International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-4,April 2016
ISSN: 2395-3470
www.ijseas.com

FINDING ANONYMITY USERS FOR SECURE CLOUD STORAGE

S.Saranya [1], S.Shanthapriya2, M.Kalaivani[3]

Department of Computer science Engineering

Dhanalakshmi College of Engineering

Abstract— Many cloud storage encryption schemes have been introduced to protect data from those who do not have access. We make use of many schemes which assumed that cloud storage providers are safe and secure. But in practice, some authorities (i.e., coercers) may try to reveal data from the cloud without the permission of the data owner. In this paper, we present that the detection of anonymity users with the use of our efficient deniable encryption scheme, while the fake users tries to get data from the cloud they will be provided with some fake files. So that hackers cannot hack the files from the cloud. And they are satisfied with their duplicate file by that way we can protect the owner secret files or confidential files.

Index Terms *Cloud storage provider, coercers, Deniable ABE Schemes, Secret key, Audit-free cloud, fake user.*

I.INTRODUCTION

In cloud, data owner can store their data and access their data anywhere at any time from the cloud. The main aim of this paper is to protect data from the outside hackers. Our proposed scheme is used not only for the protection which is also to convincing the hackers by the fake files and who cannot find whether the accessed file is true or not. Some of the proposed schemes assume storage providers in cloud are safe and cannot be hacked; however, in practice, Some coercers may intercept communications between the data owner and the storage provider and force, storage provider to release owner's secrets or confidential data by using some government power in cloud.

In such case, the storage providers are requested to reveal user secrets. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness in the previous schemes. But In our scheme, storage providers can fight against such coercers to maintain the user privacy. Therefore, user privacy is still protected.

II. EXISTING WORK

There are number of ABE schemes that have been proposed. Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management by key distributor are trusted. Some entities may intercept communication between users and cloud storage provider. Then compel storage providers to release user secrets by using 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 access 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 efficient way to relate any monotonic formula as the policy for user secret keys. Bettencourt et al. proposed the first Ciphertext-Policy ABE (CP-ABE). This scheme used a tree access structure to express any monotonic formula over attributes as the policy in the cipher text.

DISADVANTAGES OF EXISTING SYSTEM

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 or simulatable 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.

III.PROPOSED SCHEME

In this work, we describe a deniable ABE scheme for cloud storage services. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. Our scheme is based on Waters cipher text policy-

attribute based encryption (CP-ABE) scheme. We enhance the Waters scheme from prime order bilinear group to Composite order bilinear group. By the subgroup decision problem assumption, our scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers.

In this work, we construct 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.

ADVANTAGES OF PROPOSED SYSTEM

Unlike most previous deniable encryption schemes, we do not use translucent sets or simulatable public key systems to implement deniability. Instead, we adopt the idea proposed with some improvements. We construct our deniable 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, ciphertexts will be decrypted to predetermined fake data. The information defining the dimensions is kept secret. We make use of composite order bilinear groups to construct the multidimensional space.

We also use chameleon hash functions to make both true and fake messages convincing.In this work, we build a consistent environment for our deniable encryption scheme. By consistent environment, we means that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look convincing for all ciphertexts under this environment, regardless of whether a cipher text is normally encrypted or deniably encrypted.

The deniability of our 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, we can construct the released fake key to decrypt normal ciphertexts correctly.

IV.MODULE

A. Owner Module

Owner module is to upload their files using some access policy. First they get the public key for particular upload file after getting this public key owner request the secret key for particular upload file. Using that secret key owner upload their file.

B. User Module

This module is used to help the client to search the file using the file id and file name .If the file id and name is incorrect means we do not get the file, otherwise server ask the public key and get the encryption file. If you want the decryption file means user have the secret key.

C. Deniable Encryption Module

Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in ciphertexts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence.This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing.

D. Key Distributor Module

We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. The architecture is decentralized, meaning that there can be several KDCs for key management.In this module generate public key for related user based on user/owner attribute.

E. Cloud Service Provider

Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption scheme.

V. AES ALGORITHM

Advanced Encryption Standard is mainly used to encrypt a confidential text into a decryptable format, for example when you need to send sensitive data in e-mail the decryption of the encrypted text it is possible only if you know the right password. AES was designed to be efficient

in both hardware and software and supports a block length of 128 bits and key length of 128, 192, 256 bits. It works at multiple network layer simultaneously, AES is one of the most frequently used and most secure encryption algorithm available today.

The algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte-therefore the term block cipher. Those operations are repeated several times, called "rounds". During each round, a unique round key is calculated out of the encryption key and incorporated in calculations. Based on the block structure of AES, the change of single bit, either in the key, or in the plaintext block, results in a completely different cipher text box. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world.

The behavior of the graphs shows that for file size up to 1000 kb, the required is less and it gradually rises when the file size is increased. If the encryption and decryption time is compared with similar systems, it shows that time required by AES System is significantly less.

Security and as the next step an index key word should be provided for that certain file which will be useful while searching the file for downloading.

VI.LITERATURE SURVEY

1.Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

ABSTRACT:

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

2.Ciphertext-Policy Attribute-Based Encryption

ABSTRACT:

In several distributed systems a user should only be able to access data if a user posses a certain set of cre- dentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the stor- age server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data deter- mines a policy for who can decrypt. Thus, our meth- ods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our sys- tem and give performance measurements.

3. Deniable Encryption with Negligible Detection Probability: An Interactive Construction

ABSTRACT:

Deniable encryption, introduced in 1997 by Canetti, Dwork, Naor, and Ostrovsky, guarantees that the sender or the receiver of a secret message is able to "fake" the message encrypted in a specific ciphertext in the presence of a coercing adversary, without the adversary detecting that he was not given the real message. To date, constructions are only known either for weakened variants with separate "honest" and "dishonest" encryption algorithms, or for single-algorithm schemes with non-negligible detection probability. We propose the first sender-deniable public key encryption system with a single encryption algorithm and negligible detection probability. We describe a generic interactive construction based on a public key bit encryption scheme that has certain properties, and we give two examples of encryption schemes with these properties, one based on the quadratic residuosity assumption and the other on trapdoor permutations.

4. Deniable Encryption

ABSTRACT:

Consider a situation in which the transmission of encrypted messages is intercepted by an adversary who can later ask the sender to reveal the random choices (and also the secret key, if one exists) used in generating the ciphertext, thereby exposing the cleartext. An encryption scheme is deniable if the sender can generate 'fake random choices' that will make the ciphertext 'look like' an encryption of a different cleartext, thus keeping the real cleartext private. Analogous requirements can be formulated with respect to attacking the receiver and with respect to attacking both parties. Deniable encryption has several applications: It can be incorporated in current protocols for incoercible ("receipt-free") voting, in a way that eliminates the need for physically secure communication channels. It also underlies recent protocols for general incoercible multiparty com-putation (with no physical security assumptions). Deniable encryption also provides a simplified and elegant construction of an adaptively secure multiparty protocol. In this paper we introduce and define deniable encryption and propose constructions of such schemes. Our constructions, while

demonstrating that deniability is obtainable in principle, achieve only a limited level of it. Whether they can be improved is an interesting open problem.

5. Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption

ABSTRACT:

Motivated by the question of access control in cloud storage, we consider the problem using Attribute-Based Encryption (ABE) in a setting where users' credentials may change and cipher- texts may be stored by a third party. We find that a comprehensive solution to our problem must simultaneously allow for the revocation of ABE private keys as well as allow for the ability to update ciphertexts to reflect the most recent updates. Our main result is obtained by pairing two contributions:

• Revocable Storage. We ask how a third party can process a ciphertext to disqualify revoked users from accessing data that was encrypted in the past, while the user still had access. In applications, such storage may be with an untrusted entity and as such, we require that the ciphertext management operations can be done without access to any sensitive data (which rules out decryption and re-encryption). We define the problem of revocable storage and provide a fully secure construction. Our core tool is a new procedure that we call ciphertext delegation. One can apply ciphertext delegation on a ciphertext encrypted under a certain access policy to 're-encrypt' it to a more restrictive policy using only public information. We provide a full analysis of the types of delegation possible in a number of existing ABE schemes.

• Protecting Newly Encrypted Data. We consider the problem of ensuring that newly en- crypted data is not decryptable by a user's key if that user's access has been revoked. We give the first method for obtaining this revocation property in a fully secure ABE scheme. We provide a new and simpler approach to this problem that has minimal modifications to standard ABE. We identify and define a simple property called piecewise key genera- tion which gives rise to efficient revocation. We build such solutions for Key-Policy and Ciphertext-Policy Attribute-Based Encryption by modifying an existing ABE scheme due to Lewko et al. [13] to satisfy our piecewise property and prove security in the standard model.

