Available online at: http://www.ijmtst.com/vol5issue03.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 05, Issue No: 03, March 2019

Acquisition of Secured Data from Cloud

P Sunitha Madhavi[1] | G Sai Venkata Akhil[2] | M Navya Tejaswi[3] | D Sai Jithin[4]

[1]Assistant Professor, Department of Computer Science and Engineering, Dhanekula Institute of Engineering and Technology, Andhra Pradesh, India.
[2,3,4]Department of Computer Science and Engineering, Dhanekula Institute of Engineering and Technology, Andhra Pradesh, India.

To Cite this Article
P Sunitha Madhavi, G Sai Venkata Akhil, M Navya Tejaswi and D Sai Jithin, "Acquisition of Secured Data from Cloud", *International Journal for Modern Trends in Science and Technology*, Vol. 05, Issue 03, March 2019, pp.-13-16.

Article Info
Received on 18-Feb-2019, Revised on 19-March-2019, Accepted on 26-March-2019.

ABSTRACT

Data get to control is a powerful method to guarantee the data security in the cloud. Because of information out sourcing and un confided in cloud servers, the information get to control turns into a testing issue in cloud storage systems. Cipher text-Policy Attribute Based Encryption (CP-ABE) is viewed as a standout amongst the most reasonable advancements for information get to control in distributed storage, since it gives straightforward control access to the owners. It is hard to implement the existing CP-ABE schemes to access the information from cloud storage systems. we propose a plan to structure the information securing control in a revocable multi-expert CP-ABE conspire from cloud storage system.

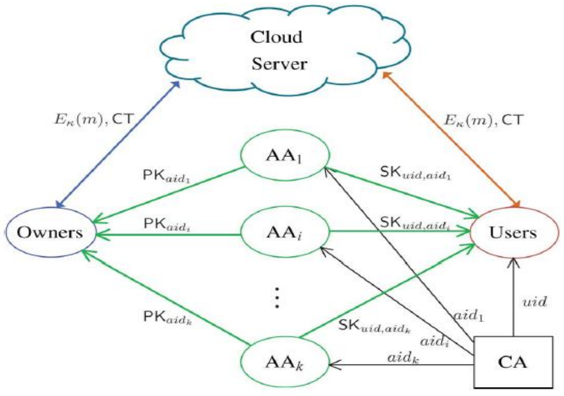
I. Introduction

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and un trusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Cipher text-Policy Attribute based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. In this project, we first propose a revocable multi authority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system. Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new cipher text that requires the revoked attribute to decrypt)and forward security (The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient attributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi trusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

II. PROPOSED METHOD

In this paper, In the existing system the Ciphertext-Policy Attribute-based Encryption (CP-ABE) algorithm is one of the most suitable technologies for data access control in cloud storage systems .In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution.Revocable multi authority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system and is secure in the sense that it can achieve both backward and forward security. We apply this multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.



III. RELATED WORK

Introduced the attribute basedencryption (ABE) for enforced access control through publickey cryptography. The main goal for these models is to provide security and access control. The main aspects are toprovide flexibility, scalability and fine grained access control.In classical model, this can be achieved only when user andserver are in a trusted domain. But what if their domains arenot trusted or not same? So, the new access control schemethat is 'Attribute Based Encryption (ABE)' scheme wasintroduced which consist of key policy attribute basedencryption (KP-ABE). As compared with classical model,KP-ABE provided fine grained access control. However itfails with respect to flexibility and scalability when authoritiesat multiple levels are considered.

In ABE scheme both the user secret key and the ciphertextare associated with a set of attributes. A user is able todecrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher-text and usersecret key. Different from traditional public key cryptographysuch as Identity-Based Encryption, ABE is implemented for one-to many encryption in which cipher-texts are 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. Attribute-Based Encryption (ABE) in which policies are specified and enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CPABE) scheme.

Key Policy Attribute Based Encryption(KP-ABE):-

To enable more general access control, *V. Goyal, O.Pandey, A. Sahai, and B. Waters* proposed a key-policyattribute-based encryption (KP-ABE) scheme. It is themodified form of classical model of ABE. Exploring KP-ABEscheme, attribute policies are associated with keys and data isassociated with attributes. The keys only associated with thepolicy that is to be satisfied by the attributes that areassociating the data can decrypt the data. Key Policy AttributeBased Encryption (KP-ABE) scheme is a public keyencryption technique that is designed for one-to-manycommunications. In this scheme, data is associated with theattributes for which a public key is defined for eachEncrypter, that is who encrypts the data, is associated with theset of attributes to the data or message by encrypting it with apublic key. Users are assigned with an access tree structureover the data attributes. The nodes of the access tree are thethreshold gates. The leaf nodes are associated with attributes.

