ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

A Novel Attribute Based Data Sharing With Attribute Weights in Cloud Computing

[1] V.Geetha, [2] V.Sridhar Reddy
[1] PG Scholar, Dept of CSE, [2] Associate Professor, Dept of CSE
[1][2] VBIT College of engineering, Aushapur (v), Ghatkasar (m), Medchal Dist, Telangana, India

***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.**

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction . Cloud Computing has become a booming research area due to its long list advantages such as high scalability, convenience, cost saving, and disaster recovery. Cloud systems can be used to enable data sharing capabilities and this can provide an abundant of benefits to the user. There is currently a push for IT organizations to increase their data sharing efforts. According to a survey by InformationWeek, nearly all organizations shared their data somehow with 74 % sharing their data with customers and 64 % sharing with suppliers. A fourth of the surveyed organizations consider data sharing a top priority. The benefits organizations can gain from data sharing is higher productivity. The Cloud however is susceptible to many privacy and security attacks. The biggest obstacle hindering the progress and the wide adoption of the Cloud is the privacy and security issues associated with it. According to a survey carried out by IDC Enterprise Panel in August 2008, Cloud users regarded security as the top challenge with 75 % of surveyed users worried about their critical business and IT systems being vulnerable to attack. Many privacy and security attacks occur from within the Cloud provider themselves as they usually have direct access to stored data and steal the data to sell to third parties in order to gain profit. Some of major requirements of secure data sharing in the Cloud are as follows. Firstly the data owner should be able to specify a group of users that are allowed to view his or her data. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The data owner should be able to add new users to the group. The data owner should also be able to revoke access rights against any member of the group over his or her shared data. No member of the group should be allowed to revoke rights or join new users to the group. One trivial solution to achieving secure data sharing in the Cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information theoretically secure against the Cloud provider and other malicious users. When the data owner wants to share his data to a group, he sends the key used for data encryption to each member of the group. Any member of the group can then get the encrypted data from the Cloud and decrypt the data using the key and hence does not require the intervention of the data owner. However, the problem with this technique is that it is computationally inefficient and places too much burden on the data owner when considering factors such as user revocation. When the data owner revokes access rights to a member of the group, that member should not be able to gain access to the corresponding data. Since the member still has the data access key, the data owner has to re-encrypt the data with a new key, rendering the revoked member's key useless. When t he data is re - encrypted, he must distribute the new key to the remaining users in the group and this is computationally inefficient and places too much burden on the data owner when considering large group sizes that could be in excess of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

millions of users . Hence this solution is impractical to be deployed in the real - world for very critical data such as business, government and/or medical related data. Therefore, data security and privacy is most important concern in cloud computing. Cryptography in the cloud provides encryption techniques to secure data that will be used or stored in the cloud. It allows users too conveniently and securely access shared cloud services, as any data that is stored in cloud storage is protected with encryption. Cryptography techniques in the cloud computing protects sensitive data without delaying information exchange. In security enforcement of information system an access control is one of most common used approach. Access control is generally a policy that permits, rejects or confines access to the resources in a computing environment. It also monitor and record all attempts made to access a system. It is a mechanism which is very much important for protection in computer security. Accordingly, how to securely and efficiently share user data is one of the toughest challenges in the scenario of cloud computing. In this paper, we reviewed on Attribute - Based Encryption methods which have been developed so far for achieving secure data sharing in cloud computing.

2. LITERATURE SURVEY

L. Cheung and C. Newport explained In cipher text policy attribute-based encryption (CP-ABE), every secret key is associated with a set of attributes, and every cipher text is associated with an access structure on attributes. Decryption is enabled if and only if the user's attribute set satisfies the cipher text access structure. This provides fine-grained access control on shared data in many practical settings, including secure databases and secure mul- ticast. In this paper, we study CP-ABE schemes in which ac- cess structures are AND gates on positive and negative at- tributes. Our basic scheme is proven to be chosen plaintext (CPA) secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. We then apply the Canetti-Halevi- Katz technique to obtain a chosen ciphertext (CCA) secure extension using one-time signatures. The security proof is a reduction to the DBDH assumption and the strong existential unforgeability of the signature primitive. In addition, we introduce hierarchical attributes to optimize our basic scheme reducing both ciphertext size and encryption/decryption time while maintaining CPA security. Finally, we propose an extension in which access policies are arbitrary threshold trees, and we conclude with a discussion of practical applications of CP-ABE.

