International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue X, October- 2016

DATA SHARING SCHEME REVISITED IN CLOUD COMPUTING USING ABE

R. Balachandran
PG Scholar
Department of Computer Science and Engineering
Adithya Institute of Technology
foreversribalu@gmail.com

V. Ganesh Karthikeyan
Assistant Professor
Department of Computer Science and Engineering Adithya Institute of Technology
saravanakumarme85@gmail.com

Dr.N.Chitra Devi
Professor & Head
Department of Computer Science and Engineering
Adithya Institute of Technology
chitradevi_n@adithyatech.com

ABSTRACT

Data sharing scheme by using attribute based to reduce the key escrow issue but also develops the expressiveness of attribute, because of that the resulting scheme is more user friendly to cloud computing. In this proposed work we are introducing an improved two-party key issuing protocol that can guarantee that neither key authority nor cloud service operator can compromise the whole secret key of a user individually. We introduce the concept of attribute with weight, being provided to enhance the expression of attribute, which can not only extend the expression from binary to arbitrary state, but also lighten the complexity of access policy. So that, both storage cost and encryption complexities for a cipher text are relieved. In our proposed work the modification process is after the data owner sends secret key to the user, the particular cloud user can view the data which is stored in cloud server. Once the user used that secret key means the key will be automatically changed for that shared data, this dynamic key will be send to the data owner also.

Keywords

Cloud Computing, Data sharing, CP-ABE Attribute, Encryption.

INTRODUCTION

Today's Cloud Computing becomes more and more sensitive information are being centralized into the cloud, such as emails, personal medical records, finance data, and government proofs, etc. The fact that data owners and cloud server are no longer in the same secured domain may put the outsourced unencrypted data at risk the cloud server may leak data information to unauthorized users or even be hacked. It follows that sensitive data has to be encrypted prior to outsourcing for data privacy and combating unsolicited accesses. Data encryption makes effective data utilization a very challenging task given that there could be a large amount of outsourced data. Data owners may share their outsourced data with a large amount of users, who might want to only retrieve certain specific data files they are interested in during a given session. One of the most popular ways to do so is through keyword-based search. Such keyword search technique allows data users to receive the files of interest and has been widely applied in plaintext search scenarios.

Data encryption, which demands user's ability to perform keyword search and further restricts the protection of keyword privacy, makes the traditional normal text search methods fail for encrypted cloud data. Traditional methods allows searchable encryption schemes to a cloud client to securely search over encrypted data through keywords without first decrypting it, these techniques support only conventional Boolean search, without capturing any relevance of the files in the search result. When directly applied in large collaborative data outsourcing cloud mechanism, they may suffer from the following two main drawbacks. Firstly for each search request, users without pre-knowledge of the encrypted cloud data have to go through every retrieved file, which

demands possibly large amount of post processing over-head; Another one is invariably sending back all files solely based on presence/absence of the keyword further incurs huge unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. Lacking of effective mechanisms to ensure the file retrieval accuracy is a significant drawback of proposed searchable encryption schemes in the context of Cloud Computing. The state of the art in information retrieval (IR) community has already been utilizing various scoring methods to quantify and rank-order the relevance of files in response to any given search query. Although the importance of ranked search has received attention for a long history in the context of plaintext searching by IR community, surprisingly, it is still being overlooked and remains to be studied in the context of encrypted cloud data search.

Cloud computing has become a research hot-spot due to its distinguished long-list advantages (e.g. convenience, 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 protection mechanism, cloud service provider (CSP), however, can fully gain access to all data of the user. This brings a potential security risk 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 scenario of cloud computing.

Ciphertext-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 ciphertext is associated with an access structure.

DO is allowed to define access structure over the universe of attributes. A user can decrypt a given ciphertext only if his/her attribute set matches the access structure over the ciphertext.

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). This brings a security 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 ciphertexts, which stands in total against to the will of the user. Secondly, the expressiveness of attribute set is another concern. As far as we know, most of the existing CP-ABE schemes can only describe binary state over attribute, for example, "1 - satisfying" and "0 - not-satisfying", but not dealing with arbitrary-state attribute.

In this paper, the weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, but also to simplify access policy. Thus, the storage cost and encryption cost for a ciphertext can be relieved. We use the following example to further illustrate our approach.

