International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 30 No. 3 May 2017, pp. 389-394
© 2017 Innovative Space of Scientific Research Journals
http://www.ijisr.issr-journals.org/

Cipher Text Attribute Based Encrypted Data Sharing With Escrow in Cloud Computing

N. Jayapriya, V. Maheswari, M. Moovarasi, and G. Shanthi

Department of Computer science and engineering,
SKP Engineering College, Thiruvannamalai, India

Copyright © 2017 ISSR Journals. This is an open access article distributed under the ***Creative Commons Attribution License***, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT: Attribute-based encryption (ABE) is a very promising scheme suitable for access control in cloud storage system. It proposes a hierarchical attribute based access control scheme with constant size cipher text. This scheme is efficient because the length of cipher text and the number of bilinear pairing evaluations through a constant are fixed. By using this, prevent KA and CSP from knowing each other's master secret key so that none of them can create the whole secret keys of users individually thus, the fully trusted KA can be semi-trusted. This scheme is implement in cloud for ensuring privacy and uphold security through upload and download file.

KEYWORDS: KA – key authority, Attribute-based encryption, remove escrow, Weighted power.

1 INTRODUCTION

Confuse compute has become a study hot-spot due touts disguised long-list advantages (e.g. ease, high scalability). One of the most promising cloud computing applications is on-line data sharing, such as photo sharing in On-line Social Networks among more than one billion users and on-line health record system. A data owner (DO) is usually willing to store large amounts of data in cloud for saving the cost on local data management. Without any data security device, cloud service provider (CSP), but, can fully gain access to all data of the user. This brings a likely security danger to the user, since CSP may compromise the data for commercial benefits. Accordingly, how to securely and efficiently share user data is one of the toughest challenges in the picture of blur compute .Cipher text-policy attribute-based encryption (CP-ABE), has turned to be an important encryption technology to tackle the challenge of secure data sharing. In a CP-ABE, user's secret key is described by an attribute set, and cipher text is associated with an access structure. DO is allowed to define access structure over the universe of attributes. A user can decrypt a given cipher text only if his/her attribute set matches the access structure over the cipher text. Employing a CP-ABE system directly into a cloud application that may yield some release problems. Firstly, all users' secret keys need to be issued by a fully trust key power (KA). This bring a safety risk that is known as key escrow problem. By knowing the secret key of a system user, the KA can decrypt all the user's cipher texts, which stands in total against to the will of the user. Secondly, the clarity of attribute set is another concern Thus, the storage cost and encryption cost for a cipher text can be relieved. We use the following example to further illustrate our approach. Suppose there is a formal structure in university, in which teachers are classified into lessons helper, lecturer, associated university lecturer and full institution of higher education lecturer.

In this case, they can be denoted by one attribute which has just dissimilar weights. Therefore, the storage visual protuberance of the parallel cipher text and the computational cost used in encryption can be reduced In addition; our method can be used to express larger attribute breathing space than increasingly under the same number of attribute. pro case, if both the attribute space and one-sided set include n elements, the proposed scheme can describe $n2$ different possibilities. In contrast, the existing CPABE schemes only show $2n$ possibilities. Employing a CP-ABE system directly into a cloud application that may yield some open problems. Firstly, all users' secret keys need to be issued by a fully trusted key authority (KA).

Corresponding Author: N. Jayapriya

2 RELATED WORK

In 2005, Sinai and Waters introduced fuzzy identity based encryption (IBE), which is the seminal work of attribute based encryption (ABE). After that, two variants of ABE were proposed: key-policy ABE (KP-ABE) and CP-ABE depending on if a given policy is associated with either a cipher text and a key. Later, many CP-ABE schemes with specific features have been presented in the literature. For example, presented a novel access control scheme in cloud computing with efficient attribute and user revocation. The computational overhead is significantly eliminated from O (2*N*) to *O*(*N*) in user key generation by improving CPABE scheme, where *N* is the number of attributes. The size of cipher text is approximately reduced to half of original size. However, the security proof of the scheme is not fully given. Most of the existing CP-ABE schemes require a full trusted authority with its own master secret key as input to generate and issue the secret keys of users. Thus, the key escrow issue is inherent, such that the authority has the "power" to decrypt all the cipher texts of system users. Chase *et al.* presented a distributed KP-ABE scheme to solve the key escrow difficulty in a multi-authority scheme. In this approach, all authorities, which are not colluded with each other, are participating in the key generation protocol in a spread way, such that they cannot team their data and link multiple attribute sets belonging to the same user. Because there is no centralized authority with master secret in order, all element authorities should speak with others in the scheme to form a user's secret key.

