figure 2 shows the result for upload time. X axis represents the file size Y axis represents the time. In existing system method 1.5mb was uploaded in 95.1s, where as in proposed system method it takes 82.1s to upload a 1.5mb file. This graph clearly shows that as compare to the existing system the performance of proposed system is higher.

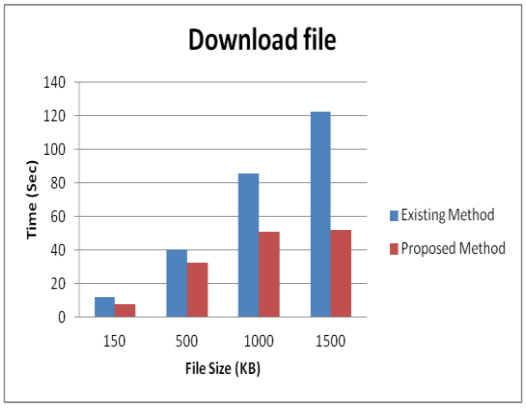

Figure 3: Performance of File Download.

In Figure 3 shows the result for download time. X axis represents the file size Y axis represents the time. In existing system method 1.5mb was downloaded in 122.2s, where as in proposed system method it takes 51.9s to upload a 1.5mb file. This graph clearly shows that as compare to the existing system the performance of proposed system is higher.

5. CONCLUSION

This paper introduces Identity Based Ring Signature, to provide the security for large amounts of data sharing in the cloud by using identity based ring signature. Ring signature is group oriented signature with privacy concerns. It is a type of digital signature. This method provides the authenticity and anonymity of the end user. Identity based ring signature reduces the process of official document verification, which is a bottleneck

problem in conventional public key infrastructure. Proposed system supports multiple users to distribute common data across the members and each member can involve in data dynamics.

6. REFERENCES

1. Zhu, Z., & Jiang, R. (2016). "A secure anti-collusion data sharing scheme for dynamic groups in the cloud". *IEEE Transactions on parallel and distributed systems*.
2. S. Vasundra (2016) "Efficient & Secure Privacy Preserving Public Auditing Scheme for Cloud Storage", ISSN- 2278-1323, Vol 5, Issue 9.
3. Camenisch, J., & Michels, M. (1998, October). A group signature scheme with improved efficiency. In *Asiacrypt* (Vol. 98, pp. 160-174).
4. Chow, S. S., Yiu, S. M., & Hui, L. C. (2005, June). Efficient identity based ring signature. In *International Conference on Applied Cryptography and Network Security* (pp. 499-512). Springer, Berlin, Heidelberg.
5. Zhu, Z., Jiang, Z., & Jiang, R. (2013, December). The attack on mona: Secure multi-owner data sharing for dynamic groups in the cloud. In *Information Science and Cloud Computing Companion (ISCC-C), 2013 International Conference on* (pp. 213-218). IEEE.
6. Liu, X., Zhang, Y., Wang, B., & Yan, J. (2013). Mona: Secure multi-owner data sharing for dynamic groups in the cloud. *ieee transactions on parallel and distributed systems*, *24*(6).
7. Zhou, L., Varadharajan, V., & Hitchens, M. (2013). Achieving secure role-based access control on encrypted data in cloud storage. *IEEE transactions on information forensics and security*, *8*(12).
8. Zou, X., Dai, Y. S., & Bertino, E. (2008, April). A practical and flexible key management mechanism for trusted collaborative computing. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE* (pp. 538-546). IEEE.
9. Nabeel, M., Shang, N., & Bertino, E. (2013). Privacy preserving policy-based content sharing in public clouds. *IEEE Transactions on Knowledge and Data Engineering*, *25*(11), 2602-2614.
10. Herranz, J., & Sáez, G. New identity-based ring signature schemes. In *ICICS* (Vol. 4, pp. 27-39).