International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Study of Controlling Cloud Data Access Privilege and Attribute Based Data Sharing with Attribute Revocation

Nishitara Shelke[1], Vidya Dhamdhere[2]

[1, 2]Savitribai Phule Pune University, G. H. Raisoni College of Engineering and Management, Wagholi, Pune, Maharashtra, India

Abstract: ***Cloud computing is a revolutionary computing environment, which allows user a flexible, on-demand, and low-cost usage of computing resources, but as the data is outsourced to some cloud servers, and various privacy issues emerge from it. To handle these security problems, various schemes based on the Attribute-Based Encryption have been proposed recently. Attribute-based Encryption (ABE) is a cryptographic conducting tool to guarantee data owner's direct control over their data in public cloud storage. ABE is an encryption method used by the user to store the data in the cloud. ABE is a public-key based one to many encryption methodologies which allows users to encrypt and decrypt data based on user attributes. In this paper we studied various schemes of ABE like KP-ABE, CP-ABE, Anony Control and Anony Control-F, also we analyzed how data access privilege and data sharing can be controlled by using various schemes of ABE.***

Keywords: Cloud Computing, Attribute-based Encryption, public keys, private keys, cipher text.

1. Introduction

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a cloud. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently [9].Cloud computing provides a scalable, location-independent and high performance solution by delegating computation tasks and storage into the resource-rich clouds. This overcomes the resource limitation of users with respect to data storage, data sharing and computation various techniques have been proposed to protect the data contents privacy via access control Identity-based encryption (IBE) [4,7.12,14,15], Fuzzy Identity-Based Encryption Key-Policy Attribute-Based Encryption (KP-ABE) [5,6,10], Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [3,8,11.13] and AnonyControl and AnonyControl-F [1] to allow cloud servers to control user's access privileges without knowing their identity information.

In the KP-ABE [5], a cipher text is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user's identity (e.g. IIT AND (Ph.D OR Master)). A user can decrypt the cipher text if and only if the access tree in his private key is satisfied by the attributes in the cipher text. However, the encryption policy is described in the keys, so the encrypter does not have entire control over the encryption policy [10]. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation.

On the other hand, those problems and overhead are all solved in the CP-ABE [3]. In the CP-ABE, cipher texts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the cipher text if and only if his attributes in the private key satisfy the access tree specified in the cipher text. By doing so, the encrypter holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots [11].

Unlike the data confidentiality, less effort is paid to protect users' identity privacy during those interactive protocols. Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes. But it seems natural that users are willing to keep their identities secret while they still get their private keys. Therefore AnonyControl and AnonyControl-F [1] to allow cloud servers to control users' access privileges without knowing their identity information. The schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. The schemes are tolerant against authority compromise, and compromising of up to (N − 2) authorities does not bring the whole system down.

2. Existing Systems

The literature survey that containing study of different schemes available in Attribute Based encryption(ABE).That are KP-ABE,CP-ABE, AnonyControl and AnonyControl–F. Also include advantage, disadvantage and a comparison table of each scheme based on fine grained access control, efficiency, computational overhead and collusion resistant.

2.1 IBE Scheme

Identity-based encryption (IBE) was first introduced by Shamir [4], in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. In an Identity-Based Encryption (IBE) scheme [7], the public key of the user is derived from its unique identity, e.g., email address or IP address. Yao et. al. [14] shows how an IBE system that encrypts to multiple hierarchical identities in a collusion-resistant manner implies a forward secure Hierarchical IBE scheme [15]. The original motivation for identity-based encryption is to help the deployment of a public key infrastructure.

Problems with IBE:

- For sending private key requires secure channel.
  Inherent key escrow: Private key is known to Private
- Key Generator (PKG)
- IBE scheme may depend on cryptographic techniques that are insecure against code breaking attack.

2.2 Attribute Based Encryption (ABE)

Few years later, Fuzzy Identity-Based Encryption [6] is proposed, which is also known as Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the one specified in the ciphertext. Sahai and Waters introduced the first attribute-based encryption (ABE) [5] where both the cipher text and the secret key are labeled with a set of attributes [10]. A user can decrypt a cipher text if and only if there is a match between the attributes listed in the cipher text and the attributes held by him. In Fuzzy IBE they 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 encrypted 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 [10] 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 inherently will have some noise each time they are sampled.

