Attribute-Based Data Sharing Scheme through Cloud Computing Cipher Text Policy

[1]MD AHMAD ALI, [2]S MD ISMAIL

[1]PG Scholar, Department of CSE, Al Habeeb College Of Engineering And Technology, Village Damergidda, Mandal Chevella , District Ranga Reddy, Telangana, India

[2]Associate Professor, Department of CSE Al Habeeb College Of Engineering And Technology, Village Damergidda, Mandal Chevella , District Ranga Reddy, Telangana, India

Abstract— Data sharing scheme by using attribute primarily based to reduce the key escrow issue however additionally develops the quality of attribute, as a result of that the resulting theme is a lot of user friendly to cloud computing. During this planned work we tend to introduce an improved two-party key provision protocol that may guarantee that neither key authority nor cloud service operator can compromise the entire secret key of a user on an individual basis. We tend to introduce the thought of attribute with weight, being provided to enhance the expression of attribute, which might not solely extend the expression from binary to discretionary state, however additionally lighten the complexness of access policy. So that, each storage cost and encoding complexities for a cipher text are relieved. In our planned work the modification method is when the data owner sends secret key to the user, the particular cloud user will read the data that is hold on in cloud server. Once the user used that secret key means that the key are automatically modified for that shared information, this dynamic key are send to the data owner additionally.

Index Terms— Cloud Computing, Attribute-Based Encryption, Key Escrow, Weighted Attribute, Key Authority, Access Control Policy, Data Sharing,;

I. INTRODUCTION

Today's Cloud Computing becomes more and more sensitive data are being centralized into the cloud, like emails, personal medical records, finance information, and government proofs, etc. the actual fact that information owners and cloud server are no longer within the same secured domain might place the outsourced unencrypted information at risk the cloud server may leak information data to unauthorized users or maybe be hacked. It follows that sensitive information should be encrypted before outsourcing for information privacy and combating unsolicited accesses. Encoding makes effective information utilization a really challenging task as long as there may well be an outsized amount of outsourced information.

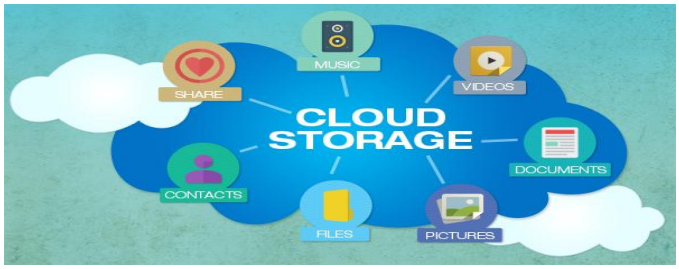


Figure 1: Architecture of Cloud Storage

In this paper data Owner (DO) is usually willing to store massive amounts of data in cloud for saving the cost on local data management. Without any information protection mechanism, cloud service provider (CSP), however, will absolutely gain access to all information of the user. This brings a possible security risk to the user, since CSP could compromise the information for business advantages. Consequently, a way to firmly and

with efficiency share user data is one in every of the toughest challenges within the situation of cloud computing. Cipher-text-policy attribute-based encoding (CPABE) has turned to be an important encoding technology to tackle the challenge of secure data sharing. In a CPABE, user's secret key is represented by an attribute set, and cipher-text is related to an access structure. DO is allowed to outline access structure over the universe of attributes. A user will decode a given cipher-text provided that his/her attribute set matches the access structure over the cipher-text. Using a CP-ABE system directly into a cloud application that will yield some open issues foremost, all users' secret keys need to be issued by a completely trustworthy key authority (KA) this brings a security risk that is referred to as key escrow problem. As way as we know, most of the prevailing CP-ABE schemes will only describe binary state over attributes, as an example, "1 - satisfying" and "0 – not-satisfying", however not managing arbitrary-state attribute. During this paper, the weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, however additionally to change access policy. Thus, the storage value and coding value for a cipher-text may be relieved. During this paper, the weighted attribute is introduced to not only extend attribute expression from binary to discretional state, however additionally to change access policy. Thus, the storage value and coding value for a cipher-text may be alleviated. We tend to use the following example to additional illustrate our approach. Suppose there is a formal structure in university, within which academics are classified into teaching assistant, lecturer, associated professor and professor. we tend to distribute the load of the attribute for every variety of the academics as one, 2, 3, and 4. Therefore, these attributes may be denoted as "Teacher: 1", "Teacher: 2", "Teacher: 3" and "Teacher: 4", respectively. During this case, they can be denoted by one attribute that has simply completely different weights. Specially, it may be arbitrary-state attributes, like "Teacher: teaching assistant, lecturer, professor, full professor". We tend to here assume that an access policy is represented as: T, and also the existing CP-ABE schemes are executed on the form of access policy T. If our planned theme is deployed, the T may be simplified as T 9, since the attribute "Teacher: 2" denotes the minimum level within the access policy and includes by default. Therefore, the storage overhead of the corresponding cipher-text and therefore the machine value utilized in encoding may be reduced.

