A dynamic searchable encryption CP-ABE scheme in cloud storage

JIANG Yi[1,a], FENG Hao[1,b]

[1]Chongqing University of Posts and Telecommunications School of computer science and technology, Chongqing 400065, China

[a]jiangyi@cqupt.edu.cn, [b]651435309@qq.com

Keywords: Ciphertext index, CP-ABE, Ciphertext sharing, Ciphertext local update, Proxy Re-encryption

Abstract. In this paper, we constructed a dynamic searchable encryption CP-ABE scheme (DSE-CP-ABE)which is based on cipher text index. The scheme combined the existing cipher text strategy of access control scheme, extended inverted index structure, and introduced the trusted third party, which not only realized the cipher text sharing, but also supported for local update of the cipher text.At the same time we used the Proxy Re-encryption to ensure the backward and forward security. Compared with the existing access control schemes, this scheme significantly reduces the number of times of local updates, and is of higher security, reliability and practicability.

1. Introduction

Cloud storage is used as a basic service because of its low cost, but how to guarantee the legal user data confidentiality and access has been the focus of cloud storage.In the literature[4], the KP-ABE scheme is proposed by using the property of the private key embedded in the user's additional identity information. In the literature [6], a kind of strategy is designed, which supports the LSSS access structure. The literature [7] proposed an AB-ACER cryptographic access control scheme. Zhou Qing etc[9] proposed a KP-ABE scheme, which combines the Lucene inverted index and the homomorphic encryption. But the above scheme cannot realize the local update of the cipher text. Literature [5] extended the inverted index and achieved the local update of the ciphertext, but it can't share of ciphertext.Aiming at the above problem, this paper proposed a dynamic access control scheme based on the cipher text index. It not only accelerated the cipher text search speed, but also realized the cipher text sharing and dynamic alterations of cipher text.

2. Preliminary knowledge

2.1 CP-ABE[10]

CP-ABE algorithm usually has following steps:

(1) $Setup$:Input a random number r ,calculate $Setup(r) = \{MK, PK\}$,where MK is main key, and PK is public key.

(2) $Encrypt$:Input PK access structure T and plaintext M , then calculate $CT = Encrypt(PK, M, T)$, where CT is cipher-text.

(3) $KenGen$:Input MK user attributes A , then calculating $SK = KeyGen(MK, A)$, where SK is private key.

(4) $Decrypt$:Input SK and CT , calculate $M = Decrypt(SK, CT)$, M is plaintext.

3. DSE-CP-ABE

The scheme includes four entities: the trusted third party(TTP), the data owner(DO), users(U), cloud storage service provider(CSP).The scheme is shown in figure 3.1:

The scheme includes key generation, encryption, file local update , attribute change algorithms.

3.1Key generation:

algorithm $Setup$ of document [10] to generate public key PK and master key MK and using the

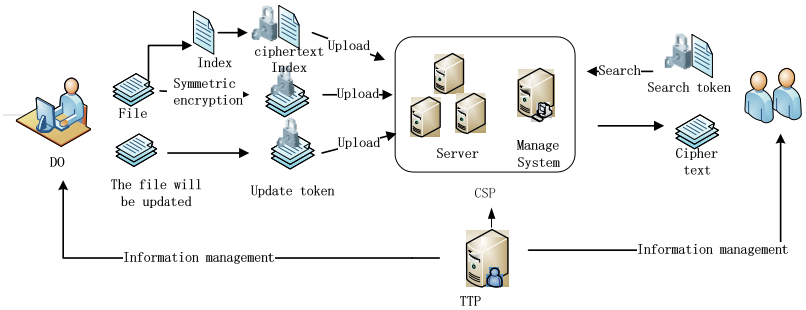


Figure 3.1 cloud storage system model

algorithm $KenGen$ to generate the private key SK .

3. 2 Encryption. It includes file encryption, index encryption, key encryption and re-encryption.

(1) Encrypt file and index: According to the algorithm Enc of literature [5] ,output cryptograph index $\gamma = (A_s, T_s, A_d, T_d)$ and cryptograph collection $c = (c_1, c_2, \mathrm{L}\ , c_n)$, which A_s is the cryptograph query array , T_s is the cryptograph query dictionary, A_d is the cryptograph delete array, and T_d is cryptograph delete dictionary, c_n is the encrypted file of file f_n .

(2) Encrypt Key: According to the algorithm $Encrypt$ of literature [5] to generation Key cipher CK .Calculate the cipher text $CT = CK \mid\mid c$. CK is used as the access control section, and c is used as the data segment of the cipher text retrieval.

