Encryption in Cloud Computing With Efficient File Hierarchy

S.K. Manigandan*, J. Rathna, J. Velmurugan and D. Ramya
Dept. of Master of computer application, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Anna University, Chennai, India.
***Corresponding author: E-Mail: kgmanigandan@gmail.com**

ABSTRACT

The scoop in cloud computing which loads in the cloud stand will use the Cipher text-policy attribute-based encryption(CP-ABE) .Here, it is a precious encryption applied science to avail in protect scoop sharing in cloud computing. The shared scoop files have multilevel chain of command, and are used in the field of the military and healthcare. But, the hierarchy structure has not been explored in CP-ABE. Here, the layered access architecture are integrated into a single access architecture, and then the files are encrypted with the integrated access architecture. The advanced blueprint is proved to be protected under the authoritative posit. The cipher text elementals affiliated to attributes could be shared by the files. Therefore, Moreover, Experimental simulation shows the number of the files incrementing, the advantages of our blueprint become more and more noticeable. Additionally, here both cipher text repository and time costs of encryption are protect.

KEY WORDS: Cloud computing, scoop sharing, file hierarchy, cipher text-policy, attribute-based encryption.

1. INTRODUCTION

Cloud computing is one of the most promising utilization scaffold to deal with the hazardous complex of scoop sharing. Online scoop sharing has become so craze in these days with gregarious media and scoop sharing designates like whatsapp, Facebook. Meanwhile, leaking, users need to encrypt their scoop before being shared.

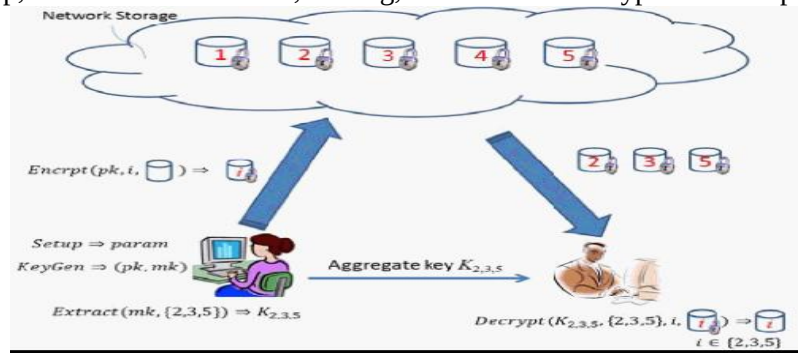

Fig.1. An example of secure data sharing in cloud computing

Access control is paramount as it is the first line of resistance that prevents unauthorized access to the shared scoop. Recently, attribute-based encryption (ABE) has been captivated much more attentions since it can keep scoop isolation and realize fine-grained, one-to-many, and non-interactive access control. Cipher text-policy attribute based encryption (CP-ABE) is one of feasible schemes which has much more appropriate and is more suitable for general applications.

In cloud computing, as illustrated in Fig.1, authority accepts the user enrolment and actualizes some parameters. Cloud service provider (CSP) is the administrator of cloud servers and provides multiple services for client. Scoop owner encrypts and uploads the engender cipher text to CSP. User downloads and decrypts the interested cipher text from CSP. The shared files usually have hierarchical structure. That is, group offices are divided into a number of hierarchy subgroups located at different access levels. If the files in the same stratified architecture could be encrypted by integrated access architecture, the repository cost of cipher text and time cost of encryption could be saved. Encryption and repository overhead of cipher text can be reduced greatly. Moreover, since convey nodes (Fig.2) are integrated in the access architecture, users can decrypt all acquiescence files with computation of secret key once. The computation cost of decryption can additionally be decreased if users need to decrypt various files simultaneously.

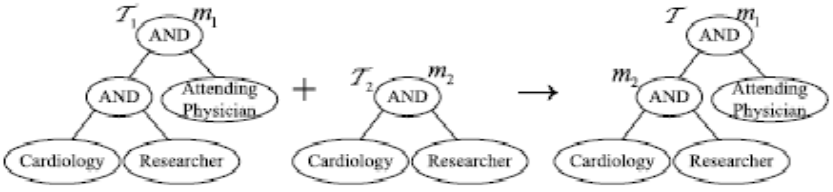

Fig.2. The integrated access structure, T_1 and T_2 are access structures m_1 and m_2 respectively, T is the integrated access structure of m_1 and m_2