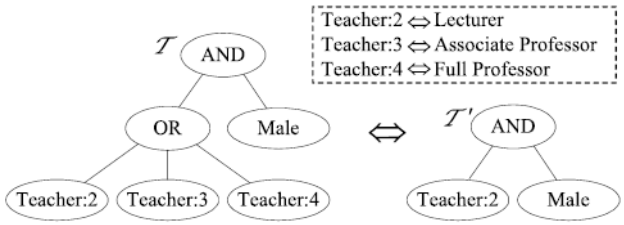


Figure 2: Architecture of Two Equivalent Access Structures of a Cipher-text.

II. RELATED WORK

In 2013, provided associate improved security data sharing theme based on the classic CP-ABE the key escrow issue is addressed by exploitation associate escrow-free key provision protocol wherever the key generation center and therefore the information storage center work together to generate secret key for user. Therefore, the computational cost in generating user's secret key will increase as a result of the protocol needs interactive computation between the each party besides; Liu et al. conferred a fine-grained access management theme with attribute hierarchy, wherever designed on prime, severally. Within the schemes, the attributes are divided into multiple levels to achieve fine-grained access management for hierarchical attributes; however the attributes will only categorical binary state. Later, Fan et al. planned an arbitrary-state ABE to resolve the difficulty of the dynamic membership management.

During this paper, a traditional attribute is divided to two parts: attribute and its price. As an example, the standard attributes will be denoted as. The improved attributes are denoted as:, wherever "Career" represents associate attribute and "Doctor", "Professor" and "Engineer" denote the values of the attribute "Career". Consequently, the computation cost for attributes is more expensive than that of the standard schemes under a similar variety of attributes. We tend to note that there are another analysis works on CP-ABE; however, they leverage completely different techniques to achieve information sharing. We are going to not compare them with our present system.

III. FRAME WORK

In this paper, for the first time, we tend to propose an attribute-based data sharing theme for cloud computing applications that is denoted as cipher-text-policy weighted Attribute Based Encryption scheme with removing escrow (CP-WABE-RE). It effectively resolves two types of problems: key escrow and arbitrary-sate attribute expression. The contributions of our work are as follows: we tend to propose associate improved key issuing protocol to resolve the key escrow problem of CP-ABE in cloud computing. The protocol will prevent KA and CSP from knowing every other's master secret key in order that none of them will produce the complete secret keys of users individually. Thus, the fully trustworthy KA may be semi-trusted. Data confidentiality and privacy can be ensured. We tend to present weighted attribute to boost the expression of attribute. The weighted attribute can not only categorical arbitrary-state attribute (instead of the traditional binary state), however additionally reduce the complexity of access policy. Therefore the storage cost of cipher-text and computation complexity in encoding are often reduced. Besides, it wills categorical larger attribute area than ever under an equivalent condition. We tend to conduct and implement comprehensive experiment for the projected theme. The simulation shows that CPWABE-RE theme is efficient each in terms of computation quality and storage price. Additionally, the protection of CP-WABE-RE theme is additionally established under the generic group model.