S. S. M. Chow studded Key escrow is inherent in identity-based encryption (IBE). A curious key generation center (KGC) can simply generate the user's private key to decrypt a ciphertext. However, can a KGC still decrypt if it does not know the intended recipient of the ciphertext? We answer by f ormalizing KGC anonymous ciphertext indistinguishability (ACI − KGC). We find that all existing pairing-based IBE schemes without random oracles, whether receipt-anonymous or not, do not achieve K GC one way ness, a weaker notion of ACI − KGC . In view of this, 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 a n authenticated user without knowing the list of users identities. This also better matches the practice that authentication should be d one 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.

H. Deng et al. explained Attribute-based encryption (ABE) systems allow encrypting to uncertain receivers by means of an access policy specifying the attributes that the in- tended receivers should possess. ABE promises to deliver fine-grained access control of encrypted data. However, when data are encrypted using an ABE scheme, key management is difficult if there is a large number of users from various backgrounds. In this paper, we elaborate ABE and propose a new versatile cryptosystem referred to as ciphertext-policy hierarchical ABE (CP-HABE). In a CP-HABE scheme, the attributes are organized in a matrix and the users having higher-level attributes can delegate their access rights to the users at a lower level. These features enable a CP-HABE system to host a large number of users from different organizations by delegating keys, e.g., enabling efficient data sharing among hierarchically organized large groups. We construct a CP-HABE scheme with short ciphertexts. The scheme is proven secure in the standard model under non-interactive assumptions.

Sahai et al. in 2005 introduced Fuzzy identity - based encryption (IBE) which is seminal work of attribute - based encryption. After that in 2006, they [4] first proposed t he attribute - based encryption. In ABE scheme both the secret user key and the ciphertext are associated with a set of attributes. A user can able to decrypt the ciphertext if and only if at least a threshold number of attributes matches associated with the cipher

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

text and user secret key. Different from traditional public key cryptography such as Identity - Based Encryption, ABE is implemented for one - to - many encryption in which cipher text is not necessarily encrypted to one particular user, it may be for more than one number of users. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system. ABE in which policies are specified and imposed in the encryption algorithm itself. The existing ABE schemes are of two types KP - ABE scheme and CP - ABE scheme.

V. Goyal et al.in 2006 introduced a KP - ABE scheme. It enables more general access control. It is the modified approach of a general model of ABE that has discussed earlier. Exploring KP - ABE scheme, attributes are associated with ciphertext and access policies related to secret keys of users. For decrypt the ciphertext, an access policy associated with user's secret key that is to be satisfied by the attributes associated with the ciphertext. KP - ABE scheme follows a public key encryption technique that is intended for one - to - many communications. For example, let us assume that the universe of attributes is defined as {A, B, C, D}. The ciphertext is computed using the set of attribute {A, B}. An access policy (A ∧ C) ∨ D is implanted into user's secret key. In this above example, the user would not be able to decrypt the ciphertext but would able to decrypt a ciphertext concerning attributes {A, C, D}.

J. Hur 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 mechanism where the key generation center and the data storage c enter work together to generate secret key for user. The protocol requires interactive computation between the both parties. So, the computational cost in generating user's secret key increases. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.

X. Xie et al. 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 of plaintext. 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 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 text of system users.

Fan et al. Proposed an arbitrary - state ABE to solve the issue of the dynamic membership management. This papers provides high flexibility of the constraints on attributes and makes users be able to dynamically join, leave, and update their attributes. 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

3. FRAMEWORK

3.1 SYSTEM MODEL 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.

Key Authority (KA): 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 (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.

