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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

An Auditing-Free Cloud Storage Using Control Attribute Based Encryption

Dr.T. Ramaprabha[1], S. Priya[2]

Professor, Department of Computer Science &Applications, Vivekanandha College of Arts and Sciences for Women, Elayampalayam, India[1]

M. Phil Full Time Research Scholar, Dept. of Computer Science, Vivekanandha College of Arts and Sciences for Women, Elayampalayam, India[2]

ABSTRACT: Cloud storage services have grow popularly. For the importance reason of privacy, many cloud storage encryption schemas has been proposed to secure the data from those who do not have access. All such schemes assumes that cloud storage providers are secure and cannot be hacked. However in practice, some authorities may compel cloud storage providers to make public user secrets and confidential data. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage provider ensure that user privacy is still securely protected.

KEYWORDS: Cloud computing, Deniable Encryption, Attribute Based Encryption, Data security and Privacy.

I. INTRODUCTION

Cloud storage services have rapidly become increasinglypopular. Users can store their data on the cloud and accesstheir data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are numerous ABE schemes that have been proposed,hiding platform and implementation details unlimited virtualized resources provided to the users as a service is a cloud computing. Presently cloud service provided to the users offered high available storage and massively parallel computing of resources at relatively low costs. But the question is about the cloud users with different privileges store data on cloud is a most challenge issue in managing cloud data storage system. Most important problem for cloud environment is privileges.

II.PROBLEM STATEMENT

The problem is to determine, public auditing for suchshared data while preserving identity privacy remains to be an open challenge. Unique problem introduced during the process of public auditing for shared data in the cloud I how to preserve identity privacy from the TPA(Third Party Auditor).

III.RELATED WORK

The concept of ABE(Attribute-Based Encryption) in which data owners can insert how they want to distribute data in terms of encryption. That is, only those who match the owner’s conditions can successfully decrypt stored data. We can say here that ABE is encryption for privileges, not for users. This makes ABE a very helpful tool for cloud storage services since data sharing is a significant feature for such services. Cloud storage users are not practical for data owners to encrypt their data by pair wise keys. Furthermore, it is also impractical to encrypt data many times for many people. With ABE, data owners make a decision only which kind of users can access their encrypted data. Users who convince the conditions are able to decrypt the encrypted data. The scheme of deniable encryption is nothing but it also

DOI: 10.15680/IJIRCCE.2016.0407141

similar to common encryption schemes, deniable encryption can be separated into a deniable shared key scheme and a public key scheme. Allowing the cloud storage scenario, we focus our efforts on the deniable public key encryption scheme. The simulatable public key system provides an unaware key generation function and an oblivious cipher text function. When transferring an encrypted bit, the sender will send a set of encrypted data which may be usually encrypted or insensible. Therefore, the dispatcher can claim some sent messages are oblivious while actually they are not. The scheme can be applied to the receiver side such that the scheme is a bi-deniable scheme. While performing this scheme there are some disadvantages may arise. Those are Computational overhead. I.e. Encryptionparameters should be totally different for each encryption operation. So each coercion will reduce flexibility. We can also face Decrypted data with missing of contents at such blocks. Entities of the cloud environment may stop communications between users and cloud storage providers and then require storage providers to release user secrets by using power or other means. In this situation, encrypted data are assumed to be known and storage providers are requested to discharge user secrets here another disadvantage is Data redundancy is Occur at each block of data. The non interactive and fully receiver deniable schemes cannot be achieved simultaneously. It is also impossible to encrypt unbounded messages, using one short key in non committing schemes. The future performance scheme with Cipher Text Policy Attribute Based encryption presents a cloud storage provider which means to make fake user secrets. Specified such fake user secrets, outside coercers can only obtained fake data from a user's stored cipher text. The coercers think the received secrets are real, they will be content and more prominently cloud storage providers will not have revealed any real secrets. So, user privacy is still confined in cloud computing environment[7].

IV.EXISTING SYSTEM

- ➢ There are numerous ABE schemes that have been proposed. Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets.
- ➢ Sahai and Waters first introduced the concept of ABE in which data owners can embed how they want to share data in terms of encryption.
- ➢ There are two types of ABE, CP-ABE and Key-Policy ABE (KP-ABE).Goyal et al. proposed the first KPABE. They constructed an expressive way to relate any monotonic formula as the policy for user secretkeys. Bethen court et al. proposed the first CP-ABE.This scheme used a tree access structure to express any monotonic formula over attributes as the policy in the ciphertext.
- ➢ It is also impractical to encrypt data many times for many people. With ABE, data owners decide only which kind of users can access their encrypted data. Users who satisfy the conditions are able to decrypt the encrypted data.
- ➢ Use translucent sets table public key systems to implement deniability.
- ➢ Most deniable public key schemes are bitwise, which means these schemes can only process one bit a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in the cloud storage service case.
- ➢ Most of the previous deniable encryption schemes are inter-encryption independent. That is, the encryption parameters should be totally different for each encryption operation. If two deniable encryptions are performed in the same environment, the latter encryption will lose deniability after the first encryption is coerced, because each coercion will reduce flexibility.
- ➢ Most deniable encryption schemes have decryption error problems. These errors come from the designed decryption mechanisms.

