IJDCST @ July-Aug-2017, Issue- V-5, I-5, SW-27
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Secure Auditing in Cloud using Attribute Based Encryption

Pathan Irfan Khan[1], Mr. M.Vijay Kumar[2], Mr. K.Gopal Reddy

[1]Amritha Sai Institute of Science & Technology, Gani Atkuru Rd, Paritala, A.P.

[2]Associate Professor, Amritha Sai Institute of Science & Technology, Gani Atkuru Rd, Paritala, A.P.

[3] Associate Professor, Amritha Sai Institute of Science & Technology, Gani Atkuru Rd, Paritala, A.P.

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. We consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. In this paper a new cloud storage encryption schema is proposed which allows cloud storage providers to protect user privacy. Since authorities cannot tell the obtained secrets are true or false, the cloud storage providers ensure that the user privacy is still securely provided. The proposed schemes believe cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked. Some times may intercept the communication 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 the encrypted data are assumed to be known and storage providers are requested to release user secrets. The proposed Deniable CP-ABE scheme is to build an Audit free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with a fine grained access controlled mechanism.

Key Words- cloud storage, service providers, key management, attributes based Encryption, Deniable Encryption process.

1. INTRODUCTION:

Cloud storage is a form of data storage where the digital data is stored in logical pools, the physical storage span multiple servers (and often locations), and the physical environment is typically owned and handled by a hosting organization. These cloud storage providers are answerable for keeping the data available and accessible, and the physical environment protected and running. Different organizations buy or lease storage capacity from the providers to store customer application data. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API)[4] or by applications that utilize the API, such as cloud desktop storage, a gateway or Web- based content management systems. In the cloud storage environment customers can store their data on the cloud and access their data from anywhere at any time by connecting to a network. Because of user privacy, the data stored on the cloud is normally encrypted and safe guarded 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. Attribute-based encryption is a kind of public-key encryption in which the secret key of a user and the ciphertext are reliant upon attributes. In such a structure, the decryption of a ciphertext is achievable only if the set of attributes of the user key equals the attributes of the ciphertext.[5]. A central security feature of Attribute-Based Encryption is collusion-resistance: An challenger that grasps multiple keys be supposed to only be capable to access data if at least one individual key grants access. The aim choosing this attribute-based encryption is that as more responsive, 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 disadvantage of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). To overcome this disadvantage we used a new cryptosystem for fine- grained sharing of

encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, ciphertext are labeled with sets of attributes and private keys are associated with access structures that control which ciphertext by this the user can easily able to decrypt the data which was encrypted. The applicability of this construction is to share the audit-log information and broadcast encryption and also supports delegation of private keys which includes the Hierarchical Identity-Based Encryption. These Encryption schemes assuring that cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked.

2. 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 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. Encryption parameters 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].

In order to overcome all these disadvantages Cipher text policy attribute-based encryption (CP-ABE) scheme is being implemented. The implementation of a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In these circumstances, cloud storage service providers will just watch as receivers in other deniable schemes. Unlike most previous deniable encryption schemes, we do not use transparent sets or simulatable public key systems to apply deniability. Deniable Cipher Text Policy Attribute Based Encryption scheme make with two encryption environments at the same time, much like the idea planned in this scheme with many sizes while claiming there is only one size. This approach removes clear redundant parts. The base ABE scheme can encrypt one block each time; our deniable CPABE is definitely a block wise deniable encryption scheme. The bilinear operation for the Composite order group is slower than the prime order group, there are some methods that can change an encryption scheme from Composite order groups to prime order groups for improved computational performance. Deniable Cipher Text Policy

Attribute Based Encryption offers a reliable environment for our deniable encryption scheme[8].

This scheme extends a pairing ABE, which has a deterministic decryption algorithm.

3. SCHEME DESCRIPTION:

Most deniable public key schemes are bitwise, which means these schemes be able to process one bit a time. Hence, bitwise deniable encryption schemes are incompetent for real use, especially in the cloud storage service case. To resolve this problem, considered a hybrid encryption scheme that concurrently uses symmetric and asymmetric encryption. They use a deniably encrypted plan-ahead symmetric data encryption key, while real data are encrypted by a symmetric key encryption mechanism. Mainly deniable encryption schemes have decryption error problems. These errors come from the considered decryption mechanisms. Uses the subset decision mechanism for decryption. The receiver decides the decrypted message according to the subset decision result. If the sender desires an element from the universal set but unluckily the element is located in the specific subset, then an error occurs. The identical error occurs in all transparent set- based deniable encryption schemes. Scope the policy of a file might be unused to under the request by the customer, when concluding the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The position when any of the above criteria exists the policy will be rejecting and the key director will totally withdraw from the public key of the associated file. So no one can pick up the control key of a repudiated file in future. Due to this reason we can say the file is certainly erased. To get well the file, the user must ask for the key controller to fabricate the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is confirmed by means of an attribute connected with the file.