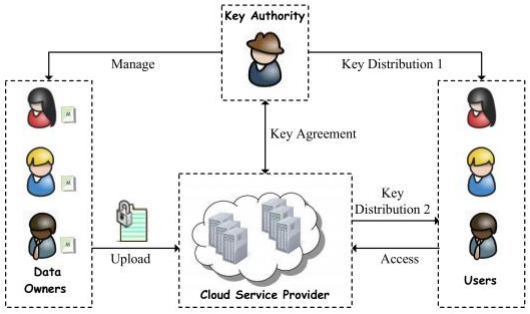


Fig 1:System model of CP-WABE-RE scheme in cloud computing.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

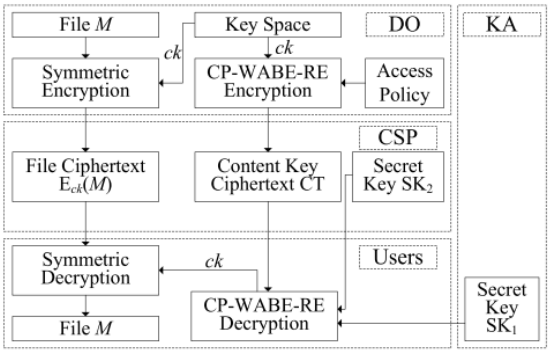
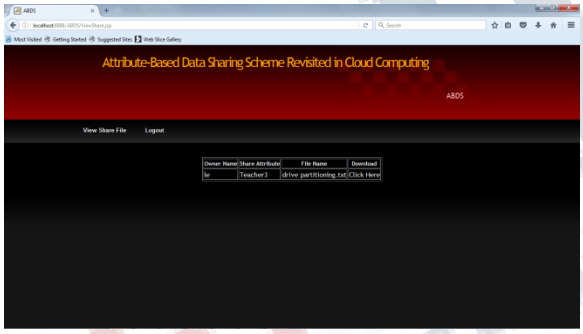


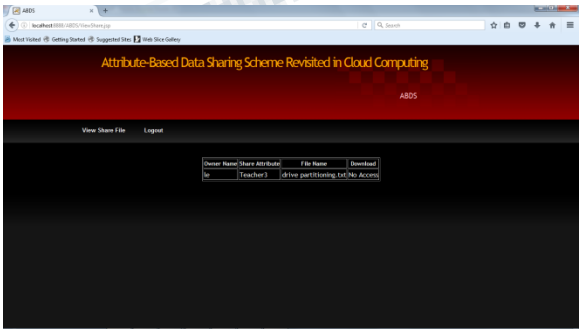
Fig 2:System framework of CP-WABE-RE scheme.

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 corresponding decryption operation.

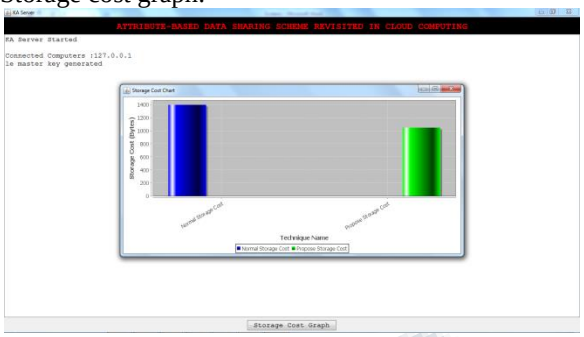
3. EXPERIMENTAL RESULTS



Less then the given weight could not able to access the cloud data:



Storage cost graph:



4. CONCLUSION

In this paper, we break down various property based encrypt ion plans: ABE, KP - ABE, CP - ABE, ABE with non - monotonic ge t to structure, HABE and MA - ABE . The fundamental get to polic i es are KP - ABE and CP - ABE, advance plans are acquired in light of these arrangements. In light of their kind of get to structure the plans are sorted as either monotonic or non - monotonic. CH - ABE an adjustment of Attribute Based Encryption (ABE)for the reaso ns for giving certifications towards the provenance the delicate information, and in addition towards the namelessness of the information proprietor; Our plan additionally empowers dynamic alteration of get to approaches o underpins proficient on - request c lient/property denial and break - glass access under crisis situations

5. 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.

[13] C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan, "Arbitrary-state attributebased encryption with dynamic membership," IEEE Trans. Comput., vol. 63, no. 8, pp. 1951–1961, Aug. 2014.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.

[15] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Oct. 2013.