Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 9, September -2017

Survey on Secure Attribute-Based knowledge sharing theme Revisited on Cloud

[1]Shubham Lodha, [2]Yash Merchant

[1]BE, Student, MIT, Pune, Maharashtra, India
[2]BE, Student, MIT, Pune, Maharashtra, India

Abstract — *Attribute-based secret writing (ABE) has been wide utilized in cloud computing wherever an information supplier outsources his/her encrypted data to a cloud service supplie, and can share the info with users possessing specific credentials (or attributes). However, the standard ABE system doesn't support secure deduplication, which is crucial for eliminating duplicate copies of identical information so as to save lots of storage space and network information measure. during this paper, we tend to gift Associate in Nursing attribute-based storage system with secure deduplication in an exceedingly hybrid cloud setting, wherever a non-public cloud is to blame for duplicate detection and a public cloud manages the storage. Compared with the previous information deduplication systems, our system has 2 advantages. Firstly, it are often accustomed confidentially share information with users by specifying access policies instead of sharing decoding keys. Secondly, it achieves the standard notion of linguistics security for information confidentiality whereas existing systems solely reach it by shaping a weaker security notion. additionally, we put forth a technique to change a ciphertext over one access policy into cipher texts of an equivalent plaintext however below alternative access policies while not revealing the underlying plaintext.*

Keywords- Secure data sharing, Attribute-based encryption, Removing escrow, Weighted attribute, Cloud computing.

I. INTRODUCTION

Cloud computing has become an exploration hot-spot because of its distinguished long-list blessings (e.g. convenience, high scalability). one amongst the foremost promising cloud computing applications is on-line information sharing, like photograph sharing in On-line Social Networks among over one billion users and on-line health record system. an information owner (DO) is sometimes willing to store massive amounts of knowledge in cloud for saving the value on native data management. with none information protection mechanism, cloud service supplier (CSP), however, will totally gain access to all or any 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 information is one amongst the toughest challenges within the situation of cloud computing. Ciphertext-policy attribute-based cryptography (CP-ABE), has turned to be a very important cryptography technology to tackle the challenge of secure information sharing. in a very CP-ABE, user’s secret secret is delineate by associate attribute set, associated ciphertext is related to an access structure. DO is allowed to outline access structure over the universe of attributes. A user will rewrite a given ciphertext given that his/her attribute set matches the access structure over the ciphertext. using a CP-ABE system directly into a cloud application which will yield some open issues. Firstly, all users’ secret keys have to be compelled to be issued by a completely trusty key authority (KA). This brings a security risk that's called key written agreement downside. By knowing the key key of a system user, the Hindu deity will rewrite all the user’s ciphertexts, that stands in total against to the need of the user. Secondly, the quality of attribute set is another concern. As way as we all know, most of the present CP-ABE schemes will solely describe binary state over attribute, as an example, “1 - satisfying” and “0 - not-satisfying”, however not managing arbitrary-state attribute.

In this paper, the weighted attribute is defined to not only extend attribute expression from binary to capricious state, but in addition to vary access policy. Thus, the storage worth and secret writing worth for a ciphertext are going to be lessened.more illustrate our approach.

II. LITERATURE SURVEY

According to literature survey after studying different IEEE paper, collected some related papers and documents some of the point discussed here:

1. Improving Privacy and Security in Multi-Authority Attribute-Based Encryption
Author: Melissa Chase, Sherman S.M. Chow
Description: Multi-authority attribute-based encryption enables a more realistic deployment of attribute-based access control, such that different

authorities are responsible for issuing different sets of attributes. The original solution by Chase employs a trusted central authority and the use of a global identifier for each user, which means the confidentiality depends critically on the security of the central authority and the user-privacy depends on the honest behavior of the attribute-authorities. We propose an attribute-based encryption scheme without the trusted authority, and an anonymous key issuing protocol which works for both existing schemes and for our new construction.

2. Randomizable Proofs and Delegatable Anonymous Credentials
Authors: Mira Belenkiy, Jan Camenisch , Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham
Description: In this paper We revise the entire approach to constructing anonymous credentials and identify randomizable zero-knowledge proof of knowledge systems as the key building block. We formally define the notion of randomizable non-interactive zero-knowledge proofs, and give the first instance of controlled rerandomization of non-interactive zero-knowledge proofs by a third-party. Our construction uses Groth-Sahai proofs.

3. Removing Escrow from Identity-Based Encryption
Authors: Sherman S.M. Chow.
Description: In this paper we first show how to equip an IBE scheme by Gentry with ACI − KGC. Second, we propose a new system architecture with an anonymous private key generation protocol such that the KGC can issue a private key to an authenticated user without knowing the list of users identities. This also

better matches the practice that authentication should be done with the local registration authorities instead of the KGC. Our proposal can be viewed as mitigating the key escrow problem in a different dimension than distributed KGCs approach.