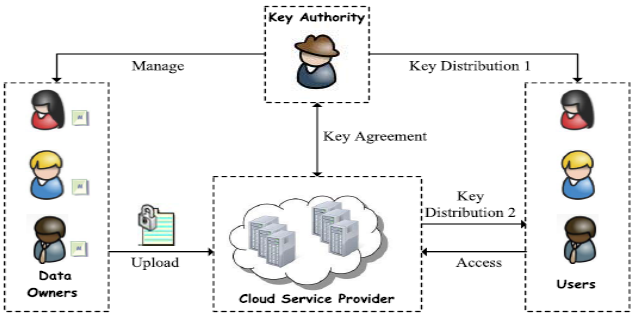


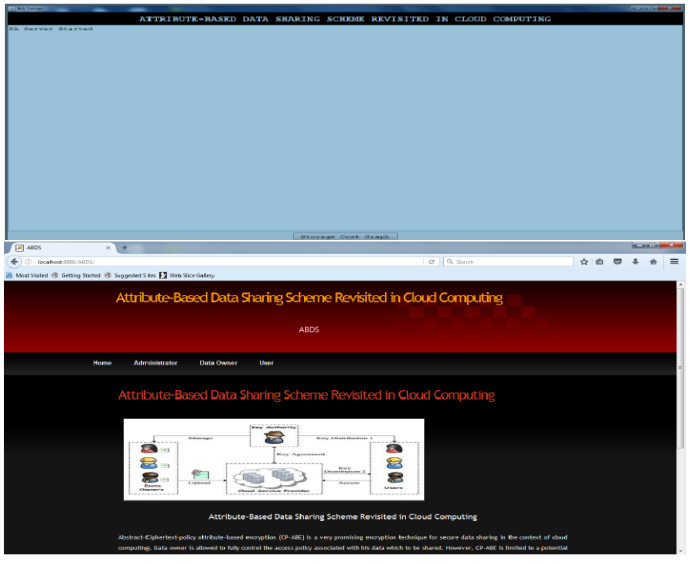
Figure 3: Architecture of CP-WABE-RE Scheme

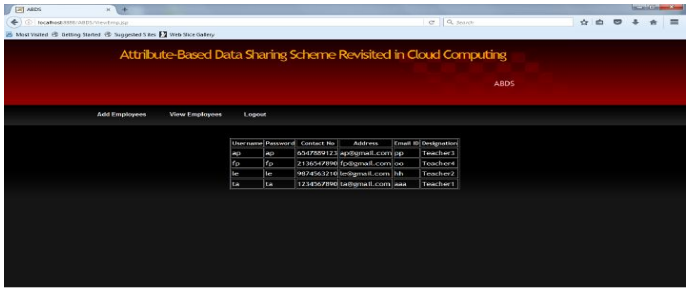
Key escrow and Weighted Attribute: the problem of key escrow, feature of weighted attribute and application in cloud computing for each scheme. The key escrow in CP-WABE-RE theme may be removed by using an improved key issuing protocol for cloud computing. Hur uses escrow-free key provision protocol to resolve the problem. On the contrary, each doesn't solve the problem of key escrow. Additionally, the weighted attribute in CP-WABE-RE theme cannot only support arbitrary-state attribute rather than the traditional binary state; however additionally simplify access policy related to a cipher-text as opposed. Unfortunately, will only express arbitrary-state attribute, and cannot alter the access structure. In, we are able to realize that only CP-WABE-RE theme can at the same time support all the three functions. Hur there for elves the matter of key escrow so it will satisfy surroundings of cloud system as ours however, each cannot remove key escrow therefore the each schemes cannot be directly applied in cloud computing.