In later we will demonstrate that following the exactly same security guarantee of existing SSE scheme, it would be very inefficient to achieve ranked keyword search, which motivates us to further weaken the security guarantee of previous SSE appropriately and realize an "as-strong-as-possible" ranked searchable symmetric encryption. This notion has been employed by cryptographers in much recent work where efficiency is preferred over security.

2 RELATED WORKS

In 2005, Sahai 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) CP-ABE depending on if a given policy is

associated with either a ciphertext 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(2N)* to *O(N)* in user key generation by improving CP-ABE scheme, where *N* is the number of attributes. The size of ciphertext 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 ciphertexts of system users. Chase and Chow presented a distributed KP-ABE scheme to solve the key escrow problem in a multi-authority system. In this approach, all authorities, which are not colluded with each other, are participating in the key generation protocol in a distributed way, such that they cannot pool their data and link multiple attribute sets belonging to the same user. Because there is no centralized authority with master secret information, all attribute authorities should communicate with others in the system to create a user's secret key. But, a major concern of this approach is the performance degradation. It results in *O(N2)* communication overhead on both the system setup phase and any rekeying phase. It also requires each user to store *O(N2)* additional auxiliary key components in addition to the attribute keys, where *N* is the number of authorities in the system. Chow later proposed an anonymous private key generation protocol for IBE where a KA can issue private key to an authenticated user without knowing the list of the user's identities. It seems that this approach can properly be used in the context of ABE if attributes are treated as identities. However, this scheme cannot be adopted for CP-ABE, since the identity of user is a set of attributes which is not publicly unknown.

In 2013, provided an improved security data sharing scheme based on the classic CP-ABE. The key escrow issue is addressed by using an escrow-free key issuing protocol where the key generation center and the data storage center work together to generate secret key for user. Therefore, the computational cost in generating user's secret key increases because the protocol requires interactive computation between the both parties.

Besides, Liu *et al.* presented a finegrained access control scheme with attribute hierarchy, where are built on top of respectively. In the schemes, the attributes are divided into multiple levels to achieve fine-grained access control for hierarchical attributes, but the attributes can only express binary state. Later, Fan *et al.* proposed an arbitrary-state ABE to solve the issue of the dynamic membership management. In this paper, a traditional attribute is divided to two parts: attribute and its value.

3 CHALLENGES AND CONTRIBUTIONS

Attribute based encryption (ABE) determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to receivers and senders can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). The CA in that construction has the power to decrypt every ciphertext, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. In that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user. In this work, we proposed a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling

their information on particular users, thus making ABE more usable in practice.

We often identify people by their attributes. In 2005, Sahai and Waters proposed a system in which a sender can encrypt a message specifying an attribute set and a number d, such that only a recipient with at least d of the given attributes can decrypt the message. However, the deployment implications of their scheme may not be entirely realistic, in that it assumes the existence of a single trusted party who monitors all attributes and issues all decryption keys. Instead, we often have different entities responsible for monitoring different attributes of a person, e.g. the Department of Motor Vehicles tests whether you can drive, a university can certify that you are a student, etc. Thus, Chase gave a multi-authority ABE scheme which supports many different authorities operating simultaneously, each handing out secret keys for a different set of attributes. However, this solution was still not ideal. There are two main problems: one concern of security of the encryption, the other the privacy of the users.

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 protection mechanism, cloud service provider (CSP), however, can fully gain access to all data of the user. This brings a potential security risk 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 scenario of cloud computing. Firstly, all users' secret keys need to be issued by a fully trusted key authority (KA). This brings a security 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 expressiveness of attribute set is another concern. As far as we know, most of the existing CP-ABE schemes can only describe binary state over attributes, for example, "1 - satisfying" and "0 - not-satisfying", but not dealing with arbitrary-state attribute.

3.1 Our Contributions

Inspired by, we propose an attribute-based data sharing scheme for cloud computing applications, which is denoted as ciphertext-policy weighted ABE scheme with removing escrow (CP-WABE-RE). It successfully resolves two types of problems: key escrow and arbitrary-sate attribute expression. The contributions of our work are as follows:

• We propose an improved key issuing protocol to resolve the key escrow problem of CP-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.

• We present weighted attribute to improve the expression of attribute. The weighted attribute can not only express arbitrary-state attribute (instead of the traditional binary state), but also reduce the complexity of access policy. Thus the storage cost of ciphertext and computation complexity in encryption can be reduced. Besides, it can express larger attribute space than ever under the same condition. Note that the efficiency analysis will be presented in Section V.