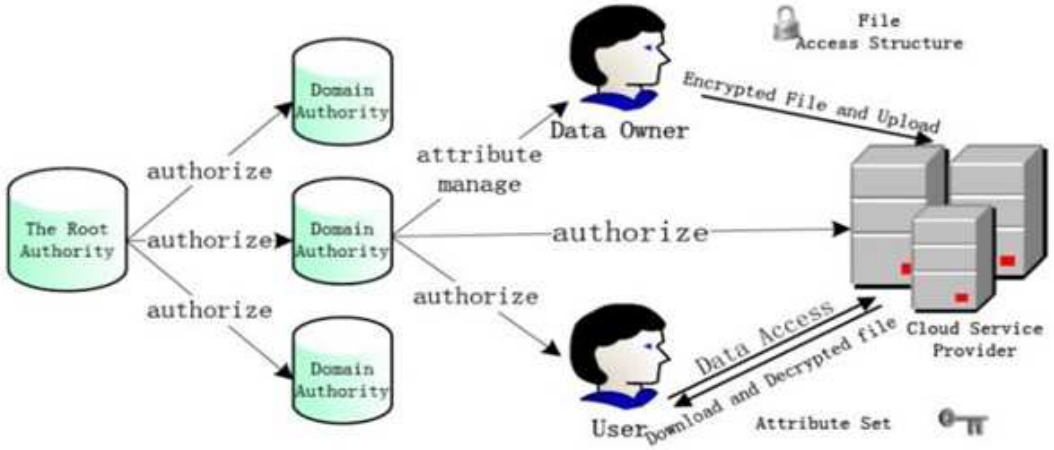
3 PROBLEM DEFINITION

A data owner (DO) is usually willing to store large amounts of data in cloud for saving the cost on local data management. Without any data safety machine, cloud service provider (CSP), however, can fully gain access to all data of the user. This brings a likely safety risk to the user, since CSP may compromise the data for commercial benefits. Firstly all users' secret keys need to be issued by a fully trusted key authority (KA). This bring a security danger that is known as key escrow problem. By knowing the secret key of a system user, the KA can decrypt all the user's cipher texts, which stands in total against to the will of the user.

4 PROPOSED SYSTEM

We propose an attribute-based data sharing scheme for cloud computing applications, which is denoted as cipher text-policy weighted ABE scheme with removing escrow (CP-WABE-RE).We propose an improved key issuing protocol to resolve the key escrow problem of ABE in cloud computing. The protocol can prevent KA and CSP from knowing each other's master secret key so that none of them can create the whole secret keys of users individually thus, the fully trusted KA can be semi-trusted. Data confidentiality and privacy can be ensured.

5 SYSTEM DESIGN



6 PERFORMANCE ANALYSIS

We investigate and evaluate the fine organization of the proposed scheme with the schemes in Theoretical and experimental aspects.

A. Theoretical Analysis

1) *Key Escrow and Weighted Attribute:* Table I shows the problem of key escrow, feature of weighted attribute and application in cloud computing for each scheme. The key escrow in CP-WABE-RE scheme can be removed by using an improved key issuing protocol for cloud computing. uses escrow-free key issuing protocol to solve the issue. On the contrary, both don't solve the problem of key escrow. In addition, the weighted attribute in CP-WABERE scheme can not only support arbitrary-state attribute instead of the traditional binary state In Table I, we can find that only CP-WABE-RE scheme can simultaneously support all the three functions. solves the problem of key escrow so it can satisfy environment of cloud system as ours. cannot remove key escrow. Thus the both schemes cannot be directly applied in cloud computing.

2) *Efficiency:* In Table II and Table III, we compare efficiency of the above four schemes on storage overhead and computation cost in theory, where the used symbols are defined in Table IV. To simplify the comparisons, access structure, data reencryption dynamic membership management that is, user joining, leaving, and attribute updating) of are not included in the following analysis. In addition, the cost of transmission isn't involved when implementing the interactive protocols in both [15] and our proposed scheme.