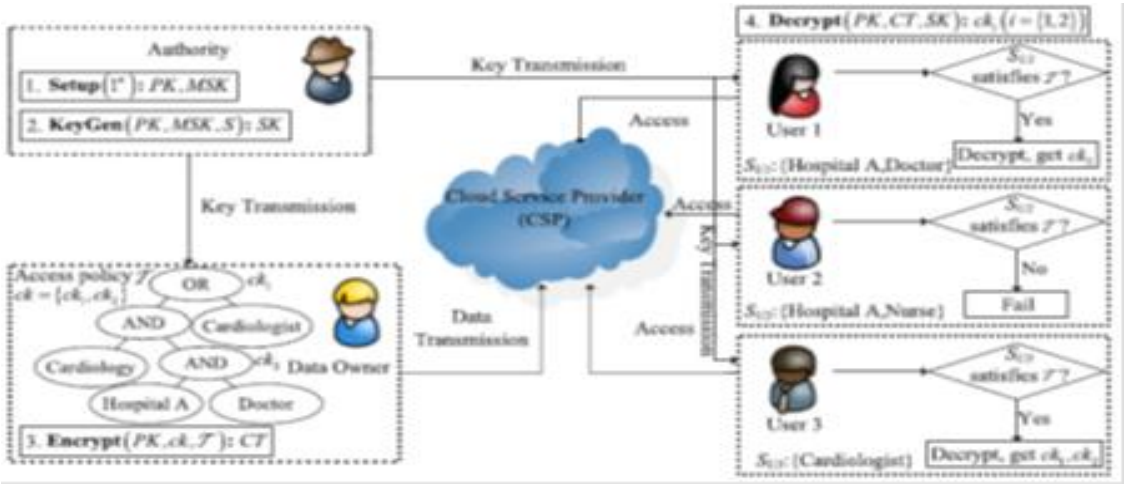

Figure.3. System archtecture

Cloud Service Provider (CSP): It is a semi-trusted entity in cloud frame of reference. It can honestly perform the allow tasks and return correct results. However, it would like to find out as much perceptive contents as possible. In the advanced system, it provides cipher text repository and transmission services.

Data Owner: It has large scoop needed to be stored and shared in cloud system. In our blueprint, the entity is in charge of defining access architecture and executing Encrypt operation. And it uploads cipher text to CSP.

User: It wants to access a large number of scoop in cloud system. The entity first downloads the corresponding cipher text. Then it executes Decrypt operation of the advanced blueprint. In Fig. 4, a scoop owner processes the files as follows:

Firstly, the scoop owner chooses k content keys {ck1, . . . , ckk}, and encrypts files {m1, . . . , mk} with the content keys by using symmetric encryption algorithm (i.e., DES, AES). The cipher texts are denoted as Eck (M) = {Eck1 (m1), . . ., Eckk (mk)}. Then, the data owner encrypts {ck1, . . . , ckk}.

2. MATERIALS AND METHODS

The Proposed FH-CP-ABE Scheme: In this section, the detailed construction of FH-CP-ABE scheme is first presented. Then, based on the scheme, an improved encryption process about FH-CP-ABE scheme is proposed in order to reduce computational complexity. In addition, a brief discussion about FH-CP-ABE scheme's features is also provided.

Security Analysis: Security of this work involves two aspects: file cipher text confidentiality and content key cipher text confidentiality. We assume that the hierarchical files are safely encrypted by using symmetric encryption algorithm (i.e., DES, AES). Therefore only the security proof of FH-CP-ABE should be provided. In this section, the security game of the proposed blueprint is given firstly. Then a formal security proof is provided based on the results of the literatures.

CPA Security Game for the Proposed Scheme: In the proposed blueprint, SK is user's secret key associated with attribute set, and CT denotes cipher text associated with access architecture. Security model of the proposed blueprint requires that the adversary selects the challenging structure A*. Moreover, the adversary can require all SK where the only restriction is that SK does not satisfy A*.

Initialization: The adversary A selects the challenging access architecture A∗ and submits A* to the challenger C.

Setup: C runs the Setup operation of FH-CP-ABE blueprint and sends public key PK to A.

Query Phase1: For the attribute sets S1, . . . , Sq1(∀i ∈[1, . . . , q1], Si /∈A∗) chosen by A, he can repeatedly ask C for the secret keys SK. Meanwhile, C answers these secret keys SK by running Key Gen algorithm.

Challenge: A submits two messages m0 and m1 of equal length. C randomly picks a bit μ ∈ {0, 1} and Encrypts mμ with A. The resulting cipher text CT∗ is given to A.

Query Phase2: Same as the Query Phase1.