(3) Re-encryption: after Do uploading cipher CT to CSP,CSP will re-encrypt it before the storage. It includes the cipher text and the encrypted index re-encryption.

① Re-encrypt cipher text: According to the re-encryption algorithm of the AB-AECR[7]to generate the re-encryption cipher text $CT^{'}$.

② Re-encrypt cipher index: By algorithm $\mathrm{Re}\,EncryptIndex(K_{\lambda_y}, T_s, T_d)$: Input the re-encryption key K_{λ_y} , T_s and T_d to calculate the re-encryption cipher text query dictionary $T_s^{'} := T_s \oplus G_{K_2}(K_{\lambda_y})$ and re-encryption cipher text delete dictionary $T_d^{'} := T_d \oplus G_{K_2}(K_{\lambda_y})$, Where $G_{K_2}(K_{\lambda_y})$ represents using the pseudo random function to encrypt K_{λ_y} . At last, update the re-encryption cipher text index $\gamma^{'} := (A_s, T_s^{'}, A_d, T_d^{'})$

3.3 File local update

File update, including add and delete file. Firstly, it must obtain the encryption key K .We can obtain K by the algorithm $Decrypt$ of reference [7].Users use K to generate the corresponding add or delete tokens, then CSP re-encrypts the token and updates the cipher text index and the cipher text.

(1) Generate token: By the algorithm $AddToken$ of the DSSE scheme[5] to generate the add token τ_a , the cipher text c_{f_1} to be added; reference algorithm $DelToken$ to generate the delete token τ_d .

(2) Re-encrypt token: Let τ_a be represented as $(\tau_1, \tau_2, \lambda_1, \mathrm{L}\ , \lambda_{\#f})$, τ_d represented as $(\tau_1, \tau_2, \tau_3, id)$. By algorithm $\mathrm{Re}\,AddToken(\tau_a, \tau_d, K_{\lambda_y})$: Input τ_a , τ_d and re-encryption key K_{λ_y} to calculate re-encrypt add token $\tau_\alpha^{'} := (\tau_1, \tau_2 \oplus G_{K_2}(K_{\lambda_y}), \lambda_1, \mathrm{L}\ , \lambda_{\#f})$ and re-encrypt delete token $\tau_d^{'} := (\tau_1, \tau_2 \oplus G_{K_2}(K_{\lambda_y}), \tau_3, id(f))$. Then let $\tau_a^{'}$ be represented as $(\tau_1, \tau_2^{'}, \lambda_1, \mathrm{L}\ , \lambda_{\#f})$, $\tau_d^{'}$ represented as $(\tau_1, \tau_2^{'}, \tau_3, id)$.

(3) File updates: $DecryptT(T_s^{'}, T_d^{'}, \tau_2^{'})$: Input $T_s^{'}$, $T_d^{'}$, $\tau_\alpha^{'}$ and $\tau_2^{'}$,then calculate cryptograph query dictionary $T_s := T_s^{'} \oplus \tau_2^{'}$ and cryptograph delete dictionary $T_d := T_d^{'} \oplus \tau_2^{'}$.

① Add file: Re-encrypt c_{f_1} by algorithm $\mathrm{Re}\,Encrypt$ of literature [7],and get the

re-encryption cipher text CT_{f_1}; According to algorithm *Add* by literature[5], get new A_s, T_s, A_d and T_d. At last, CSP updated file as follows: $CT' = CT' + CT_{f_1}$.

② Delete file: Obtain new T_s and T_d by the algorithm *Del* of document[5],and then delete the file represented as id as $CT' = CT' - C_{id}$.

(4) Update index by $\mathrm{Re}\,EncryptIndex(K_{\lambda_\gamma}, T_s, T_d)$ and get the new cipher index $\gamma' = (A_s, T_s', A_d, T_d')$.

3. 4 Attributes change

We re-encrypt the cipher text and the index when attributes change. For the cipher text re-encryption, we can reference to the literature [7].For the index, we follow the algorithm $Index\,\mathrm{Re}\,Encrypt(T_d', T_s', K_{\lambda_i})$: Input T_s', T_d' and the re-encryption key K_{λ_i} when attributes changing, calculate $T_s'' = T_s' \oplus G_{K_2}(K_{\lambda_i}')$, $T_d'' := T_d' \oplus G_{K_2}(K_{\lambda_i}')$ and get the new index $\gamma'' := (A_s, T_s'', A_d, T_d'')$.

