TRADEMARK BASED DATA SHARING SCHEME REVISITED IN CLOUD COMPUTING

T.Sirisha[1], Ch.Shiva Kumar[2]

[1]*Student, Computer Science and Engineering Department, Prakasam Engineering College, Andhra Pradesh, India,* ***Tokalasirisha65@gmail.com***

[2]*Asociate Professor, Computer Science and Engineering Department, Prakasam Engineering College, Andhra Pradesh, India,* ***chskumars3@gmail.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. Cloud storage is the best and proficient approach to handle our information remotely. In any case, since information proprietors and clients are more often than not outside the trusted area of cloud specialist co-ops the information security and get to control is the critical component at the season of delicate information put away in the cloud. Additionally, now days there are distinctive systems are accessible for information sharing and saving security of information proprietor and client. Key Escrow is the one of the significant issue now a day. We can't keep full trust over the key power focus since they might be abuse their benefits. This is unsatisfactory for data sharing circumstances. In this paper we concentrated the current procedure for sharing the information from information proprietor to information client. The methodology propose an enhanced two-party key issuing convention that can ensure that neither key power nor cloud specialist co-op can bargain the entire mystery key of a client exclusively. The method also present the idea of quality with weight, being given to upgrade the statement of characteristic, which cannot just extend the expression from paired to discretionary state, additionally help the intricacy of get to approach. 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.

Index Terms: *Cloud Computing, Data sharing, CP-ABE Attribute, Encryption, Data Confidentiality, Key Authority, Access Control policy, Data Sharing, Attribute-based encryption*

---------- *** ----------

1. INTRODUCTION

In current era there are bunches of quickly developing patterns and cloud registering is one of them. Cloud gives simple, proficient stage to store information, secure information, and get to information at any area with the assistance of web. Additionally it gives client adaptable foundations, storage room and execution. Accordingly, how to securely and efficiently share user data is one of the toughest challenges in the scenario of cloud computing.

In a CP-ABE, client's mystery key is portrayed by a trait set, and ciphertext is connected with a get to structure. DO is permitted to characterize get to structure over the universe of traits. A client can unscramble a given ciphertext just if his/her trait set matches the get to structure over the ciphertext. Utilizing a CP-ABE framework specifically into a cloud application that may yield some open issues Firstly, all clients' mystery keys should be issued by a completely trusted key power (KA). This brings a security hazard that is known as key escrow issue. By knowing the mystery key of a framework client, the KA can unscramble the entire client's ciphertext, which remains altogether against to the will of the client. 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.

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.

Assume there is a formal structure in college, in which instructors are characterized into showing partner, speaker, related teacher and full educator [1]. We circulate the heaviness of the characteristic for every kind of the instructors as 1, 2, 3, and 4. In this way, these qualities can be indicated as "Educator: 1", "Educator: 2", "Instructor: 3" and "Instructor: 4", individually. For this situation, they can be signified by one trait which has quite recently extraordinary weights. Specifically, it can be arbitrary state properties, for example, "Instructor: showing associate, teacher, relate educator, full teacher". We here accept that an get to arrangement is spoken to as: T {("Lecturer" OR "Partner Teacher" OR "Full Professor") AND "Male"}, and the current CP-ABE plans are executed on the type of get to strategy T . On the off chance that our proposed plan is sent, the T can be rearranged as T ′{"Teacher: 2" AND "Male"}, since the characteristic "Instructor: 2" indicates the base level in the get to approach and incorporates {"Teacher: 2", "Instructor: 3" "Instructor: 4"} as a matter of course. In this manner, the capacity overhead of the comparing ciphertext and the computational cost utilized as a part of encryption can be lessened. These two structures are appeared in Fig. 1. Likewise, our technique can be utilized to express bigger quality space than any time in recent memory under a similar number of qualities. For instance, if both the property space and weighted set incorporate n components, the proposed plan can portray n2 distinctive potential outcomes. Interestingly, the current CPABE plots just show 2n conceivable outcomes.

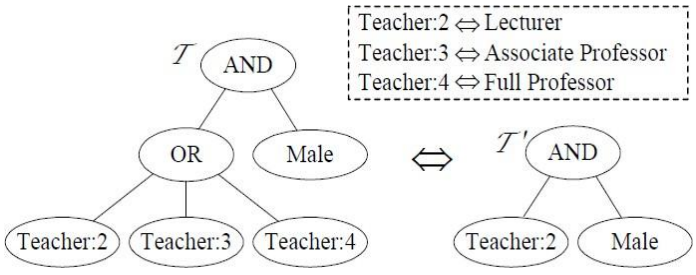

Fig. 1.Two equivalent access structures of a ciphertext. T represents a general access policy in the existing CP-ABE schemes. T ′denotes an improved access policy in the proposed scheme [1].

