ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

A Survey on Ciphertext-Policy Attribute based Encryption and Time Specified Approach.

Yugandhara L. Rothe, Prof. Vijay Gadicha, Prof.Y B Jadhao.

M.E Student, Dept. of Computer Engineering, Padm .Dr VB Kolte College of Engineering and Technology, Malkapur, Buldhana (M.S.), India

Asst. Professor, Dept. of Computer Science and Engineering, P.R.Pote College of Engineering and Management, Amravati, India

Asst. Professor, Dept. of Computer Science and Engineering, Padm.Dr VB Kolte College of Engineering and Technology, Malkapur, Buldhana (M.S.), India

ABSTRACT: The secure data sharing in cloud cipher text policy attribute based encryption is promising because data owner having full control over access policy of shared data. But CP-ABE having a key escrow problem whereby the secret keys of users have to be issued by a trusted key authority. CP-ABE schemes cannot support attribute with arbitrary state. So we revisit attribute-based data sharing to solve the key escrow issue but also improve the expressiveness of attribute, so that the resulting scheme is more-friendly to cloud computing applications. We propose an improved two-party key issuing protocol that can Guarantee that neither key authority nor cloud service provider can compromise the whole secret key of a user individually also we check deduplication of file uploading on cloud If file is duplicate then proof of ownership is provided to that user.

KEYWORDS: Secure data sharing, Attribute-based encryption, Removing escrow, Weighted attribute, Cloud computing, Time Server, Deduplication

.

I. INTRODUCTION

In cipher text attribute base encryption scheme (CP-ABE) is a secure encryption technique use in cloud computing. In this scheme Data owner has full authority to assign all access permission .But In recent scenario data user are increase, so with the increasing number of cloud users there is a risk of users secret key will be escrow. Key of data owner will be manage or escrow because the key authority or cloud service provider both are not trusted. So to manage key of data owners and implement attribute with arbitrary state. So we propose a scheme with two party key issuing mechanisms with weighted attribute. Therefore both storage cost and encryption complexity for ciphertext are solve. 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. We use the following example to further illustrate our approach.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. We also provide deduplication check over files which are uploading on cloud by data owner to avoid duplicate file storage on cloud and also to save storage space require in cloud. A of ownership is provided to new user who uploads file on cloud and which is duplicate..

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

II. LITRATURE SURVEY

In Improving Privacy and Security in Multi-Authority Attribute-Based Encryption it is unrealistic to assume there is a single authority which can monitor every single attribute of all users[1]. 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[1].A system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption[5].

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[2].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].It is possible to design a challenge-response protocol which imposes a strong incentive onto the cloud providers to store their clients' data at rest[8].

In this Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage propose a novel server-side deduplication scheme for encrypted data[4]. It allows the cloud server to control access to outsourced data even when the ownership changes dynamically by exploiting randomized convergent encryption and secure ownership group key distribution. This prevents data leakage not only to revoked users even though they previously owned that data, but also to an honest-but-curious cloud storage server.we proposed a ciphertext-policy attribute-based encryption scheme with dynamic membership[9].

In this, Randomizable Proofs and Delegatable Anonymous Credentials revise the entire approach to constructing anonymous credentials and identify randomizable zero-knowledge proof of knowledge systems as the key building block[3].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[3].The 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[11].

Our construction uses Groth-Sahai proofs.In this paper, we propose a novel server-side deduplication scheme for encrypted data. It allows the cloud server to control access to outsourced data even when the ownership changes dynamically by exploiting randomized convergent encryption and secure ownership group key distribution[4].

In this paper, we proposed a ciphertext-policy attribute-based encryption scheme with dynamic membership[6].In this paper, we proposed a ciphertext-policy attribute-based encryption scheme with dynamic membership[7].A novel ciphertext policy attribute-based proxy reencryption scheme which is based on AND-gates policy supporting multi-value attributes, negative attributes and wildcards[10].In this mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE) which extends CP-ABE with instantaneous attribute revocation. Furthermore, we demonstrate how to apply the proposed mCP-ABE scheme to securely manage Personal Health Records (PHRs)[12].

