International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 03 | Mar -2020 ISSN: 2582-3930

ON THE SECURITY OF DATA ACCESS CONTROL FOR MULTI AUTHORITY CLOUD STORAGE

[1]K.Kalai Selvan[2] M.Mohamed Rafi[3]N.Bala Subramanian

[1]Research Scholar[2]Associate Professor [3]Associate Professor

(Dept Of MCA, Mohamed Sathak Engg College,kilakarai)

Abstract:

Data access control has becoming a challenging issue in cloud storage systems. Some techniques have been proposed to achieve the secure data access control in a semi trusted cloud storage system. Recently, K. Yang et al. proposed a basic data access control scheme for multiauthority cloud storage system (DAC-MACS) and an extensive data access control scheme (EDAC-MACS). They claimed that the DAC-MACS could achieve efficient decryption and immediate revocation and the EDAC-MACS could also achieve these goals even though nonrevoked users reveal their Key Update Keys to the revoked user. However, through our cryptanalysis, the revocation security of both schemes cannot be guaranteed. In this paper, we first give two attacks on the two schemes. By the first attack, the revoked user can eavesdrop to obtain other users' Key Update Keys to update its Secret Key, and then it can obtain proper Token to decrypt any secret information as a nonrevoked user. In addition, by the second attack, the revoked user can intercept Ciphertext Update Key to retrieve its ability to decrypt any secret information as a nonrevoked user. Secondly, we propose a new extensive DAC-MACS scheme (NEDAC-MACS) to withstand the above two attacks so as to guarantee more secure characteristic revocation. Then, formal cryptanalysis of NEDAC-MACS is presented to prove the security goals of the scheme. Finally, the performance comparison among NEDAC-MACS and related schemes is given to demonstrate that the performance of NEDAC-MACS is superior to that of DACC, and relatively same as that of DAC-MACS.

Introduction:

Cloud storage is an imperative service of cloud computing, which offers services for data owners to host their data in the cloud. This new standard of data hosting and data access services introduces a great experiment to data access control. Because the cloud server cannot be fully trusted by data owners, this has been solved by using the characteristic based encryption in the previous methods [1]. In the previous method, the data owner defines the access policies and encrypts data according to the policies. Each user will be issued a secret key reflecting its characteristic. A user can decrypt the data only when its characteristic satisfy the access policies.There are two types of CP-ABE systems: single-authority CP-ABE [2], [3], [4], [5] where all characteristic are managed by a single authority, and multi-authority CP-ABE [6], [7], [8] where characteristic are from different domains and managed by different authorities. Multi-authority CP-ABE is more appropriate for data access control of cloud storage systems, as users may hold characteristic issued by multiple authorities and data owners may also share the data using access policy defined over characteristic from different authorities.

In multi-authority cloud storage systems, users' characteristic can be changed dynamically. A user may be entitled some new characteristic or revoked some current characteristic. And his permission of data access should be changed accordingly. In the existing system the characteristic changes dynamically but still the user can able to access the data even after revocation.

In this paper, I first propose a revocable Multiauthority system in which the data can be shared by the user by characteristic based encryption, Second we encrypt the characteristic and send the encrypted private key to the user.

PROBLEM IDENTIFICATION

In the existing system the user need to share the data to the another user using Collaborative Policy characteristic based encryption (CP- ABE), in this approach the data access can be revoked by the data owner, while revoking process the characteristic in the system will dynamically change, the problem will occur here. If the characteristic in the System is not changed then the user can still able to access the data from the cloud storage. In the previous approach they have mentioned that, each user is dishonest and may collude to obtain unauthorized access to data.