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(*2*N)* 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(N*2*)* communication overhead on both the system setup phase and any rekeying phase. It also requires each user to store *O(N*2*)* 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 poolingtheir 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.

SYSTEM MODEL

As illustrated in Fig. 3 and Fig. 4, the system model and framework of CP-WABE-RE scheme in cloud computing are given, where the system consists of four types of entities: KA, CSP, DO and Users. In addition, we provide the detailed definition of CP-WABE-RE scheme

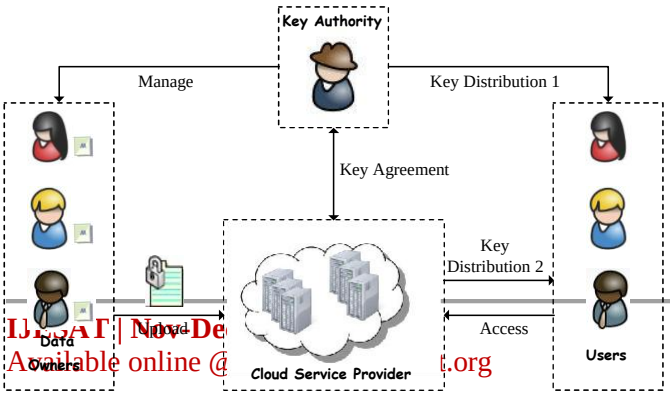

Fig. 3. System model of CP-WABE-RE scheme in cloud computing

It is a semi-trusted entity in cloud system. Namely, 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 cloud system, the entity is responsible for the users' enrollment. Meanwhile, it not only generates most part of system parameter, but also creates most part of secret key for each user.

Cloud Service provider 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

Data Owners (DO). They are owners of files to be stored in cloud system. They are in charge of defining access structure and executing data encryption operation. They also upload the generated ciphertext to CSP.

Users. They want to access ciphertext stored in cloud system. They download the ciphertext and execute the cor- responding decryption operation.

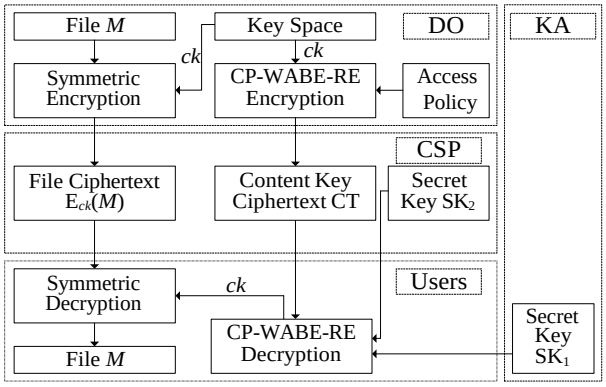

Fig. 4. System framework of CP-WABE-RE scheme

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] *Shulan Wang, Kaitai Liang, Joseph K. Liu, JianyongChen, Jianping Yu, WeixinXie ,"Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEETransactions on Information Forensics and Security, 2016.*

[2] *Shulan Wang, Junwei Zhou, Joseph K. Liu, JianpingYu,Jianyong Chen, WeixinXie ,"An Efficient File HierarchyAttribute-Based Encryption Scheme in CloudComputing", IEEE Transactions on Information Forensicsand Security, 2016*

[3] *Kaitai Liang and Willy Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage", IEEE Transactions on InformationForensics and Security, 2015*

[4] *JieXu, Qiaoyan Wen, Wenmin Li and ZhengpingJin,"Circuit Ciphertext-policy Attribute-based HybridEncryption with Verifiable Delegation in CloudComputing", IEEE TRANSACTIONS ON PARALLELAND DISTRIBUTED SYSTEMS ,2015*

[5] *Danwei Chen, Liangqing Wan, Chen Wang, Su Pan,YutingJi, "A Multi-authority Attribute-based EncryptionScheme with Pre-decryption", 2015 IEEE SeventhInternational Symposium on Parallel Architectures,Algorithms and Programming*

[6] *J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attributebased encryption "in Proceedings of IEEE Symposium on Security andPrivacy, pp. 321V334, 2007.*

[7] *V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, "Multiauthorityattribute-based encryption with honest- but-curious centralauthority" International Journal of Computer Mathematics, vol. 89,pp. 3,2012.*

[8] *V. Goyal, O. Pandey, A. Sahai, and B.Waters"Attribute-basedencryption for fine-grained access control of encrypted data," inProceedings of the 13th ACM conference on Computer andcommunications security, pp. 89{98, 2006}*

[9] *Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryptionscheme for secure data sharing in a cloud environment," InformationSciences .In Press, 2012.*

[10] *M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. "Secureattribute-based systems". In Proceedings of the 13th ACM conference onComputer and communications security, pages 99{112. ACM Press NewYork, NY, USA, 2006*