III. EXISTING SYSTEM

In Cipher text policy attribute base encryption scheme provides an efficient scheme for encrypting files and assign attribute access policy to file while uploading file on cloud but this cause problem while uploading files with attribute access policy its attributes are not fully encrypted while uploading only its name is encrypted but value of attributes remain unencrypted. If unauthorized user gets this value then he may get file and access that file so security concern arises. Also data owner having more direct control on access policy and it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

In this scheme file is upload on cloud without entering any keywords of file. File upload on cloud only with attribute access policy for access of file. While cloud consumer want to download file from cloud then consumer enter only attributes and user get resulted file with that file. This resulted file contains many files matching to attributes but this is not exact matching result. Also this file are once upload remain for long time on cloud, this cause wastage of space on cloud and cloud consumers get this file as a result each and every time and this file is of no use after long time. File uploading on cloud are in encrypted format so many difficulty occur searching over an encrypted data. The cloud server is not fully trusted authority, if users sensitive data or files remain for long time on cloud then file are not secure.

III. PROPOSED SYSTEM

We propose associate attribute-based knowledge sharing theme for cloud computing applications, that is denoted as cipher text-policy weighted ABE theme with removing written agreement (CP-WABE-RE). we tend to propose associate improved key issuance protocol to resolve the key written agreement downside of CP-ABE in cloud computing. The protocol will stop KA and CSP from knowing every other's master secret key in order that none of them will produce the total secret keys of users on an individual basis therefore, the totally trusty KA will be semi-trusted. Knowledge confidentiality and privacy will be ensured. we tend to gift weighted attribute to boost the expression of attribute. The weighted attribute cannot solely specific arbitrary-state attribute (instead of the normal binary state), however conjointly cut back the quality of access policy. There fore the storage price of cipher text and computation quality in coding will be reduced. Besides, it will specific larger attribute house than ever beneath constant condition. We also provide deduplication check over files which is uploading on cloud by data owner to avoid duplicate file storage on cloud and also to save storage space require in cloud. A of ownership is provided to new user who uploads file on cloud and which is duplicate. We tend to conduct and implement comprehensive experiment for the planned theme. The simulation shows that CP-WABE-RE theme is economical each in terms of computation quality and storage price. Additionally, the safety of CP-WABE-RE theme is additionally established beneath the generic cluster model. Time server is introducing for distribution a time interval with file at time ofat time of uploading. Thus this file is accessible to user just for time such that by time server.

We conjointly give deduplication check out files that square measure uploading on cloud by information owner to avoid duplicate file storage on cloud and conjointly to avoid wasting space for storing need in cloud. A of possession is provided to new user World Health Organization uploads file on cloud and that is duplicate. uploading. Thus this file is accessible to user just for time such that by time server.

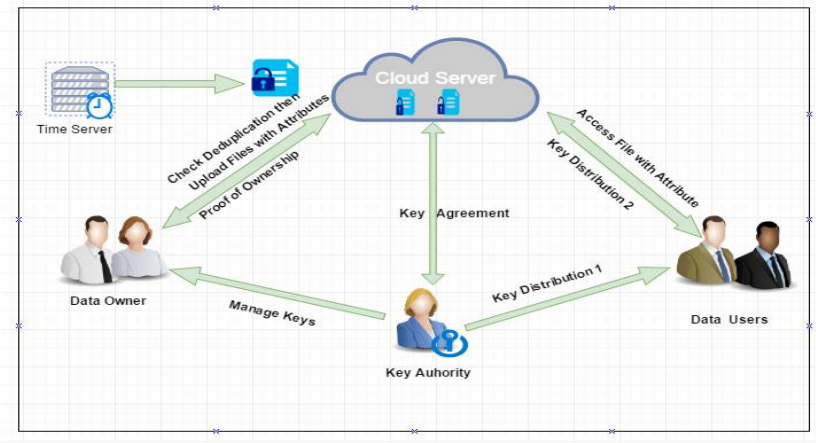

Figure 1. System Architecture of CP-ABE and time Specified Approach

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

IV. ADVANTAGES OF PROPOSED SYSTEM

1. 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.
2. Time server makes it efficient to provide security over a file.
3. Attribute are well decorated and so to know to user and easy access and security over files attribute
4. Storage space is save as duplicate files cannot be store on cloud.