The secret key of the user is defined to reflect the access treestructure. Hence, the user is able to decrypt the message thatis a ciphertext if and only if the data attributes satisfy theaccess tree structure. In KP-ABE, a set of attributes isassociated with ciphertext and the user's decryption key isassociated with a monotonic *access tree structure*. Whenthe attributes associated with the cipher text satisfy the access tree structure, then the user can decrypt the ciphertext.

IV. LITERATURE SURVEY

1"Multi-Authority Attribute Based Encryption,"

AUTHORS: M. Chase

an identity based encryption scheme, each user is identified by a unique identity string. An attribute based encryption scheme (ABE), in contrast, is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each cipher text. Sahai and Waters introduced a single authority attribute encryption scheme and left open the question of whether a scheme could be constructed in which multiple authorities were allowed to distribute attributes [SW05]. We answer this question in the affirmative.Our scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k. Our scheme can tolerate an arbitrary number of corrupt authorities. We also show how to apply our techniques to achieve a multiauthority version of the large universe fine grained access control ABE presented by Gopal et al.

2.**"Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,"**

AUTHORS:M. Chase and S.S.M. Chow

Attribute based encryption (ABE) [13] 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 users and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase [5] gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every cipher text, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. Moreover, 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 paper, we propose 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.

3.**"Decentralizing Attribute-Based Encryption,"**

AUTHORS: A.B. Lewko and B. Waters

We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority.

In constructing our system, our largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. However, in our system each component will come from a potentially different authority, where we assume no coordination between such authorities. We create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers. We prove our system secure using the recent dual system encryption methodology where the security proof works by first converting the challenge cipher text and private keys to a semi-functional form and then arguing security. We follow a recent variant of the dual system proof technique due to Lewko and Waters and build our system using bilinear groups of Composite order. We prove security under similar static assumptions to the LW paper in the random oracle model.

V. CONCLUSION

In this paper Cloud computing brings great convenience for people. In this project, we build a cost-effective and secure datasharing system in cloud computing, we propose a revocable multi-authority CPABE scheme that can supportefficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authoritycloud storage systems. We also proved that our scheme was provable secure in the random oracle model. Therevocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systemsand online social networks etc.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of CloudComputing," National Institute of Standards and Technology,Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-PolicyAttribute-Based Encryption," in Proc. IEEE Symp. Security andprivacy (S&P'07), 2007, pp. 321-334.

[3] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: AnExpressive, Efficient, and Provably Secure Realization," in Proc.4th Int'l Conf. Practice and Theory in Public Key Cryptography(PKC'11), 2011, pp. 53-70.

[4] V. Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded CiphertextPolicy Attribute Based Encryption," in Proc. 35th Int'l Colloquiumon Automata, Languages, and Programming (ICALP'08), 2008,pp. 579-591.

[5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters,"Fully Secure Functional Encryption: Attribute-Based Encryptionand (Hierarchical) Inner Product Encryption," in Proc.Advances in Cryptology-EUROCRYPT'10, 2010, pp. 62-91.

[6] M. Chase, "Multi-Authority Attribute Based Encryption," inProc. 4th Theory of Cryptography Conf. Theory of Cryptography(TCC'07), 2007, pp. 515-534.

[7] M. Chase and S.S.M. Chow, "Improving Privacy and Securityin Multi-Authority Attribute-Based Encryption," in Proc. 16thACM Conf. Computer and Comm. Security (CCS'09), 2009,pp. 121-130.

[8] A.B. Lewko and B. Waters, "Decentralizing Attribute-BasedEncryption," in Proc. Advances in Cryptology-EUROCRYPT'11,2011, pp. 568-588.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based DataSharing with Attribute Revocation," in Proc. 5th ACM Symp.Information, Computer and Comm. Security (ASIACCS'10), 2010,pp. 261-270.

[10] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, "Scalable and SecureSharing of Personal Health Records in Cloud Computing UsingAttribute-Based Encryption," IEEE Trans. Parallel DistributedSystems, vol. 24, no. 1, pp. 131-143, Jan. 2013.