6. Fuzzy Identity-Based Encryption

Abstract:

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext en- crypted with an identity, ω, if and only if the identities ω and ω are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inher- ently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption". In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

7. Trusted Cloud Computing with Secure Resources and Data Coloring

ABSTRACT:

Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized data-center resources, uphold user privacy, and preserve data integrity. The authors suggest using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners. Data coloring and software watermarking techniques protect shared data objects and massively distributed software modules. These techniques safeguard multi-way authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds.

SYSTEM ARCHITECTURE

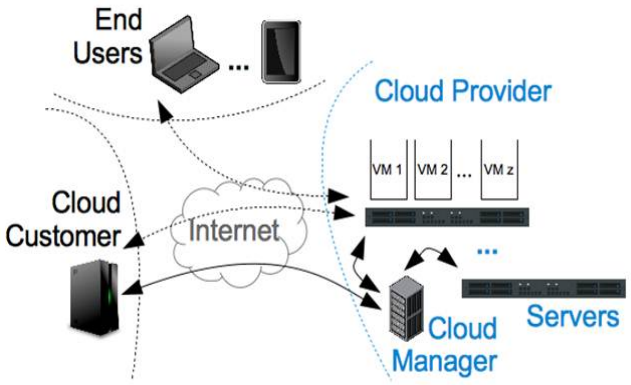

Figure 1 Architecture diagram

V.CONCLUSION

In this work, we proposed a deniable CP-ABE scheme to develop an secure storage of data in cloud using deniable encryption scheme for audit-free cloud storage service. The deniability feature makes fake users to be satisfied by the fake file given to them, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism. Our proposed scheme provides cloud

storage to be secure by the way of encrypted master key which is distributed to the user. Master key will be in an encrypted type key so that the fake user cannot hack file through mail. We hope more schemes can be created to protect cloud user privacy.

VI.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 ex- pressive, 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 re- encryption-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] ——. (2014) Edward snowden. [Online]. Available: http://en. wikipedia.org/wiki/Edward Snowden
[11] ——. (2014) Lavabit. [Online]. Available: http://en.wikipedia. org/wiki/Lavabit
[12] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in Crypto, 1997, pp. 90–104.
[13] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Eurocrypt, 2010, pp. 62–91.
[14] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ra`fols, "Attribute-based encryption schemes with constant-size ciphertexts," Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.
[15] M. Du¨rmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in Eurocrypt, 2011, pp. 610–626.
[16] A. O'Neill, C. Peikert, and B. Waters, "Bi-deniable public-key encryption," in Crypto, 2011, pp. 525–542.
[17] P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in WPES, 2010, pp. 31– 42.
[18] M. Klonowski, P. Kubiak, and M. Kutylowski, "Practical deniable encryption," in SOFSEM, 2008, pp. 599–609.
[19] M. H. Ibrahim, "A method for obtaining deniable public-key encryption," I. J. Network Security, vol. 8, no. 1, pp. 1–9, 2009.
[20] J. B. Nielsen, "Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case," in Crypto, 2002, pp. 111–126.
[21] R. Bendlin, J. B. Nielsen, P. S. Nordholt, and C. Orlandi, "Lower and upper bounds for deniable public-key encryption," Cryp- tology ePrint Archive, Report 2011/046, 2011, http://eprint.iacr. org/.
[22] D. M. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in Eurocrypt, 2010, pp. 44–61.
[23] A. B. Lewko, "Tools for simulating features of composite order bilinear groups in the prime order setting," in Eurocrypt, 2012, pp. 318–335.
[24] A. Beimel, "Secure schemes for secret sharing and key distribu- tion," Ph.D. dissertation, Israel Institute of technology, 1996.
[25] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in TCC, 2005, pp. 325–341.
[26] H. Krawczyk and T. Rabin, "Chameleon signatures," in NDSS, 2000.
[27] D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," in Eurocrypt, 2006, pp. 573–592.
[28] J. Katz, A. Sahai, and B. Waters, "Predicate encryption support- ing disjunctions, polynomial equations, and inner products," in Eurocrypt, 2008, pp. 146–162.
[29] S. Meiklejohn, H. Shacham, and D. M. Freeman, "Limitations on transformations from composite-order to prime-order groups: The case of round-optimal blind signatures," in Asiacrypt, 2010, pp. 519–538.
[30] D. Boneh, R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext se- curity from identity-based encryption," SIAM J. Comput., vol. 36, no. 5, pp. 1301–1328, 2007.
[31] 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.
[32] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommen- dation for key management: Part 1: General (revision 3)," NIST, Tech. Rep., 2012.