Guess: Finally, A guesses ˆμ ∈ {0, 1}. If ˆμ = μ, A wins the security game. In this game, A can win the game which is defined as AdvA(1κ) = |Pr[ˆμ = μ] −(1/2)|.

3. RESULTS AND DISCUSSION

The experimental results are given in Fig.4. Fig.4(a) shows the time cost of encryption and decryption, while Fig.4(c) shows the storage cost of cipher text for various attributes with two hierarchy files. Fig.4(b) and Fig.4(d) shows the time cost and the storage cost for various files with fixed attributes N = 30, respectively. In addition, for various attributes and files, the numbers of attributes and files used in the simulation are N= {10, 15, 20, 25, 30, 35, 40, 45, 50} and k = {2, 4, 6, 8}.

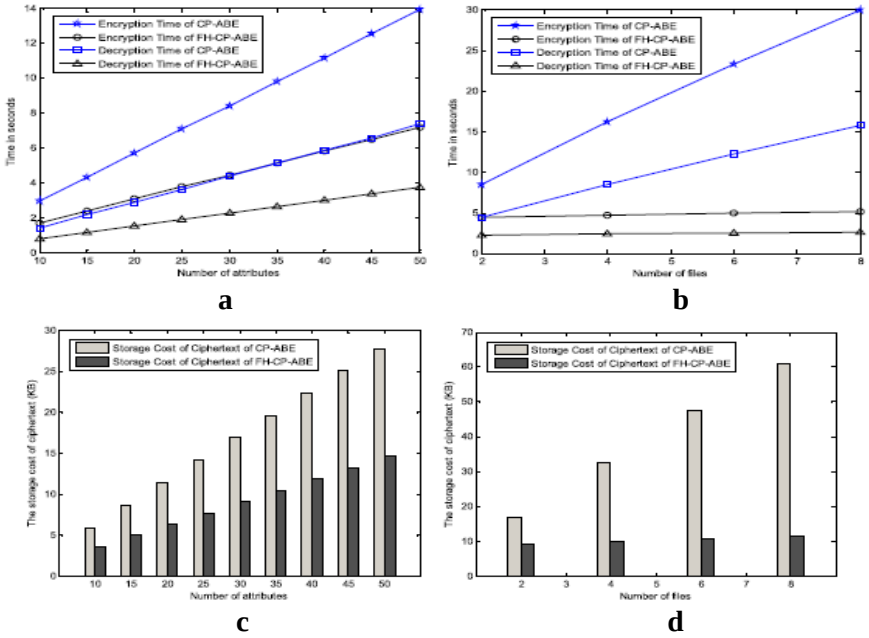

Figure.4. Experimental analysis

As illustrated in Fig.4(a), we can find that the proposed scheme improves the efficiencies of encryption and decryption greatly when two hierarchy files are shared. We can also find that the results are gradually increasing and approximately following a linear relationship with the number of attributes in Fig.4(a). When the number of files is fixed, the more the number of attributes is used, the more time cost of encryption and decryption in FH-CP-ABE scheme is saved. For example, in Fig.4(a), the encryption costs of FH-CP-ABE and CP-ABE scheme are 1.8s and 3s approximately when $N = 10$. Similarly, the values are 7s and 14s when $N = 50$. The difference jumps from 1.2s to 7s when N is changed from 10 to 50. For the storage cost of cipher text, we find that the value in FH-CP-ABE scheme is smaller than CP-ABE's and follows a linear relationship approximately as the number of attributes grows as shown in Fig.4(c). If the number of files is fixed, the more the number of attributes is used, the higher efficiency in our scheme is improved in terms of storage cost of cipher text. For example, in Fig.4(c), when $N = 20$ and $N = 50$, the approximate storage costs of cipher text are equal to 6.3KB and 14.6KB in FH-CP-ABE scheme, and the values are 11.3KB and 27.8KB in CP-ABE scheme.

