RESEARCH ARTICLE OPEN ACCESS

Protected Data Distribution for Multiple Owners in Dynamic Groups of Public Clouds

P.J.Thangamani[1], G.Nagalakshmi[2]
M.Tech Research Scholar[1], HOD[2]
Department of Computer Science and Engineering
SISTK, Puttur
JNTU Anantapur
A.P-India

ABSTRACT
Protected data Distribution in mulitiple owner manner for dynamic groups preserves data, identity privacy from an untrusted cloud and allows frequent change of membership. In RLS while the number of invoked users grows larger, the length of RL increases. To send all user invocation details to the group members for sharing purpose, leads to communication overhead. To address this issue, in thispaper, By leveraging group signature and dynamic broadcast encryption techniques and for overall security Elliptic curve cryptography (ECC) algorithm is used, so that any cloud user can anonymously distribute data with others. The storage overhead and encryption computation cost of the schemeare independent with the number of revoked users.

Keywords:- Cloud Computing, Data distribution, Mutiple Owners, Dynamic groups, privacy-preserving, group signature, Dynamic broadcast encryption, public clouds.

I. INTRODUCTION

When you store your photos online on your personal computer and in a social networking site, it's a "cloud computing" service. In an organization, you want to use an online invoicing service instead of updating the in house one you have been using for many years, that online service is a cloud computing service. Cloud computing is mainly used for resource sharing and with very low maintenance cost.

The cloud service providers (CSPs), such as Amazon, are able to provide a various services to cloud users with the not fully trusted the cloud servers operated by cloud provider while sensitive data stored in the cloud. Cloud storage, designed a virtual private storage services are based on cryptographic techniques. Service should provide confidentiality and integrity.

The main benefits of a public storage services are availability, reliability, efficient retrieval, and data sharing. When preparing data to store in the cloud, the data processor begins by indexing it and encrypting it with a symmetric encryption scheme (e.g., AES) under a unique key refer to single writer/single reader (SWSR). It then encrypts the index using a searchable encryption scheme and encrypts the unique key with an attribute-based encryption scheme under an appropriate policy. Finally, it encodes the encrypted data and index in such a way that the data verifier can later verify their integrity using a proof of storage.

Asymmetric searchable encryption (ASE) schemes where the party searching over the data is different from the party that generates and refer to many writer/single reader (MWSR).It is very inefficient. Attribute-based encryption scheme each user in the system is provided with a decryption key that has a set of attributes associated with it.

A user can then encrypt a message under a public key and a policy. Decryption will only work if the attributes associated with the decryption key match the policy used to encrypt the message.

The described access policies based on data attributes and allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents. The issue is mainly caused by the operation of user revocation, which inevitably requires the data owner to re-encrypt all the data files accessible to the leaving user, or even needs the data owner to stay online to update secret keys for users. Achieve this goal, by uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Data confidentiality is also achieved since cloud servers are not able to learn the plaintext of any data file in our construction. For further reducing the computation
overhead on cloud Servers and thus saving the data owner's investment, take advantage of the lazy re-

encryption technique and allow Cloud Servers to "aggregate" computation tasks of multiple system operations.
The described an efficient system that was expressive; it allowed to encrypt or to express an access predicate in terms of any monotonic formula over attributes. The techniques provide a framework for directly realizing provably secure CP-ABE systems. In this, the ciphertext distributes shares of a secret encryption exponent across different attributes according to the access control LSSS matrix M. A user's private key is associated with a set S of attributes and he will be able to decrypt a ciphertext if his attributes "satisfy" the access matrix associated with the ciphertext.

II. RELATED WORKS

In [4], Kallahalla et al. proposed cryptographic storage systems that enable secure file distribution on untrusted servers, named Plutus. By dividing files into filegroups and encrypting each filegroup with a unique file-block key, the data owner can distribute the filegroups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings regarding a heavy key distribution overhead for large-scale file distribution. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

In [5], files stored on the untrusted server include two parts: file metadata and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the public key of authoritative users. Thus, the size of the file metadata is relative to the number of authorized users. The user revocation in the scheme is an intractable issue especially for large-scale distribution, since the file metadata needs to be updated. In their extension version, the NNL construction [10] is used for efficient key revocation. However, when a new user joins the group, the private key of each user in an NNL system wants to be recomputed, which may limit the application for dynamic groups. Another concern is that the computation overhead of encryption linearly increases with the distribution scale.

Ateniese et al. [6] leveraged proxy reencryptions to secure distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to straightforwardly reencrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launch, which enables them to study the decryption keys of all the encrypted blocks.