V. PROPOSED SYSTEM

- ➢ In this work, It is describing a deniable ABE scheme for cloud storage services. By make use of ABE characteristics for securing stored data with a finegrained access control mechanism and deniable encryption to prevent outside auditing. This scheme is based on Waters ciphertext policy-attribute based encryption (CP-ABE) scheme. This enhance the Waters scheme from prime order bilinear groups to composite order bilinear groups. By the subgroup decision problem assumption, this scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers.

- In this work, constructing a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In this scenario, cloud storage service providers are just regarded as receivers in other deniable schemes.
- Unlike most previous deniable encryption schemes, it is not using translucent sets table public key systems to implement deniability. Instead, this adopt the ideaproposed with some improvements. This constructdeniable encryption scheme through a multidimensional space. All data are encrypted into the multidimensional space.
- Only with the correct composition of dimensions is the original data obtainable. With false composition, cipher texts will be decrypted to predetermined fake data. The information defining the dimensions is kept secret. This make use of composite order bilinear groups to construct the multidimensional space. This also use chameleon hash functions to make both true and fake messages convincing.
- In this work, there is a consistent environment for deniable encryption scheme. By consistent environment, means that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look convincing for all cipher texts under this environment, regardless of whether a cipher text is normally encrypted or deniably encrypted. The deniability of this scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, can construct the released fake key to decrypt normal cipher texts correctly.

VI. ALGORITHMS USED

The planned scheme consists of four algorithms which is defined as follows: Setup (1) -> (PP,MSK):This algorithm takes security parameter as input and returns public parameter as PP and system master key MSK. KeyGen(MSK,S) →SK : Given set of attributes S and MSK. This algorithm outputs private key SK. Enc(PP,M,A) →C :This encryption algorithm takes as input public parameter PP, message M and LSSS access structure A=(M,) over the universe of attributes, This algorithm encrypts M and outputs a cipher text C, which can be decrypted by those who possess an attribute set that satisfies access structure A. Note A is contained in C. Verify(PP,C,M, PE, PD) → {T, F}: This algorithm is used to verify the correctness of PE and PD OpenEnc(PP,C,M) → PE: This algorithm is for the sender to release encryption proof PE for (M,C).OpenDec(PP, SK,C,M) → PD: This algorithm is for the receiver to release decryption proof PD for (M,C). Dec(PP, SK,C) → {M,⊥}: This decryption algorithm takes as input public parameter PP, private key SK with its attribute set S, and ciphertext C with its access structure A. If S satisfies A, then this algorithm returns M.

VII.CONCLUSION

A deniable CP-ABE scheme is an audit-free cloud storage service. The deniability feature makes force invalid, and the Attribute Based Encryption belongings guarantee secure cloud data sharing with a fine-grained access control method. This scheme presents a likely way to struggle next to dissipated intervention with the right of privacy. Not only the above can this scheme be formed to guard cloud user privacy with high computational performance. It can be conclude this paper deals with how to securely audit public data and how to put security public data when share data. How to provide security base on attribute schema.

REFERENCES

[1] A. Sahai and B. Waters, “Fuzzy identity based encryption,” in Eurocrypt, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[4] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography, 2011, pp. 53–70.

[5] A. Sahai, H. Seyalioglu, and B. Waters, “Dynamic credentials and ciphertext delegation for attribute-based encryption,” in Crypto, 2012, pp. 199–217.

[6] S. Hohenberger and B. Waters, “Attribute-based encryption with fast decryption,” in Public Key Cryptography, 2013, pp. 162–179.

[7] P. K. Tysowski and M. A. Hasan, “Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds.” IEEE T. Cloud Computing, pp. 172–186, 2013.
[8] Wired. (2014) Spam suspect uses Google docs; fbi happy. [Online]. Available: http://www.wired.com/2010/04/cloud-warrant/
[9] Wikipedia. (2014) Global surveillance disclosures (2013present). [Online]. Available: http://en.wikipedia.org/wiki/Global surveillance disclosures (2013-present)
[10] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Eurocrypt, 2005, pp. 457–473.
[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.
[12] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.
[13] B.Waters,“Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography, 2011, pp. 53–70.
[14] A. Sahai, H. Seyalioglu, and B. Waters, “Dynamic credentials and ciphertext delegation for attribute-based encryption,” in Crypto, 2012, pp. 199–217.
[15] S. Hohenberger and B. Waters, “Attribute-based encryption with fast decryption,” in Public Key Cryptography, 2013, pp. 162–179.
[16] K. Liang, L. Fang, D. S. Wong, and W. Susilo, “A ciphertext policy attribute-based proxy re-encryption with chosen-ciphertext security,” IACR Cryptology ePrint Archive, vol. 2013, p. 236, 2013.