B. Experimental Analysis

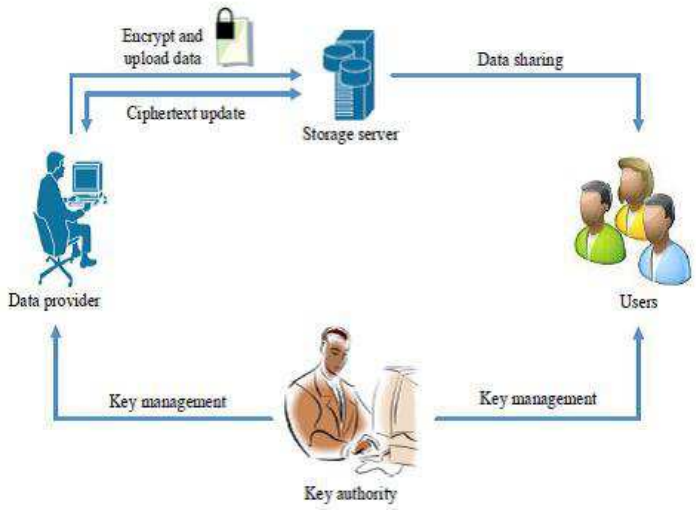
Now, to validate theoretical analysis proposed in previous subsection, we execute CP-WABE-RE scheme by using the cape toolkit and the Java Pairing-Based Cryptography library (JPBC). *Simulation Analysis of Weighted Attribute:* Next, we measure and analyze the storage overhead and computation cost for encrypting (by a DO) data, where the number of attributes in access policy is $N = \{10, 20, 30, 40, 50\}$.

- Key Generation: Private key = x 2R G;
  - Public key is y=g power of x.
- Signature : 0 < k < p -1 and gcd(k; p -1) = 1.
  - Compute r =gk mod p.
  - Compute s = (H(m)- xr)k-1 (modp - 1).
  - Signature = (r; s)
- Veri_cation : gH(m) = yrrs mod p.

7 MODULE DESCRIPTION

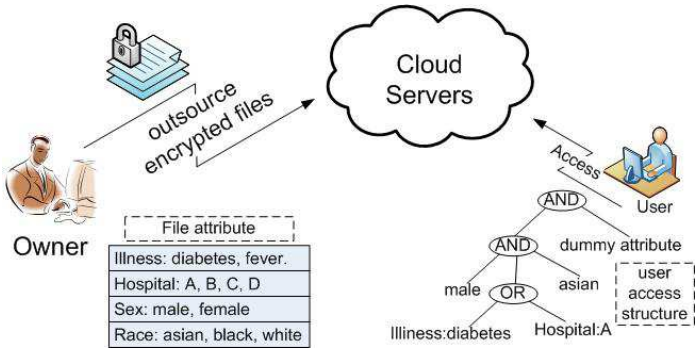
A. Key Authority (KA):

It is a semi-trusted entity in confuse system. i.e., KA is honest-but-curious, which can honestly perform the assigned tasks and return correct results. However, it will collect as many sensitive contents as possible. In confuse system, the unit is responsible for the users' employment. Meanwhile, it not only generates most part of system parameter, but also creates most part of secret key for each user.



B. Cloud Service Provider (CSP):

It is the manager of cloud servers and also a semi-trusted entity which provides many services such as data storage, computation and transmission. To solve the key escrow problem it generates both parts of system parameter and secret key for each user.



C. Data Owners (DO):

They are owners of files to be store in cloud method. They are in blame of defining contact structure and execute data encryption operation. They also upload the cipher text to CSP.

F

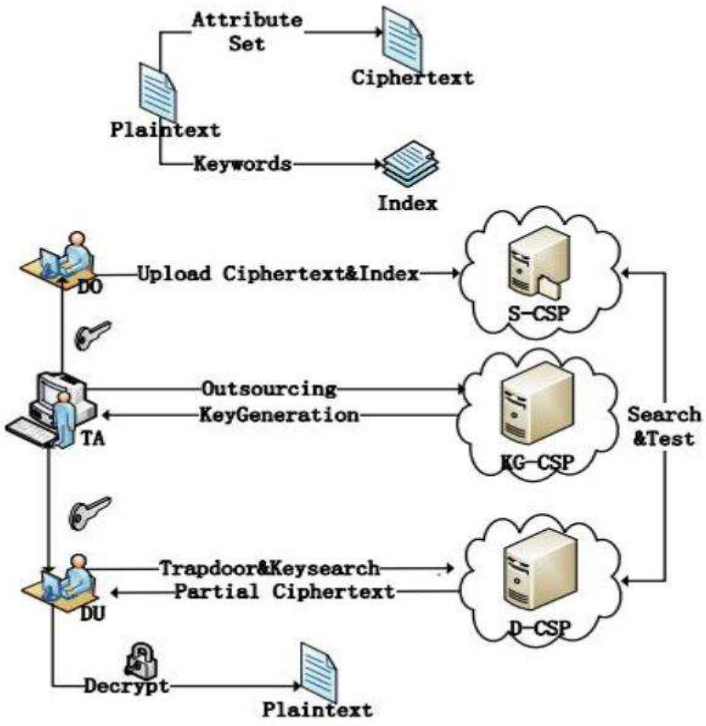
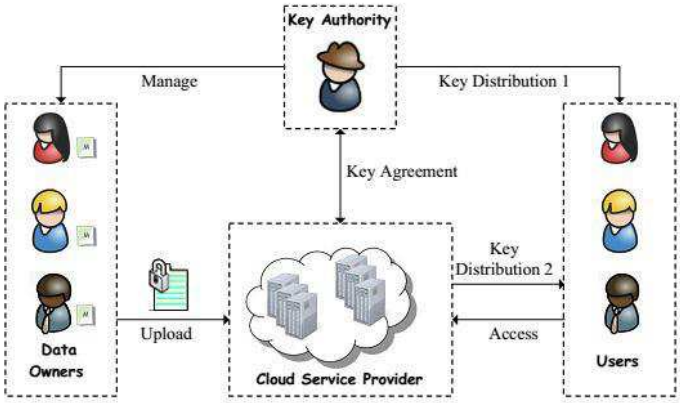