In [3], Yu et al. presented a scalable and fine-grained data access control system in cloud computing based on the KPABE technique. The data owner uses a random key to encrypt a file, where the random key is additional 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 formation. To achieve user revocation, the manager delegates' tasks of data file reencryption and user secret key update to cloud servers. However, the single owner manner may hold back the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

Lu et al. [7] proposed a secure origin scheme, which is built upon group signatures and ciphertext-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is capable of encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs encrypted data with her group signature key for privacy preserving and traceability. However, user revocation is not supported in their scheme. From the above study, we can watch that how to securely share data files in a multiple-owner manner for dynamic groups while preserving identity privacy from an untrusted cloud remains to be a challenging issue. In this paper, we propose a novel Mona protocol for secure data sharing in cloud computing. Compared with the existing works, Mona offers unique features as follows:

1. Any user in the group can store up and share data fileswith others by the cloud.
2. The encryption complexity and size of ciphertextsare autonomous with the number of revoked users in the system.
3. User revocation can be achieves without updating the private keys of the left over users.
4. A new user can openly decrypt the files stored inthe cloud before his participation.

III. PRELIMINARIES

3.1 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 selected group manager can reveal the identity of the signature's originator when a disagreement 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.

3.2 Dynamic Broadcast Encryption

Broadcast encryption [16] enables a broadcaster to convey encrypted data to a set of users in order that only a privileged subset of users can decrypt the data. Besides the above characteristics, dynamic broadcast encryption also allow the group manager to dynamically include new members while preserving before computed information, i.e., user decryption keys need not be recomputed, the morphology and size of ciphertexts are unaffected and the group encryption key require no change. 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 foundation for file sharing in dynamic groups.

3.3 Elliptic Curves Cryptography

The idea of using Elliptic curves in cryptography was introduced by Victor Miller and Neal Koblitz as an option to established public-key systems such as DSA and RSA. The Elliptical curve Discrete Log Problem (ECDLP) makes it difficult to crack an ECC as compared to RSA and DSA where the problems of factorization or the discrete log problem can be solved in sub-exponential time. This means that significantly smaller parameters can be used in ECC than in other competitive systems such as RSA and DSA. This help in having smaller key size hence earlier computations.

IV. SYSTEM MODEL AND DESIGN GOALS

4.1 System Model

We regard as a cloud computing architecture by combining with an example that a company uses a cloud to facilitate 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.

Cloud is operated by CSPs and provides priced plentiful storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be exterior of the cloud users' trusted domain. Similar to [3], [7], we imagine that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the security of data auditing schemes [17], [18], but will try to learn the content of the stored data and the identity of cloud users.

Group manager takes charge of system parameters generation, user registration, user revocation, and enlightening the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. So, we assume that the group manager is completely trusted by the other parties.

Group members are a set of registered users that will store up their personal data into the cloud server and distribute 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 contribution in the company.

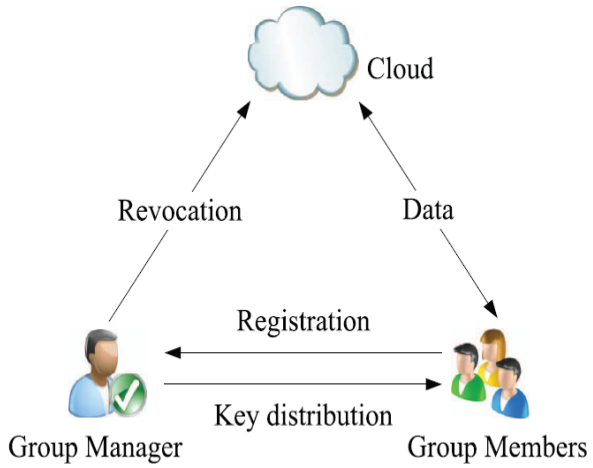

Fig. 1. System model.

4.2 Design Goals

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

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

Data confidentiality: Data confidentiality requires that unauthorized users jointly with the cloud are unable of learning the content of the stored data. An important and challenging issue for data confidentiality is to preserve its availability for dynamic groups. Specially, new users should decrypt the data stored in the cloud previous to their contribution, and revoked users are unable to decrypt the data moved into the cloud later than the revocation.