The generic fuzzy IBE scheme (Sahai and Waters, 2005 [5]) consists of the following algorithms.

Setup→Taking a security parameter as input, the PKG runs this algorithm to generate its master key mk and public parameters params which contain an error tolerance parameter d. Note that params is given to all interested parties while mk is kept secret.

KeyGen(mk, ID) → Taking the master key mk and an identity ID as input, the PKG runs this algorithm to generate a private key associated with ID, denoted by dID.

Encrypt (params, ID, mk) → Taking the public parameters params, an identity ID, and a plaintext m as input, a sender runs this algorithm to generate a ciphertext c.

Decrypt(params, dID, c) → Taking the public parameters params, a private key dID associated with an identity ID and a ciphertext c encrypted with an identity ID such that $|ID \cap ID| \; d$ as input, a receiver runs this algorithm to get a decryption, which is either a plaintext or an error message.

Problems with ABE:

- The lack of expressibility seems to limit its applicability to larger systems.
- On demand user revocation and other technique were not adoptable with this encryption method.

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

In the KP-ABE [6], a ciphertext is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user's identity (e.g. IIT AND (Ph.D OR Master)). A user can decrypt the ciphertext if and only if the access tree in his private key is satisfied by the attributes in the ciphertext.

An (Key-Policy) Attribute Based Encryption scheme consists of four algorithms:

Setup→ This is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Encryption→ This is a randomized algorithm that takes as input a message m, a set of attributes γ, and the public parameters PK. It outputs the ciphertext E.

Key Generation→ This is a randomized algorithm that takes as input – an access structure A, the master key MK and the public parameters PK. It outputs a decryption key D.

Decryption→ This algorithm takes as input – the ciphertext E that was encrypted under the set γ of attributes, the decryption key D for access control structure A and the public parameters PK. It outputs the message M if $\gamma \in A$.

Problems with KP-ABE:

- An encryption is the access policy is constructed into user's personal key. So data owner does not have the option on who can decrypt the data except encrypting the data with the set of attributes.
- The data owner is also a trusted authority (TA) at a same time.

2.4 Cipher-Text Policy Attribute Based Encryption (CP-ABE)

Sahai et al [3] introduced the concept of another modified form of ABE called CP-ABE. It allows the data owner to encrypt the data on an access policy, which will be based on the attributes of the user or data. So, the decryption is possible when the secrete key is matching with the access control policy. The key idea of CP-ABE [8] is: the user secret key is associated with a set of attribute and each cipher text will embedded with an access structure. The user can

decrypt the message only if the users attribute satisfied with the access structure of the cipher text. This method has the benefits such that the third party sever won't have the access on the plain data, decryption will be possible only when the secret key matched up with access policy defined on attributes, and every user is needed proper authorization to access the data. And also it removes the need for knowing the identity of the patients for providing access grant. CP-ABE [11] improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt it.

While in KP-ABE access policy is associated with private key, while in CP-ABE access policy is associated with cipher text.

Algorithm:
Setup→ The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Encrypt (PK, M, A) →The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.

Key Generation (MK, S) → The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

Decrypt (PK, CT, SK) →The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

Delegate (SK, S˜) →The delegate algorithm takes as input a secret key SK for some set of attributes S and a set S˜ ⊆ S. It output a secret key SK for the set of S˜ attributes S

Problems with CP-ABE:
- Difficulty in user revocation.
- Whenever owner wants to change the access right of user, it is not possible to do efficiently.
- Decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combination of attributes in a single set issued in their keys to satisfy policies.

2.5 AnonyControl and AnonyControl-F

In this system [1], there are four types of entities: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers (refer Fig.3). A user can be a Data Owner and a Data Consumer simultaneously. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them. Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree Tp can execute the operation associated with privilege p. The server is delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree Tp.

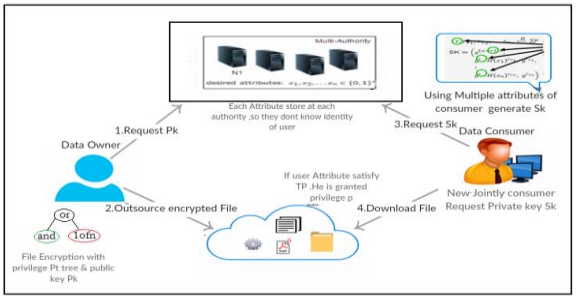

Figure 1: System Architecture

Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F

To formally define the security of our AnonyControl, we first give the following definitions.

