IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 4, April 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Protected Anti-Collusion Dynamic Data Sharing System for Active Groups in the Cloud Computing

S.David Arokkiya Doss M.Phil Scholar, Tamil University, Thanjavur, Tamil Nadu, India.

A.Senthil Kumar, Assistant Professor, Tamil University, Thanjavur, Tamil Nadu, India.

Abstract

Improved from cloud computing, users can accomplish an efficient and economical approach for data sharing surrounded by group members in the cloud with the characters of low safeguarding and little association cost. In the meantime, we must supply security reassurance for the sharing data files since they are outsourced. Regrettably, as of the general change of the attachment, sharing data while given that privacy-preserving is silent a demanding subject, particularly for an untrusted cloud due to the collusion attack. Additionally, for existing system, the protection of key allotment is based on the protected announcement channel, on the other hand, to have such channel is a sturdy statement and is complicated to achieve. In this paper, we fine competence, which means earlier users need not to update their private keys for the circumstances either a new user joins in the group or a user is withdraw from the group.

Introduction

Manner may delay the achievement of applications, where any member in the group can use the cloud service to store and divide data files with others. Conversely, the file-block keys need to be updated and distributed for a user revocation, so, the system had a heavy key distribution overhead. Additional system for data sharing on untrusted servers has been proposed in [1]. Still, the difficulty of user participation and revocation in these systems is linearly rising with the number of data owners recommend a protected data sharing proposal for energetic members. Firstly, we put forward a protected way for key allocation without any protected communiqué channels, and the users can firmly obtain their private keys from group manager. Secondly, this system can achieve fine-grained access control, any user in the collection can use the reserve in the cloud and revoked users are not able right to use the cloud another time after they are revoked. Thirdly, we be capable of look after the system from collusion attack, which resources that revoked users cannot acquire the innovative data file even if they come together with the untrusted cloud. In this advance, by leveraging polynomial utility, we can realize a protected user revocation format. Finally, the system can accomplish

and the revoked users. Nabeel et al. planned a privacy preserving policy-based content sharing system in public clouds. Yet, this system is not protected as the weak protection of assurance in the phase of identity token issue. It is maintained that the system can attain well-organized user revocation that merge role-based access control policies with encryption to protected large data storage in the cloud. Regrettably, the verifications between entities are not disturbed, the system easily suffer from attacks, for example, collusion attack. To conclude, this attack can lead to revealing sensitive data files.

Liu et al [2] proposed a secure multi-owner data sharing system, named Mona. It is claimed that the system can achieve fine-grained access

control and revoked users will not be able to access the sharing data again once they are revoked. Conversely, the system will easily suffer from the collusion attack by the revoked user and the cloud. The revoked user can use his private key to decrypt the encrypted data file and get the secret data after his revocation by combining with the cloud. In the stage of file access, first of all, the revoked user throws his request to the cloud, then the cloud act in response the corresponding encrypted data file and revocation list to the revoked user without verifications. Next, the revoked user can calculate the decryption key with the help of the attack algorithm. Lastly, this attack can guide to the revoked users receiving the sharing data and releasing other secrets of legal members.

Lu et al anticipated a protected derivation system by leveraging group signatures and cipher text-policy attribute-based encryption techniques. Each user acquire two keys after the registration while the attribute key is used to decrypt the data which is encrypted by the attribute-based encryption and the group signature key is used for privacy-preserving and traceability. On the other hand, the revocation is not supported in this system.

Zouetal. [3] Presented a sensible and flexible key management method for trusted joint computing. By leveraging access control polynomial, it is designed to achieve well-organized access control for dynamic groups. Regrettably, the protected way for sharing the private permanent portable secret between the user and the server is not sustain and the private key will be revealed once the personal everlasting portable secret is obtained by the invader/attackers.

Related Work

In this paper, we recommend a protected data sharing system, which can achieve protected key distribution and data sharing for dynamic group. The main contributions of our system include:

1. Our system is able to carry dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and altered.

2. We suggest a protected data sharing system which can be confined from collusion attack. The revoked users can not be capable to get the original data files once they are revoked even if they combine with the untrusted cloud. Our system can accomplish protected user revocation with the help of polynomial function.

3. We offer security examination to prove the security of our system. In addition, we also perform imitations to exhibit the competence of our system.

4. We provide a protected way for key distribution without any protected communication channels. The users can firmly obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.

5. Our system can accomplish fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

3. THREAT MODEL, SYSTEM MODEL AND DESIGN GOALS

3.1 Threat Model:

In this paper, we propose our plan taking into account the Dolev-Yao model [4], in which the attacker can catch, capture and combination any message at the correspondence channels.

With the Dolev-Yao model, the best way to protect the data from attack.

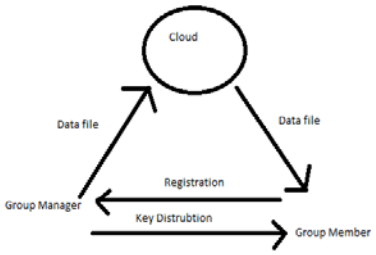

Figure 1: System model

Here the proposed model is illustrated in figure 1, the system model consists of three different entities: the cloud, a group manager and a large number of group members.

The cloud, sustaining by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner. On the other hand, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the content of the stored data. Group manager will obtain charge of system parameters generation, user registration, also, client

3.2. MODULES

- Cloud Module
- Group Manager Module
- Group Member Module
- File Security Module
- Group Signature Module
- User Revocation Module.