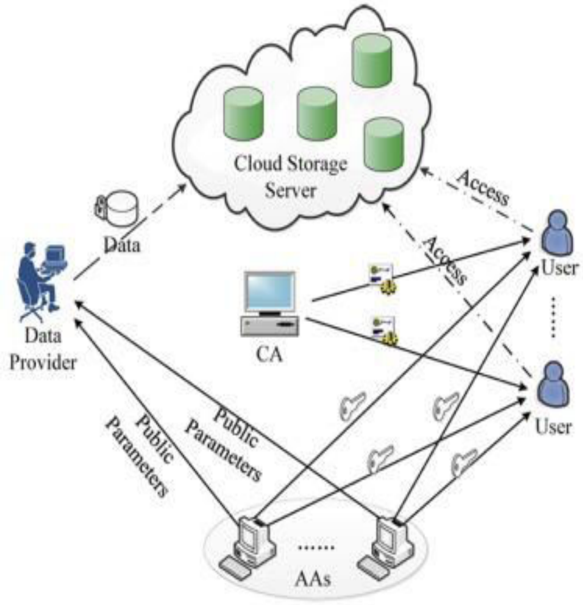
RELATED WORK

Data Access Control: A plurality of data access control systems (e.g. [2], [3], [7]-[19]) based on the promising CPABE technique are proposed to construct the efficient, secure, fine grained and revocable access schemes. S.Ruj et al. (2011) proposed a distributed access control scheme in clouds (DACC) [9] that supported attribute revocation. In DACC, one or more key distribution centers (KDCs) distributed keys to data owners and users. Technically, it requires not only forward security but more indispensable backward security in context of the attribute revocation. However, DACC supported attribute revocation with vulnerable forward security [2]. J.Hur et al. (2011) proposed an attribute-based DAC scheme [12] with efficient revocation in cloud storage systems, whereas it was designed only for the cloud systems with single trusted authority. In addition, the above two schemes both require data owners to encrypt the outsourced cipher text after revocation. Liu et al. (2013) presented a secure multi-owner data sharing scheme called Mona [20]. It is claimed that the scheme can achieve fine-grained access control and secure revocation. However, the scheme will easily suffer from collusion attack by the revoked user and the cloud [21]. Recently, K.Yang et al. proposed a data access control scheme for multi authority cloud storage system (DACMACS) [2] and [3] which both supported more efficient decryption and secure attribute revocation without encryption by the data owners. In reference [2], due to a strong security assumption in DAC-MACS that the non revoked users will not reveal their key update keys to the revoked user, the authors further removed the assumption and proposed the extensive data access control scheme (EDAC-MACS). In context of secure attribute revocation, DAC-MACS and EDAC-MACS could both achieve forward revocation security irrespective of active attacks. However, the backward revocation security both in DAC-MACS and EDAC-MACS still cannot be guaranteed when the revoked user eavesdrops to obtain more than two users' Key Update Keys to update its Secret Key, or when the revoked user intercepts the Cipher text Update Key. In both scenarios, the revoked user can retrieve its ability to decrypt any secret information as a non revoked user just as before.

IMPLIMENTATION

In this paper, two attacks are first given on the DAC- MACS's and EDAC-MACS's revocation security which cannot be guaranteed through our cryptanalysis. Subsequently, a new extensive DAC-MACS scheme (NEDACMACS) is proposed to withstand above two attacks so as to support more secure characteristic revocation. The main contributions of this paper are summarized as follows: 1. In this paper, two attacks are firstly constructed on the vulnerabilities of revocation security in DACMACS and EDAC-MACS. By the first attack, the revoked user can eavesdrop to obtain other users' Key Update Keys to update its Secret Keys, and then it can obtain proper Token to decrypt any secret information as a nonrevoked user as before. In addition, by the second attack, the revoked user can intercept the Ciphertext Update Key to retrieve its ability to decrypt any secret information as a nonrevoked user as before. 2. Secondly, we propose a new extensive DACMACS scheme, denoted as the NEDAC-MACS, to withstand above two attacks and support more secure characteristic revocation. We modify some DACMACS's algorithms, and perform the vital ciphertext update communication between cloud server and AAs with some more secure algorithms. Our NEDAC-MACS scheme mainly includes two improvements on the DAC-MACS at Secret Key Generation phase and Characteristic Revocation phase, and it can run correctly according to the correctness proof of NEDAC-MACS. 3. Then, formal cryptanalysis of the NEDAC-MACS is described to prove that the proposed NEDACMACS can guarantee collusion resistance, secure characteristic revocation, data confidentiality, and provable security against static corruption of authorities based on the random oracle model. 4. Finally, performance analysis of our NEDACMACS are conducted by making an efficiency comparison among related CP-ABE schemes to testify that the NEDAC-MACS is securityenhanced without reducing more efficiency. The major overhead of decryption is also securely outsourced to the cloud servers, and the overall overheads of storage, communication and computation of the NEDAC-MACS are superior to that of DACC and relatively same as that of DAC-MACS

System architecture



System Model of DAC-MACS

A cloud storage system with multiple characteristic authorities (DAC-MACS) has five types of entities involved: global certificate authority (CA), users, cloud servers, data owners, and characteristic authority (AA). Table Ⅱ presents the roles and behaviors of all involved parties in DAC-MACS. In DAC-MACS, the global certificate authority (CA) accepts both users' and characteristic authorities' registrations to initialize the system by two steps CA setup and AA setup, and hence assign a global unique identity to each valid user and a global unique *aid* to each AA.After registration, each AAk∈SA runs Secret Key generation algorithm to compute valid user's secret keys {SK} according to the user's role or hierarchy in a defined access policy to some sensitive data. Then, for each data m, data owners first define an access structure [24], [25] $\mathbb{A}$ = (M,), encrypt the data under this access structure and then outsource the encrypted data CT to the proxy cloud server. Thereafter, the user Uj∈SU can upload $\mathbb{A}$-related secret keys {SK} and its global public key GPK to cloud for a decryption token TK computed by cloud servers, then the user can decrypt the data m with the TK and its global secret key. The CA, AAs, and cloud servers cannot decrypt the data m without user's global secret key. For characteristic revocation, the corresponding AA, which supervises the revoked characteristic, first assigns a version key to each characteristic and then generates Ciphertext Update Key for cloud to update CT and Key Update Key for users to update SK. Only those CTs, SKs related to the revoked characteristic need to be updated to implicitly contain the latest version key of the revoked characteristic. After characteristic revocation, all algorithms in system stay unaltered.