V. ALGORITHM

AES Algorithm

- ✓ The AES-256 algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion. Cipher converts data to an unintelligible form called cipher text while Inverse Cipher converts data back into its original form called plaintext. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedure. Cipher and Inverse Cipher are composed of specific number of rounds For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations:
- ✓ 1) Byte substitution using a substitution table (S-box)
- ✓ 2) Shifting rows of the State array by different offsets
- ✓ 3) Mixing the data within each column of the State array
- ✓ 4) Adding a Round Key to the State
- ✓ The Cipher transformations can be inverted and then implemented in reverse order to produce a straightforward Inverse Cipher for the AES algorithm. The individual transformations used in the Inverse Cipher.
- ✓ 1) Inverse Shift Rows
- ✓ 2) Inverse Sub Bytes
- ✓ 3) Inverse Mix Columns
- ✓ 4) Add Round Key
- ✓ The AES inverse cipher core consists of a key expansion module, a key reversal buffer, an initial permutation module, a round permutation module and a final permutation module. The key reversal buffer first store keys for all rounds and the presents them in reverse order to the rounds. The round permutation module will loop maternally to perform 14 iterations (for 256 bit keys).

MD5 Algorithm:

MD5 algorithm takes input message of arbitrary length and generates 128-bit long output hash. MD5 hash algorithm consist of 5 steps:

- Step 1. Append Padding Bits
- Step 2. Append Length
- Step 3. Initialize MD Buffer
- Step 4. Process Message in 16-Word Blocks
- Step 5. Output

VI. CONCLUSION

In this Ciphertext-policy attribute based encryption and time specified approach project we slove key escrow problem.Also gives security over files attribute.And time server to provide efficient security over file attribute.Storage space is save as duplicate files cannot be store on cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFERENCES

[1] A. Balu and K. Kuppusamy. "An expressive and provably secure ciphertext-policy attribute-based encryption."Information Sciences, 276(4):354–362, 2014.
[2] 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.
[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]Junbeom Hur, Dongyoung Koo, "Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage,"IEEE Transactions on Knowledge and Data Engineering DOI 10.1109/TKDE.2016.2580139,
[5] J. Bethencourt, A. Sahai, and B. "Waters. Ciphertext-policy attribute based encryption,"IEEE Symposium on Security and Privacy, pages 321–334, 2007.
[6] C. Fan, S. Huang, and H. Rung. Arbitrary-state attribute-based encryption with dynamic membership. *IEEE* Transactions on Computers, 63(8):1951–1961, 2014.
[7] Vipul Goyal,Omkant Pandey, Amit Sahai, Brent Waters, **"**Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," ACM 1-59593-518-5/06/0010
[8] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. K. Liu. Towards secure and reliable cloud storage against data re-outsourcing. *Future Generation Computer Systems*, 52:86–94, 2015.
[9] C. Fan, S. Huang, and H. Rung. Arbitrary-state attribute-based encryption with dynamic membership. *IEEE Transactions on Computers*, 63(8):1951–1961, 2014.
[10] Song Luo, Jianbin Hu, and Zhong Chen, "Ciphertext Policy Attribute-Based Proxy Re-encryption",DOI 10.1007/978-3-642-17650-0_28.
[11] Sherman S.M. Chow. "Removing Escrow from Identity-Based Encryption," NCS 5443, pp. 256–276, 2009
[12] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker. Mediated ciphertext-policy attribute-based encryption and its application. Proceedings of the 10th International Workshop on Information Security Applications, pages 309–323, 2009.