IV. EXPERIMENTAL RESULTS

In our experiments, first we need the start the Key Authority server it is responsible for public and master

keys after that we can start the user application in that application we have three modules are there Admin, Data Owner and User Modules first we need to login as Admin module after successful login Admin can add and view the employees for example Admin adding an employees of type teaching assistant of weight 1, lecturer of weight 2 and assistant professor of weight 3 and professor of weight 4 after successfully adding the employees admin can also view the adding employees after that Login as a registered Data Owner here login as a employee of a type lecturer and his weight as 2 after that upload the file into server now the owner is sharing the data with Asst.Professor of weight 3, so this uploaded data will accessible for the users of weight >=3 In this application we are overcoming the key escrow problem by managing some keys at Key Authority and some at cloud server the data owner can delete the uploaded cloud files after that logged as a user, with any of the employee the user who is meeting with the given condition can look and download the files. Now we login as full professor of weight 4, they can be able to view and download the data as the owner has shared with users of weight >=3 user weight 3 the given weight could not able to access the cloud data after that authorized user logout into the system to shown in below screens





In the below chart we can observe that difference between the Normal Storage Cost and Propose Storage Cost

We can observe that Normal Storage Cost is higher than Propose Storage cost in the sense of Storage cost in Bytes based on that through our implementation 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. Therefore, both storage cost and encryption complexity for a cipher-text are relieved. The performance analysis and the security proof show that the proposed scheme is able to achieve efficient and secure data sharing in cloud computing at lower cost then compare to current methods.

V. CONCLUSION

In this paper, we tend to redesigned an attribute-based information sharing theme in cloud computing. The improved key issue protocol was presented to resolve the key escrow drawback. It enhances data confidentiality and privacy in cloud system against the managers of KA (Key Authority) and CSP (Cloud Service Provider) additionally as malicious system outsiders, wherever KA (Key Authority) and CSP (Cloud Service Provider) are semi-trusted. Additionally, the weighted attribute was planned to boost the expression of attribute, which might

not only describe arbitrary-state attributes, however additionally cut back the quality of access policy, so the storage price of cipher-text and time cost in encoding is saved. Finally, we tend to confer the performance and security analyses for the planned scheme, during which the results demonstrate high efficiency and security of our scheme. Though the parameter is downloaded with cipher-texts, it might be higher if its size is independent of the maximum number of cipher-text categories. On the opposite hand, once one carries the delegated keys around in a very mobile device without using special trusty hardware, the secret's prompt to leakage, designing a leakage-resilient cryptosystem however allows efficient and flexible key delegation is additionally an interesting direction.

REFERENCES

[1] X. Liu, J. Ma, J. Xiong, and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," *Int. J. Netw. Secur.*, vol. 16, no. 6, pp. 437–443, Nov. 2014.

[2] P. Morillo, C. Padró, G. Sáez, and J. L. Villar, "Weighted threshold secret sharing schemes," *Inf. Process. Lett.* vol. 70, no. 5, pp. 211–216, Jun. 1999.

[3] S. Müller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption," in *Proc. 11th Int. Conf. Inf. Secur. Cryptol.*, 2009, pp. 20–36.

[4] T. Paul, A. Famulari, and T. Strufe, "A survey on decentralized online social networks," *Comput. Netw.*, vol. 75, pp. 437–452, Dec. 2014.

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2005, pp. 457–473.

[6] J. T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *J. ACM*, vol. 27, no. 4, pp. 701–717, Oct. 1980.

[7] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013.

[8] B.Waters, "Ciphertext policy attribute based encryption: An expressive, efficient, and provably secure realization," in *Proc. 14th Int. Conf. Pract. Theory Public Key Cryptogr.*, 2011, pp. 53–70.

[9] F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, and P. Krause, "An efficient PHR service system supporting fuzzy keyword search and fine-grained access control," *Soft Comput.*, vol. 18, no. 9, pp 1795–1802, 2014.

[10] X. Xie, H. Ma, J. Li, and X. Chen, "An efficient cipher text-policy attribute-based access control towards revocation in cloud computing," *J. Universal Comput. Sci.*, vol. 19, no. 16, pp. 2349–2367, Oct. 2013.

[11] 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.

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

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

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

[15] S. S. M. Chow, "Removing escrow from identity-based encryption, in *Proc. 12th Int. Conf. Pract. Theory Public Key Cryptogr.*, 2009, pp. 256–276.