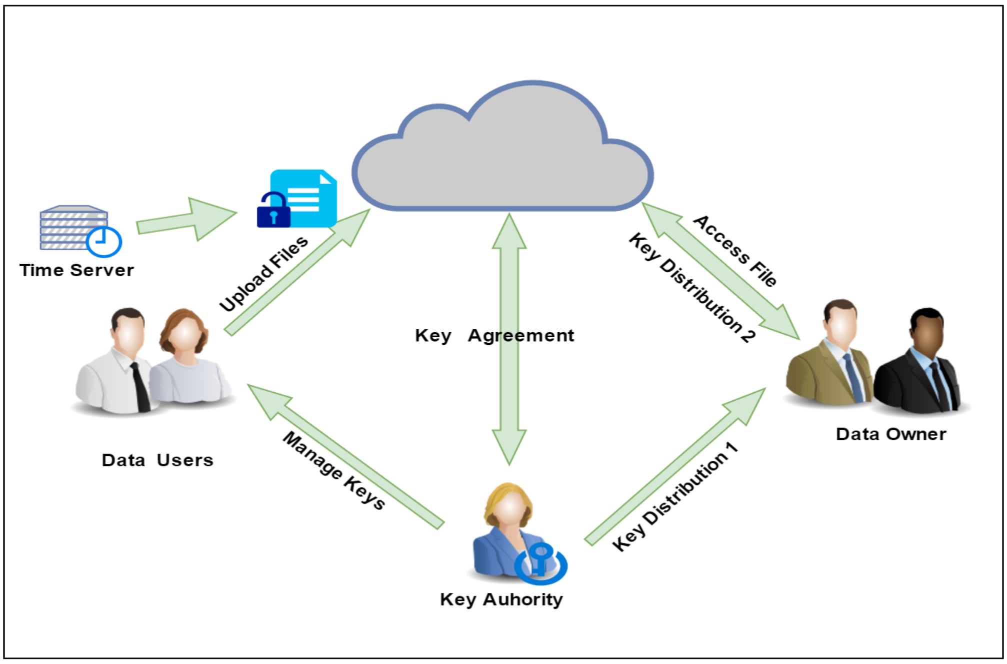
4. Arbitrary-State Attribute-Based Encryption with Dynamic Membership
Author: Chun-I Fan, Vincent Shi-Ming Huang, He-Ming Ruan
Description: In this paper, we proposed a ciphertext-policy attribute-based encryption scheme with dynamic membership. A user is allowed to enroll and leave from an ABE system, and she/ he can also change her/his attributes and the values corresponding to the attributes. It is unnecessary for anyone else to update her/his private key when enrollment, leaving, or attribute updating occurs. In addition, to the best of our knowledge, our scheme is the first ABE scheme which can support arbitrary-state attributes and attribute (and value) updating with Sender Updating Only. These advantages will make an ABE service more efficient and flexible for practical applications.

5. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data
Author: Vipul Goyal,Omkant Pandey, Amit Sahai, Brent Waters
Description: In this paper, we introduce new techniques to implement fine grained access control. In our techniques, the data is stored on the server in an encrypted form while different users are still allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access.

III. PROPOSED SYSTEM

We propose associate attribute-based data sharing theme for cloud computing applications, that's denoted as cipher text-policy weighted ABE theme with removing legal document (CP-WABE-RE). we tend to propose associate improved key issuing protocol to resolve the key legal document drawback of CP-ABE in cloud computing. The protocol can stop Hindu deity and CSP from knowing each other’s master secret key so as that none of them can manufacture the whole secret keys of users on a personal basis so, the wholly fiducially Hindu deity are going to be semi-trusted

IV. SYSTEM DESIGN



V. ADVANTAGES

- The problem of key escrow is solve by Cipher text policy-Weighted attribute base encryption Scheme as Complete key is not known to any of Key authority and cloud service provider.
- Time server makes it efficient to provide security over a file.
- Attribute are well decorated and so to know to user and easy access and security over files attribute

VI. CONCLUSION

In this paper, we tend to analyze totally different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, ABE with non-monotonic access structure, HABE and MA-ABE .The main access polices area unit KP-ABE and CP-ABE, further schemes area unit obtained supported these policies. Based on their variety of access structure the schemes area unit classified as either monotonic or non-monotonic. CHABE associate degree adaptation of Attribute based mostly cryptography (ABE) for the needs of providing guarantees towards the origin the sensitive data, and furthermore towards the namelessness of the info owner. Our theme conjointly allows dynamic modification of access policies o supports economical on-demand user/attribute revocation and break-glass access underneath emergency scenarios.

REFRENCES

[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 Transactions on Cloud Computing*, 3(2):233–244, 2015.

[2] A. Balu and K. Kuppusamy. An expressive and provably secure ciphertext-policy attribute-based encryption. *Information Sciences*, 276(4):354–362, 2014.

[3] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham. Randomizable proofs and delegatable anonymous credentials. *Proceedings of the 29th Annual International Cryptology Conference*, pages 108–125, 2009.

[4] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attributebased encryption. *IEEE Symposium on Security and Privacy*, pages 321–334, 2007.

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. *Journal of Cryptology*, 17(4):297–319, 2001.

[6] M. Chase. Multi-authority attribute based encryption. *Proceedings of the 4th Conference on Theory of Cryptography*, pages 515–534, 2007.

[7] M. Chase and S. S. Chow. Improving privacy and security in multiauthority attribute-based encryption. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pages 121–130, 2009.

[8] L. Cheung and C. Newport. Provably secure ciphertext policy ABE. *Proceedings of the 14th ACM conference on Computer and communications security*, pages 456–465, 2007.

[9] S. S. Chow. Removing escrow from identity-based encryption. *Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography*, pages 256–276, 2009.

[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 Computing*, 12(4):50–57, 2013.

[11] A. De Caro and V. Iovino. JPBC: java pairing based cryptography. *IEEE Symposium on Computers and Communications*, 22(3):850–855, 2011.

[12] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu, and W. Shi. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. *Information Sciences*, 275(11):370–384, 2014.

[13] C. Fan, S. Huang, and H. Rung. Arbitrary-state attribute-based encryption with dynamic membership. *IEEE Transactions on Computers*, 63(8):1951–1961, 2014.