4. Security analysis

The security of data includes the security of the cipher text data, the secret key and the cipher text. For the security of the cipher text data and the secret key, its security has been proved in the literature [7]. As for the index γ, CSP re-encrypted the re-encryption key K_{λ_γ} by pseudo random function, encrypted the index γ with XOR. DSE-CP-ABE scheme has the key updating mechanism, which ensures the backward security and forward security. The forward and backward security of the cipher text has been proved in the literature [7]. For the cipher text index, before a user has the attribute, he cannot decrypt the CSP re-encryption cipher text index, because he couldn't get re-decryption key K_{λ_i}', which is the backward security. When a user's attribute is removed, he will be immediately withdrawn from the users group by TTP, and re-encryption will be executed immediately, then his decryption key will lose the decryption ability, which is the forward security.

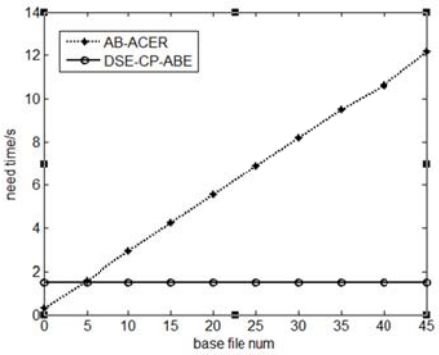
5. Performance analysis

Based on the same CP-ABE algorithm, our scheme is compared with the document [7] AB-AECR scheme. Experiment 1: update an encrypted file, with the base file number changing, then compare the update time of two schemes.Experiment2: With the same base file number, and the encrypted file number changing, then compare the update time of two schemes.

The analysis of the experimental results: as AB-AECR does not support local update, when update

the same file number, the time of AB-AECR scheme will increase with the base file number, while the time of our scheme is constant. When the base file number is same, with the increased of update

file number, the time of AB-AECR is more than our scheme.



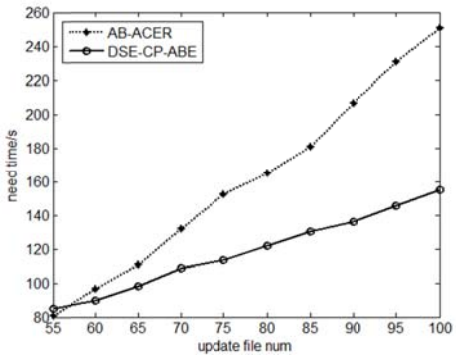


Fig.1 update same file count Fig.2 with the same base file count

6. Conclusion

In this paper, for the traditional CP-ABE local update, which is based on the security index, a new dynamic CP-ABE is proposed. The scheme improves the search efficiency, realizes the file sharing and the local update of the encrypted data, and ensures the security when the attributes change.

Acknowledgements

This paper was financially supported by Chongqing Municipal Education Committee of science and technology research project (KJ1400414). The correspondence Author: Feng Hao, 13637828641.

References

[1] Liu Z, Cao Z, Wong D S. Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay[C]//Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013: 475-486.

[2] Naveed M, Prabhakaran M, Gunter C. Dynamic searchable encryption via blind storage[C]//Security and Privacy (SP), 2014 IEEE Symposium on. IEEE, 2014: 639-654.

[3] Kamara S, Papamanthou C. Parallel and dynamic searchable symmetric encryption[M]//Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013: 258-274.

[4] Li Q, Feng D, Zhang L. An attribute based encryption scheme with fine-grained attribute revocation[C]//Global Communications Conference (GLOBECOM), 2012 IEEE. IEEE, 2012: 885-890.

[5] Kamara S, Papamanthou C, Roeder T. Dynamic searchable symmetric encryption[C]//Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012: 965-976.

[6] Chen J, Ma H. Efficient decentralized attribute-based access control for cloud storage with user revocation[C]//Communications (ICC), 2014 IEEE International Conference on. IEEE, 2014: 3782-3787.

[7] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. Parallel and Distributed Systems, IEEE Transactions on, 2011, 22(7): 1214-1221.

[8] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007: 321-334.

[9] Zhou Qing. Research and implementation of the support sort of the cipher text retrieval[D]. Huazhong University of Science and Technology,2013

[10] Xiong A P, Gan Q X, He X X, et al. A searchable encryption of CP-ABE scheme in cloud storage[C]//Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2013 10th International Computer Conference on. IEEE, 2013: 345-349.

[11] Liu Aifen. Efficient and dynamic search method of cipher text in cloud environment[D]. Northeastern University,2013.