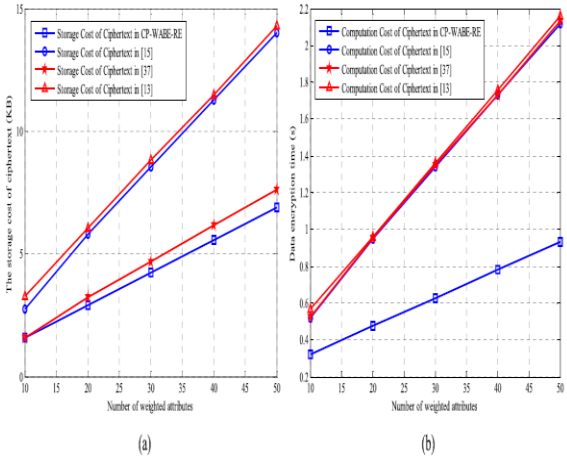
• We conduct and implement comprehensive experiment for the proposed scheme. The simulation shows that CP-WABE-RE scheme is efficient both in terms of computation complexity and storage cost. In addition, the security of CP-WABE-RE scheme is also proved under the generic group model.

4. METHODOLOGY OVERVIEW

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. Hur 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-WABE-RE scheme can not only support arbitrary-state attribute instead of the traditional binary state, but also simplify access policy associated with a ciphertext as opposed. Unfortunately, can only express arbitrary-state attribute, and cannot simplify the access structure. In Table I, we can find that only CP-WABE-RE scheme can simultaneously support all the three functions. Hur solves the problem of key escrow so it can satisfy environment of cloud system as ours. However, both cannot remove key escrow. Thus the both schemes cannot be directly applied in cloud computing.

2) Efficiency: we compare efficiency of the above four schemes on storage overhead and computation cost in theory. To simplify the comparisons, access structure, data re-encryption of, and 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 and our proposed scheme. In the schemes are compared in terms of CT size, SK size, PP size and MSK size. CT size represents the storage overhead in cloud computing and also implies the communication cost from DO to CSP, or from CSP to users. SK size denotes the required storage cost for each user. PP and MSK sizes represent the storage overhead of KA and CSP in terms of public parameter and master secret key.



CONCLUSION AND FEATURE WORKS

In this paper, we redesigned an attribute-based data sharing scheme in cloud computing. The improved key issuing protocol was presented 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 outsiders, where KA and CSP are semi-trusted. In addition, the weighted attribute was proposed to improve the expression of attribute, which can not only describe arbitrarystate attributes, but also reduce the complexity of access policy, so that the storage cost of ciphertext and time cost in encryption can be saved. Finally, we presented the performance and security analyses for the proposed scheme, in which the results demonstrate high efficiency and security of our scheme. Although the parameter can be downloaded with ciphertexts, it would be better if its size is independent of the maximum number of ciphertext classes. On the other hand, when one carries the delegated keys around in a mobile device without using special trusted hardware, the key is prompt to leakage, designing a leakage-resilient cryptosystem yet allows efficient and flexible key delegation is also an interesting direction.

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 smart grid," *IEEE Trans. Cloud Comput.*, vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.

[2] A. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," *Inf. Sci.*, vol. 276, no. 4, pp. 354–362, Aug. 2014.

[3] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham, "Randomizable proofs and delegatable anonymous credentials," in *Proc. 29th Annu. Int. Cryptol. Conf.*, 2009, pp. 108–125.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334.

[5] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, 2004.

[6] M. Chase, "Multi-authority attribute based encryption," in *Proc. 4th Conf. Theory Cryptogr.*, 2007, pp. 515–534.

[7] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 121–130.

[8] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 456–465. [9] S. S. M. Chow, "Removing escrow from identity-based encryption," in *Proc. 12th Int. Conf. Pract. Theory Public Key Cryptogr.*, 2009,pp. 256–276.

[10] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," *IEEE Pervasive Comput.*, vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[11] A. De Caro and V. Iovino, "JPBC: Java pairing based cryptography," in *Proc. 16th IEEE Symp. Comput. Commun.*, Jun./Jul. 2011, pp. 850–855.

[12] H. Deng *et al.*, "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," *Inf. Sci.*, vol. 275, no. 11, pp. 370–384, Aug. 2014.