EDAC-MACS Description

A first have DAC-MACS a strong security assumption that all the nonrevoked users will not send their received Key Update Keys to the revoked user, since they found the revoked user can technically update its secret key to the latest vision via using other user's Key Update Key. Then they removed this assumption and propose the extensive data access control scheme (EDAC-MACS). Compared to DAC-MACS, three algorithms' outputs are modified: SKeyGen, TKGen and UKeyGen. With these fraction modifications, they claimed that the revoked user has no chance to update its Secret K

Attack Model

t

update its Secret Key, or when it intercepts the Ciphertext Update Key. Therefore, we modify the vulnerable algorithms on the EDAC-MACS schemes at Secret Key Generation phase and Attribute Revocation phase, so that

In this paper, we make the cryptanalysis and propose our new extensive scheme based on the Dolev-Yao model [30], in which the adversary can overhear, intercept, insert arbitrary information into, synthesis, and replay any message delivered in the communication channels. Under the Delov-Yao model, the only way to protect the transmitted information from passive or active attacks by eavesdroppers or malicious adversaries is to design the effective security protocols. This means there is no "secure communication channels" assumption between all the involved communication entities. Therefore, it is reasonable that Delov-Yao model can be more appropriate and practical to describe the attackers and demonstrate the communication protocols in reality

The attacks I

Includes two phases: attack preparation and attack implementation. At the preparation phase, the revoked user (attacker) eavesdrops to obtain any two nonrevoked users' Key Update Keys at Attribute Revocation phase of EDAC-MACS. Then at the implementation phase, the revoked user can update its own Secret Key SK and then successfully decrypt corresponding CT′ as a nonrevoked user

Attack Ⅱ

The attack 2 also includes two phases: attack Preparation and attack Implementation. At the preparation phase, the revoked user (attacker Uμ) intercepts the previous CUK$\tilde{x}k$ at the Attribute Revocation phase in DAC-MACS or EDACMACS. /Then at the implementation phase, the revoked user can use the previous CUK$\tilde{x}k$ to decrypt any secret information as a nonrevoked user. Furthermore the revoked user Uμcan properly complete all related operations on its own since it can learn the algorithms CTUpdate, TKGen and all the corresponding inputs

NEW EXTENSIVE DAC-MACS SCHEME

NEDAC-MACS

The open and non-secure communication channel in context of attribute revocation, the revoked user, as a Dolev-Yao attacker, can still breach the backward revocation security both in DAC-MACS and EDAC-MACS when it eavesdrops to obtain more than two users' Key Update Keys

the vital ciphertext update communications between cloud servers and AAs are performed with security-enhanced algorithms in our NEDAC-MACS scheme, which can ensure the real security goals on the open and non-secure communication channels.

PERFORMANCE ANALYSIS

To validate the efficiency of our NEDAC-MACS, performance comparisons are carried out in terms of storage overhead, computation overhead and communication overhead among CP-ABE schemes of DACC [9], DACMACS [2] and our NEDAC-MACS.

CONCLUSION

we first give two attacks on DAC-MACS and EDAC-MACS for their backward revocation security.Then, a new effective data access control scheme for multi authority cloud storage systems (NEDAC-MACS) is proposed to withstand the two vulnerabilities and thus to enhance the revocation security. NEDACMACS can withstand the two vulnerabilities even though the non revoked users reveal their received key update keys to the revoked user. In NEDAC-MACS, the revoked user has no chance to decrypt any objective cipher text even if it actively eavesdrop to obtain an arbitrary number of non revoked users' Key Update Keys KUK or collude with some non revoked users or obtain any transmitted information**.**

SECURITY ANALYSIS OF NEDAC-MACS

In the formal security analysis of NEDAC- MACS is given to prove that our NEDAC-MACS can guarantee collusion resistance, revocation security, data confidentiality and provable security against static corruption of authorities under security. NEDAC-MACS scheme supports backward security in context of attribute revocation if the x ˜$k$revoked user has no chance to passively retrieve its ability to decrypt any x ˜k-corresponding ciphertext CT as a nonrevoked user, whether the CT is updated previous ciphertext or the newly outsourced ciphertext

REFERENCES:

[1] Kan Yang and Xiaohua Jia, ―Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage ―, in IEEE Trans. Parallel Distributed System, vol 25, No.7, pp 17351744, July 2014.

[2] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-Policy

Characteristic-Based Encryption,'' in Proc. IEEE Symp. Security and privacy (S&P'07), 2007, pp. 321-334.

[3] B. Waters, ''Ciphertext-Policy Characteristic-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,'' in Proc. 4th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC'11), 2011, pp. 53-70.