Deniable Encryption process:

Deniable encryption involves senders and receivers creating believable fake proof of fake data in cipher texts such that outside coercers are pleased. Note that deniability comes from the truth that coercers cannot confirm the proposed facts is incorrect and as a result no reason to decline the given evidence. This approach tries to overall block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can give audit-free storage services. In the cloud storage situation, 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.

Composite order Bilinear Group:

Design a deniable CP-ABE scheme with Composite order bilinear groups for building audit-free cloud storage services. Composite order bilinear groups contain two attractive properties, namely projecting and cancelling. We make use of the cancelling property for building a consistent environment; on the other hand, Freeman also pointed out the important problem of computational cost in regard to the Composite order bilinear group. The bilinear map operation of a Composite order bilinear group is much slower than the operation of a prime order bilinear group with the same security level. That is, in this scheme, a user will pay out too much time in decryption when accessing files from the cloud. To make Composite order bilinear group schemes more realistic, into prime order schemes. Both projecting and cancelling cannot be simultaneously achieved in prime order groups in. For the same reason, we use a simulating tool projected to convert our Composite order bilinear group scheme to a prime order bilinear group scheme. This tool is based on dual orthonormal bases and the subspace assumption. Unlike subgroups are simulated as different orthonormal bases and therefore, by the orthogonal property, the bilinear operation will be cancelled between different subgroups. Our formal deniable CP-ABE construction method uses only

the cancelling property of the Composite order group.

Attribute-Based Encryption:

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. For the reason of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the mutual property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are several ABE schemes that have been proposed, including. Most of the proposed schemes assume cloud storage service providers or trusted third parties managing key management are trusted and cannot be hacked; yet, in practice, some entities may cut off 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 understood to be known and storage providers are requested to release user secrets[6].

Cloud Storage:

Cloud storage services have grown popularly. For the reason of the importance of privacy, many cloud storage encryption schemes have been projected to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked. Still, in practice, some authorities (i.e., coercers) may force cloud storage providers to expose user secrets or confidential data on the cloud, thus in total circumventing storage encryption schemes. Here we present a design for a new cloud storage encryption scheme that enables cloud storage providers to generate realistic fake user secrets to protect user privacy. As coercers cannot tell if obtained secrets are correct or not, the cloud storage providers make sure that user privacy is still firmly protected. Most of the projected schemes guess cloud storage service providers or trusted third parties managing key management are trusted and cannot be hacked.

Distributed Key Policy Attribute Based Encryption:

KP-ABE is a public key cryptography primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is described. The encryptor acquaintances the set of attributes to the message by scrambling it with the comparing public key parts. Each client is assigned an access arrangement which is normally characterized as an access tree over information attributes. Client secret key is characterized to reproduce the access structure so the client has the skill to decipher a cipher-text if and just if the information attributes fulfill his access structure.

4. 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.

5. ACHIEVEMENTS BY CIPHER TEXT POLICY ATTRIBUTE-BASED ENCRYPTION SCHEME:

We can achieve high Computational performance. While using this scheme no security violence will occur. Deniable Cipher Text Policy Attribute Based Encryption construct at reliable environment. Reliable environment which means that one encryption environment can be worn for multiple encryption times exclusive of system updates. No error occurrences will face in decryption level. There is no data redundancy. The opened receiver verification should look believable for all cipher texts under this situation, apart from of whether a cipher text is usually encrypted or deniably encrypted. The deniability of this scheme comes from the secret of the subgroup task, which is resolute only once in the scheme setup phase. With this canceling property and the proper subgroup assignment, we can construct the released false key to decrypt normal cipher texts correctly Deniable Cipher Text Policy Attribute Based Encryption Extends a pairing ABE, which has a deterministic decryption algorithm, from the prime order group to the Composite order group. The decryption algorithm in this scheme is still deterministic; hence, there is no decryption errors using this scheme.

6. 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.

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)