Fig. 1. System architecture

D. Users:

They want to access cipher text stored in cloud system. They download the cipher text and execute the corresponding decryption operation.



8 ALGORITHMS/TECHNIQUES USED

Setup (λ)→PP

1. Randomly choose y ∈ z_P to be the master secret key,MSK.
2. Output PP = (G,GT, g, g^y,H) where G and GT are main p-ordered group, g is a generator for G, and H : ID_{space} -> G is some hash function.

Encrypt(M, ID) -> CT

(Note that M,CT ∑GT .)

1. Randomly choose s ∑ Z_p.
2. Compute e(H(ID) ,g^y)^s = e(H(ID),g)^{ys}.
3. Output CT = (g^s,M . e(H(ID),g)^{ys}).

KeyGen(ID,MSK) -> SK

1. Output SK_{ID} = H(ID)^y, noting that y is the MSK.

Decrypt (CT,SK_{ID}) ->M

1. Compute e(SK_{ID},C_1) = e(H(ID)^y,g^s)

Which is the blind thing for the meaning M in C2.

2. Output M = C_2/e(SK_{ID},C_1).

Note the relative among D-H three-party key agreement and B-F:

Party X ~ Hash function g^x ~ H(ID)

Party Y ~MSK authority g^y ~ g^y

Party Z ~Encrypter g^z ~ g^s.

9 CONCLUSION AND FUTURE WORK

In this paper, we redesigned an attribute-based data allocation plan in cloud compute. The improved key issue protocol was open to resolve the key escrow problem. It enhances data confidentiality and privacy in cloud system against the managers of KA and CSP as well as malicious system outsider, where KA with CSP are semi-trusted. In adding, the one-sided attribute was proposed to improve the expression of attribute, which can not only describe arbitrare state attributes, but also reduce the complexity of access policy, so that the storage space rate of cipher text and time cost in encryption can be saved. Finally, we vacant the act and security analysis for the proposed scheme, in which the results show high effectiveness and security of our plan.

REFERENCES

[1] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A secure cloud computing based framework for big data information management of IEEE Transactions on Cloud Smart grid. IEEE Transaction on cloud computing 2015.

[2] H.Deng,Q. Wu,B.Qin,J.Han,J.K.LIU,j.Xu,andJ.Zhou.Security concers in popular cloud storage services.IEEE Pervasive Computing,12(4):50-57,2013

[3] A. Balu and K. Kuppusamy. An expressive and provably secure Cipher text-policy attribute-based encryption Information Science2014.

[4] J. Bethencourt, A. Sahai, and B. Waters. Cipher text-policy attribute-based encryption.IEEE Symposium on Security and Privacy,pages 321-334,2007.

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil *the 4th Conference on Theory of Cryptography* , 17(4):297–319, 2007.

[6] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[7] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[8] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007.

[9] M.Chese.Multi-authority attribute based encryption the 4th Conference on Theory of Cryptography, pages 515-514,2007.

[10] L.Cheung and C.Newport.Provably secure cipher text policy ABE.Proceeding of the 14thACM conference on computer and communications security ,pages 456-465,2007.

[11] S.SCHOW.Removing escrow from identity-based encryption,proceedingnof the 12th International Conference on Practice and Theory in Public Key Crptography,pages 256,276,2009.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for Fine-grained access control of encrypted data proceeding od the 13th ACM conference on computer communication pages 89_98,2006.