Cloud Module: In this element, we generate a local Cloud and present priced plentiful storage services. The users can upload their data in the cloud. We expand this module, somewhere the cloud storage container be made protected. However, the obscure is not fully conviction by users since the CSPs are very expected to be outside of the darken users' trusted domain. Similar to we believe that the darken server is honest but curious. That is, the cloud server will not unkindly delete or change user data due to the fortification of data auditing system, but will try to study the content of the stored data and the identities of cloud users.

Group Manager Module:

Group manager receive incriminate of followings:

1. Classification parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of an argument data owner.

Therefore, we suppose that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of every and every process in the cloud. The group manager is accountable for user registration and also user revocation too.

Group Member Module:

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.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can vision the files which are uploaded in their assembly and also modify it.

File Security Module:

- Encrypting the data file.
- 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).

Group Signature Module:

A group signature system agrees to any component of the group to sign communication while keeping the individuality secret from verifiers. Besides, the selected group manager can expose the identity of the signature's designer when an argument occurs, which is symbolize as traceability.

User Revocation Module:

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.

3.3 Bilinear Maps

Let G1 and G2 be additive cyclic groups of the same prime Order q [13].

Let e : G1 X G1 -> G2 denote a bilinear map
Constructed with the following properties:

1) Bilinear: For all a,b Σ Z*q and P,Q Σ G1, $e(aP,bQ) = e(P,Q)^{ab}$.

2) Nondegenerate: There exists a point Q such that $e(Q,Q) \neq 1$.

3) Computable: There is an efficient algorithm to compute
e (P,Q) for any P,Q Σ G1.

3.4 Complexity Assumptions

Definition 1 (Basic Diffie-Hellman Problem (BDHP))

Assumption [5]). Given base point P and a value γ Σ Z q, it is easy to compute γ. P. However, given P, γ. P it is infeasible to compute γ because of the discrete logarithm problem.

Definition 2 (Decisional Diffie-Hellman Problem (DDHP))

Assumption[6]). Similar to definition 1, given base point P and aP, (a+b) P; it is infeasible to compute bP.

Definition 3 (Weak Bilinear Diffie-Hellman Exponent (WBDHE))

Assumption [7]). For unknown a Σ Z*q ; given $Y, aY, a^2Y, \ldots, a^lY$, $P\Sigma G_1$, it is infeasible to compute $e(Y, P)^{1/a}$.

3.5 Notations

Each user has a pair of keys (pk, sk), which is used in the asymmetric encryption algorithm, and pk needs to be negotiated with the group manager on the condition that no Certificate Authorities and security channels are involved in. KEY is the private explanation of the user and is used for data sharing in the system. UL is the group user list which records part of the private keys of the legal group users. DL is the data list which records the identity of the sharing data and the time that they are updated.

3.6 System Description

The scheme of our system includes system initialization, user registration for existing user, file upload, user revocation, registration for new user and file download.

3.6.1 System Initialization

The group manager takes charge of this operation. He produce a bilinear map collection system S = (q, G1, G2, e (.)), then select two random elements P, G Σ G1 and a number γ Σ Zq , then computes W = γ. P, Y = γ. G and Z = e (G,P) At last, the collection manager distribute the parameters (S,P,W,Y,Z,f, f1,Enc()), where f is hash purpose {0,1}*-> Z*q, f1 is hash function { 0, 1}*-> G1, and Enc() is a symmetric encryption algorithm. Besides, the group manager will stay the parameters (γ, G) as the secret master key.

3.6.2 Notations Notation Description

IDEi the identity of user i

IDdatai the identity of data i

qk the public key of the user

tk the corresponding private that needs to be negociated with the group manager

KEY= (xi,Ai,B) the private key which is distributed to the user from the group manger and used for dynamic data sharing

4. SECURITY ANALYSIS

Here, we show the security of our system in terms of key distribution, access control and data confidentiality.

4.1 Key Distribution

Theorem 1

In this system, the communication entities can securely consult the public key qk and allocate the Private Key KEY= {xi, Ai, Bi } to users without any Certificate Authorities and protected communication channels.

Proof: In user registration, the user sends his public key qk and a random number v1€Zq to the group manager with his identity IDEi .Then the group manager computes corresponding value V, S.

Furthermore, the user can confirm the identity of the group manager by the equation:

S .e .v. f. (qk || ac || IDE). Q, X) = e (V, Q).

The *qk becomes* the negotiated public key after successful verification equation. Then the group manager can firmly allocate the private key *KEY* , which is used for dynamic data sharing, to users with the help of public key and without any Certificate Authorities and protected communication channels. Base point *Q* and *aQ,(a+b)Q*, it is infeasible to compute b *Q*.

Definition 3
(Weak Bilinear Diffie-Hellman Exponent):

For unknown *e(X, P) a*

Encpk() symmetric encryption algorithm used the encryption key k

ASENC () asymmetric encryption algorithm used the encryption key

ULI group user list

DLI data list

Conclusion

In this paper, we design a protected anti-collusion dynamic data sharing system for active groups in the cloud computing. In our system, the users can strongly obtain their private keys from group manager Certificate Authorities and safe communication channels. Also, our system is able to support active

groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, our system can achieve protected user revocation the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. 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] E. Goh, H. Shacham, N. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[3] 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, pp. 282-292, 2010.

[4] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. http://eprint.iacr.org/2008/290.pdf, 2008

[5] B. Den Boer, "Diffie–Hellman is as strong as discrete log for certain primes," in Proc. Adv. Cryptol., 1988, p. 530.

[6] D. Boneh, X. Boyen, and H. Shacham, "Short group signature," In Proc. Int. Cryptology Conf. Adv. Cryptology, 2004, pp. 41–55.

[7] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based Encryption with constant size ciphertext," in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 440–456.