When two hierarchy files are shared, the performance of FH-CP-ABE blueprint is better than CP-ABE's in terms of encryption and decryption's time cost, and *CT*'s storage cost. The reason is described as below. As shown in Fig.4(a) and Fig.4(c), the number of files is $k = 2$. Based on the Table I, the encryption time in CP-ABE and FH-CP-ABE scheme can be simplified as $[2(|AC1|+|AC2|)+ 2]G0 + 4GT$ and $(2|AC1| + 2)G0 + (2\ j\ |AT| + 4)GT$, respectively, where j and $|AT|$ are relatively small in proposed encryption operation. It shows that our scheme can save more encryption time with more common attributes $|AC2|$. Similarly, the storage cost of *CT* in both schemes can be denoted as $[2(|AC1| + |AC2|) + 2]LG0 + 2LGT$ and $(2|AC1| + 2)LG0 + (\ j\ |AT| + 2)LGT$, respectively. It indicates that the FH-CP-ABE scheme has smaller storage cost of cipher text than the CP-ABE in the same condition. In addition, the decryption time for CP-ABE and FH-CP-ABE is approximate to $(4|Au| + 2)Ce + [2(|S1| + |S2|) + 4]GT$ and $(2|Au| + 1)Ce + [2|S1| + (\ j\ |AT| + 4)]GT$, respectively. Obviously, FH-CP-ABE scheme has lower decryption cost with a same number of common nodes $|S2|$. So, comparing with CP-ABE and FH-CP-ABE, the encryption cost in our scheme is decreased by $(2|AC2|G0 - 2\ j\ |AT\ |GT)$ in Fig.4(a). Similarly, the storage cost of CT and the decryption cost in FH-CP-ABE scheme are reduced by $2|AC2|LG0 - j\ |AT\ |LGT)$ and $(2|Au| + 1)Ce + [2|S2| - j\ |AT|]GT$ in Fig.4(c) and Fig.4(a), respectively, compared to CP-ABE's. The above simulation results also confirm to theoretical analysis described in previous subsection.

Above all, when multiple hierarchy files with different access levels are shared, the experiment results indicate that FH-CP-ABE blueprint performs better than CP-ABE in terms of the time cost of encryption and decryption, and storage cost of *CT*, if the number of attributes is fixed. The reason is described as follows. In Fig.4(b) and Fig.4(d), the number of attributes is fixed as $N = 30$. Based on the Table.1, the encryption cost in CP-ABE and FH-CP-ABE blueprint can be denoted as $[2(|AC1| + \ldots + |ACk|) + k]G0 + 2kGT$ and $(2|AC1| + k)G0 + (2\ j\ |AT| + 2k)GT$, where $k = \{2, 4, 6, 8\}$ in the simulation, and j and $|AT|$ are relatively small in our proposed blueprint. It indicates that FH-CP-ABE requires less encryption time than CP-ABE with more hierarchy files k. Similarly, the *CT*'s storage cost in both blueprints can be denoted as $[2(|AC1| + \ldots + |ACk|) + k]LG0 + kLGT$ and $(2|AC1| + k)LG0 + (j\ |AT| + k)LGT$, respectively. And the decryption time for CP-ABE and FH-CP-ABE is approximate to $k(2|Au|+1)Ce+[2(|S1|+\ldots+|Sk|)+2k]GT$ and $(2|Au|+ 1)Ce + [2|S1| + (\ j\ |AT| + 2k)]GT$, respectively. The results show that FH-CP-ABE blueprint can save more storage cost and decryption time than CP-ABE under the same condition.

In Fig.4(b), the time cost of encryption and decryption in FH-CP-ABE blueprint is reduced by [2*(*|A*C*2|+. . .+|A*Ck*|*)*G0− 2 *j* |A*T* |G*T*] and *(k* −1*)(*2|A*u*|+1*)Ce* +[2*(*|S2|+. . .+|*Sk* |*)*− *j* |A*T* |]G*T* , respectively, compared to CP-ABE's. Similarly, comparing with CP-ABE and FH-CP-ABE, the storage cost m of *CT* in our scheme is decreased by [2*(*|A*C*2| + . . . + |A*Ck*|*)L*G0 − *j* |A*T* |*L*G*T*] in Fig.4(d). Meanwhile, the results are also consistent with theoretical analysis presented in previous subsection.

4. CONCLUSION

In this paper, we proposed a variant of CP-ABE to efficiently share the stratified files in cloud computing. The stratified files are encrypted with integrated access architecture and the cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption are saved. The advanced blueprint has an advantage that users can decrypt all authorization files by computing protect key once. Thus, the time cost of decryption is also saved if the user needs to decrypt various files. Moreover, the advanced blueprint is proved to be protecting under DBDH assumption. The saved storage cost is approximately 44.2% and 47.5% with *N* changed from 20 to 50.

Conflict of interest: The author declares having no competing interests.

5. ACKNOWLEDGEMENT

The author wish to thank Vel Shree Dr. R. Rangarajan, Chancellor, Vel Tech High Tech Dr. RR and Dr. SR Engineering College, for the support and facilities provided for the preparation of this paper.