Anonymity and traceability: Anonymity guarantees that group members can access the cloud without enlightening the real identity. Although anonymity represents an effective safety 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 advantage. Thus, to tackle the inside attack, the group manager should have the capability 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 not including involving the remaining users. That is, the left over 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

In this proposed system secure data sharing in a multi-owner manner for dynamic groups preserves data, identity privacy from an untrusted cloud and allows frequent change of the membership. In RLS while the number of invoked users grows larger, the length of RL increases. To send all user revocation details to the group members for sharing purpose, leads to communication overhead .To address this issue, in this paper, By leveraging group signature and dynamic broadcast encryption techniques and for overall security Elliptic curve cryptography(ECC) algorithm is used, so that any cloud user can anonymously share data with others. The storage overhead and encryption computation cost of the scheme are independent with the number of revoked users.

MODULES:

1. User Registration
2. User Revocation
3. File Generation
4. File Access
5. File Deletion
6. Traceability
7. Delta RLS

MODULES DISCRIPTION:

User Registration:

User registered with their details such as identity (user name, password and email-id). Group manager select random number, base point , parameters and performs modulo with prime number, by using ECC (Elliptic Curve Cryptography) generate an private key. For registered users they will obtain private key, that private key is used for group signature and file decryption. The Group manager adds the user identity (ID) to the group user list that will be used in traceability phase.

User Revocation:

User Revocation is performed by the group manager. Delta Revocation List is publicly available based on those, group members are allowed to encrypt the data and make that data confident against revoked users. Revoked users are maintained in the revoke user list and make publicly available in the cloud. Delta RL is bounded by signature to declare its validity. Upon receiving the resignation request from the group member, group member will be in revoked user list.

File Generation:

Group members will store their data in real cloud. Aspose real cloud (SaaS) is provided by CSP mainly for storage. The group members will request with group id and based on the Delta RL allow the data owner to upload the data in the cloud, if their signature is true. If it's a revoked user, cloud server will not allow generating the data and signature verification status false. When generating the data, hash id will be generated that will be used for deleting the data.

Data owner	File name	Hash id	Hash code	date
Name	name	F(∂)	C1,c2,c	t_{data}

File Access:

To access the data that are stored 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 modify the data that are stored in the cloud. If any request from revoked user, cloud server won't allow accessing the data.

File Deletion:

File that are stored in the cloud can be deleted by either group member (i.e., the member who uploaded the file into the server) or by group manager. It allows data owners to delete their own files that are stored in the cloud. If any delete request from the group member, cloud server will verify the signature and delete the data file that are stored in the cloud.

Traceability:

Group manager will reveal their real identity in case of any dispute occurs. If any malpractice happened inside the organization it can be easily traceable. If any group members are modify or delete the data file of other groups, it can easily identify which member doing such activities.

Delta RLS:

In existing RLS, revoked user details such as private key are updated manually for every day. Revoked users can access the cloud, hacking is possible. But in Delta RLS set a ttp value (threshold value), when it reaches the threshold value revoked users are updated automatically. Revoked users can't able to access the cloud hacking attack is reduced and communication overhead is also reduced.

VI. CONCLUSION

In this paper, securely share the data file among the dynamic groups. Without revealing their identity members in the same group can share the data efficiently. Elliptic curve cryptography is used for over all security. When compared to other algorithm key size is very small, it is not able to hack easily. Delta RL is used for efficient revocation without updating private keys of remaining users.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwins ki, 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.

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

[3] 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.

[4] 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.

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

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "ImprovedProxy Re-Encryption Schemes with Applications to SecureDistributed Storage," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.

[7] [7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in CloudComputing," Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.

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

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

[10]] 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), pp. 41-62, 2001.

[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[13] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based

[14] Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[15] [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, pp. 39-59, 2007.

[16] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.
[17] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.
[18] 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.
[19] [18] 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.
[20] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, pp. 46- 50, 2008.
[21] 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.
[22] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.
[23] The GNU Multiple Precision Arithmetic Library (GMP), http:// gmplib.org/, 2013.
[24] [23] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL), http://certivox.com/, 2013.
[25] [24] The Pairing-Based Cryptography Library (PBC), http://crypto.
[26] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 41-55, 2004.
[27] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.
[28] 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.
[29] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.
[30] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp.480-491, 1993.
[31] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu "Plutus: Scalable Secure File Sharing on Untrusted Storage," Pro USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[32] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.
[33] S.Kulkarni and Bezawada Bruhadeshwar, "Rekeying and Storage Cost for Multiple User Revocation," Department of Computer Science and Engineering, Michigan State University, East Lansing, MI48824USA.
[34] 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
[35] Information, Computer and Comm. Security, pp. 282-292, 2010.
[36] 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), pp. 41-62, 2001.
[37] 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 KeyCryptography, [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