Setup→ PK,MK*k* : This algorithm takes nothing as input except implicit inputs such as security parameters. Attributes authorities execute this algorithm to jointly compute a system-wide public parameter PK as well as an authority-wide public parameter *yk* , and to individually compute a master key MK*k* .

KeyGenerate(PK, MKk, Au) → SK*u*: This algorithm enables a user to interact with every attribute authority, and obtains a private key SK*u* corresponding to the input attribute set A*u*.

Encrypt(PK, M, {Tp}p∈{0,...,r−1}) → (CT,VR): This algorithm takes as input the public key PK, a message *M*, and a set of privilege trees $\{Tp\}p\in\{0,...,r-1\}$, where *r* is determined by the encrypter. It will encrypt the message *M* and returns a ciphertext CT and verification set VR so that a user can execute specific operation on the ciphertext if and only if his attributes satisfy the corresponding privilege tree *Tp*. As we defined, *T*0 stands for the privilege to read the file.

Decrypt (PK, SKu , CT) → *M* or verification parameter: This algorithm will be used at file controlling (e.g. reading, modification, deletion). It takes as input the public key PK, a ciphertext CT, and a private key SK*u*, which has a set of attributes A*u* and corresponds to its holder's GID*u*. If the set

Au satisfies any tree in the set $\{Tp\}p\in\{0,...,r-1\}$, the algorithm returns a message M or a verification parameter. If the verification parameter is successfully verified by Cloud Servers, who use VR to verify it, the operation request will be processed.

3. Proposed Solution

As we studied various schemes of ABE like IBE, KP-ABE, CP-ABE also one access control system i.e AnonyControl but the common problem with this techniques that no author work on user revocation strategy with these techniques, because whenever we want to implement these techniques in real scenario then there will be a need of user revocation, so here we proposed user revocation strategy which can work with AnonyControl system. In Revocational AnonyControl system after key generation phase, multi authority system build revocation tree Rt by using attributes of user. The revocation tree corresponds to time t and the identifier of revoked user is uid which is associated with one leaf node. So user uid is revoked only when there attributes matches with revocation tree Rt attribute set.

4. Conclusion and Future Work

In this paper, the survey of different encryption scheme like IBE, ABE, KP-ABE, CP-ABE, Anonycontrol and AnonyControl-F is mentioned with their advantage and disadvantage. The different variation of this scheme are compared and discussed with the existing scheme according to the rise in the security issues in cloud computing. The comparisons and study of those encryption scheme are done according to the problems arises and the solution on those the problem are mentioned.

Direction for future work is to allow multi authority servers to update user secret key without disclosing user attribute information. Also in AnonyControl system we worked with multi authority system, so it will be interesting to work with load balancing techniques to handle overhead.

5. Acknowledgement

We would like to thank all the authors of different research papers referred during writing this paper. It was very knowledge gaining and helpful for the further research to be done in future.

References

[1] Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption 190 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015

[2] A Privilege Based Attribute Encryption System For Secure and Reliable Data Sharing. International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 5, May 2014

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE SP, May 2007, pp. 321–334.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th

[7] Identity-Based Encryption with Outsourced Revocation in Cloud Computing IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 2, FEBRUARY 2015

[8] Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption Jinguang Han, Member, IEEE, Willy Susilo, Senior Member, IEEE, Yi Mu, Senior Member, IEEE,

[9] Jianying Zhou, and Man Ho Allen Au, Member, IEEE K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2895–2903.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS'10), 2010, pp. 261–270.

[11] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP'07, Washington, DC, USA, 2007.

[12] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," CRYPTO '01: Proc. Advances in Cryptology, J. Kilian, ed., pp. 213-229, Aug. 2001.

[13] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in ICALP'08. Springer, 2008, pp. 579–591.

[14] Y. Dodis, N. Fazio, A. Lysyanskaya, and D.F. Yao. ID-Based Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption. In ACM conference on Computer and Communications Security (ACM CCS), pages 354, 363, 2004.

[15] M. K. F. Dan Boneh: \Identity-based encryption from the weil pairing", In: Proceedings of The 21st Annual International Cryptology Conference on Advances in Cryptology CRYPTO'01, Santa Barbara, California, USA, Springer LNCS, Vol.2139, pp. 213-229 (2001).