Financial disclosure: No financial support was received for this implementation.

REFERENCES

Balu A and Kuppusamy K, An expressive and provably secure cipher text-policy attribute-based encryption, Inf. Sci, 276, 2014, 354–362.

Bethencourt J, Sahai A, and Waters B, Cipher text-policy attribute based encryption, in Proc. IEEE Symp. Secur. Privacy, 2007, 321–334.

Chen Y, Jiang Z.L, Yiu S.M, Liu J.K, Au M.H, and Wang X, Fully secure cipher text-policy attribute based encryption with security mediator, in Proc. 16th Int. Conf. Inf. Commun. Secur, 8958, 2014, 274–289.

Cheung L and Newport C, Provably secure cipher text policy ABE, in Proc. 14th ACM Conf. Comput. Commun. Secur, 2007, 456–465.

Chu C.K, Zhu W.T, Han J, Liu J.K, Xu J, and Zhou J, Security concerns in popular cloud storage services, IEEE Pervasive Comput, 12 (4), 2013, 50–57.

Fan C.I, Huang V.S.M, and Ruan H.M, Arbitrary-state attribute based encryption with dynamic membership, IEEE Trans. Comput, 63 (8), 2014, 1951–1961.

Goyal V, Pandey O, Sahai A, and Waters B, Attribute-based encryption for fine-grained access control of encrypted data, in Proc. 13th ACM Conf. Comput. Commun. Secur, 2006, 89–98.

Guo F, Mu Y, Susilo W, Wong D.S, and Varadharajan V, CP-ABE with constant-size keys for lightweight devices, IEEE Trans. Inf. Forensics Security, 9 (5), 2014, 763–771.

Ibraimi L, Petkovic M, Nikova S, Hartel P, and Jonker W, Mediated cipher text-policy attribute-based encryption and its application, in Proc. 10th Int. Workshop Inf. Secur. Appl, 2009, 309–323.

Jiang T, Chen X, Li J, Wong D.S, Ma J, and Liu J, TIMER: Secure and reliable cloud storage against data re-outsourcing, in Proc. 10th Int. Conf. Inf. Secur. Pract. Exper, 8434, 2014, 346–358.

Liang K, A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing, IEEE Trans. Inf. Forensics Security, 9 (10), 2014, 1667–1680.

Liang K, A secure and efficient cipher text-policy attribute-based proxy re-encryption for cloud data sharing, Future Generat. Comput. Syst, 52, 2015, 95–108.

Liang K, Liu J.K, Wong D.S, and Susilo W, An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing, in Proc. 19th Eur. Symp. Res. Comput. Secur, 8712, 2014, 257–272.

Liu J, Huang X, and Liu J.K, Secure sharing of personal health records in cloud computing: Cipher text-policy attribute-based sign cryption, Future Generat. Comput. Syst, 52, 2015, 67–76.

Liu J.K, Au M.H, Huang X, Lu R, and Li J, Fine-grained two factor access control for Web-based cloud computing services, IEEE Trans. Inf. Forensics Security, 11 (3), 2016, 484–497.

Liu X, Ma J, Xiong J, and Liu G, Cipher text-policy hierarchical attribute-based encryption for fine-grained access control of encryption data, Int. J. Netw. Secur, 16 (6), 2014, 437–443.

Sahai A and Waters B, Fuzzy identity-based encryption, in Advances in Cryptology, Berlin, Germany: Springer, 2005, 457–473.

Xie X, Ma H, Li J, and Chen X, An efficient cipher text-policy attribute-based access control towards revocation in cloud computing, J. Universal Comput. Sci, 19 (16), 2013, 2349–2367.

Yang Y, Liu J.K, Liang K, Choo K.K.R, and Zhou J, Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data, in Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS), 9327, 2015, 146–166.

Yuen T.H, Liu J.K, Au M.H, Huang X, Susilo W, and Zhou J, k-times attribute-based anonymous access control for cloud computing, IEEE Trans. Comput, 64 (9), 2015, 2595–2608.

Yuen T.H, Zhang Y, Yiu S.M, and Liu J.K, Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks, in Proc. 19th Eur. Symp. Res. Comput. Secur, 8712, 2014, 130–147.

Zheng H, Yuan Q, and Chen J, A framework for protecting personal information and privacy, Secur. Commun. Netw, 8 (16), 2015, 2867–2874.

Zhu W, Yu J, Wang T, Zhang P, and Xie W, Efficient attribute-based encryption from R-LWE, Chin. J. Electron, 23 (4), 2014, 778–782.