International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-3)

Research Article

March
2014

Analysis and Security based on Attribute based Encryption for data Sharing

Ms. Snehlata V. Gadge
Dept. of Computer Engineering, University of Pune
Pune, India

Abstract –

In Attribute-based Encryption (ABE) scheme, attributes are focused for important role. Attributes are to be segregate to generate a public key for encrypting data and have been used as an access policy to control users' access. The access policy is flavored in two- key policy & cipher text policy. The key-policy attribute are used for describing encrypting data and policy implemented in user`s key, and the cipher text policy is the access structure on the cipher text. And the access structure can also be present in either monotonic or non-monotonic.ABE schemes can have the benefits: (1) decreasing the communication ,overhead of the Internet, and (2)a fine grained access control.[9]Storing data on untrusted storage like cloud space makes secure data and sharing of data a challenging issue. To resolve these issues cryptographic methods are implied. Cryptographic methods have scalability data access control along with key management etc. Attribute-based encryption (ABE) is one of the techniques that are more suitable for storing data with encryption. And the issue of key-escrow problem is resolved by issuing 2-pc protocols in system, which will protect the scene of key-escrow problem. The parameter like performance and security are satisfied for managing the data in disturbed way in data sharing networks.

Keywords – Identity based encryption, Cipher policy, key-escrow, 2-pc protocol, and access-structure.

I. INTRODUCTION

Social networks, such as orkut, Face book, Friendster [1], are an online application which enables users to find other users with similar interests. To use these applications, users must reveal large quantities of personal information (e.g. name, age, address, personal interests, sexuality, etc.) into the public domain. Groups of people sharing similar attributes and friends are then automatically linked to each other. Currently, such systems provide only weak privacy guarantees network membership allows access to the wealth of user information. Accordingly, user data can readily be mined and abused by undesirable parties. ABE-based systems are well suited to provide user controlled-privacy, as users in these communities are already characterized by their attributes. In Friendster, for example, a user with the attribute "Anon U. Alumnus" is automatically enrolled in a group of the same name. Accordingly, the creation of "white-lists" for communication immediately becomes possible without requiring enumeration of all user identities. Constructing a social network using ABE also provides scalability. Current social networks require a trusted central server to store all profile information and enforce policy. Because ABE-based systems do not require a trusted storage system, profile information could be stored on untrusted servers, significantly decreasing the traffic and storage requirements incurred by a system. To keep data confidential to data servers the data owner encrypts data before upload. User access is granted by possessing the data decryption key(s). When this kind of cryptographic-based access control scheme provide security protection on data, there are also several major challenges pertained to the scheme design [4]. To gain privacy of data from cloud service provider and other non related nodes encryption techniques are key source that provides relevant security. Network security consists of number of methods to achieve cryptographic security. One of them is most popular method is Attribute-based encryption (ABE).

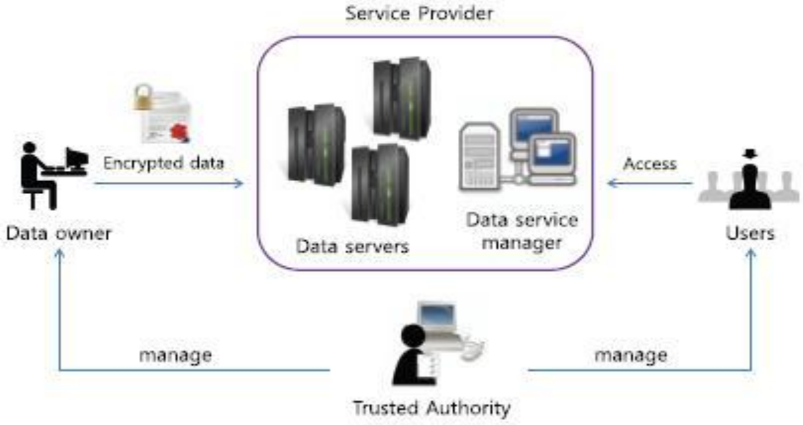

Fig 1 Architecture of Data sharing System

Architecture of data sharing system consists of the following entities:

A. Data Owner

It is a client who owns data, and wishes to upload it into the external data storing centre for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. Data Owner to get key from key generator Encrypt the file. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.

B. Data Storing Centre

It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. The data storing centre is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control. Data storing centre store the data. Data Storage Centers provides offsite record and tape storage, retrieval, delivery and destruction services [2].

C. User

This is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then he will be able to decrypt the cipher text and obtain the data.

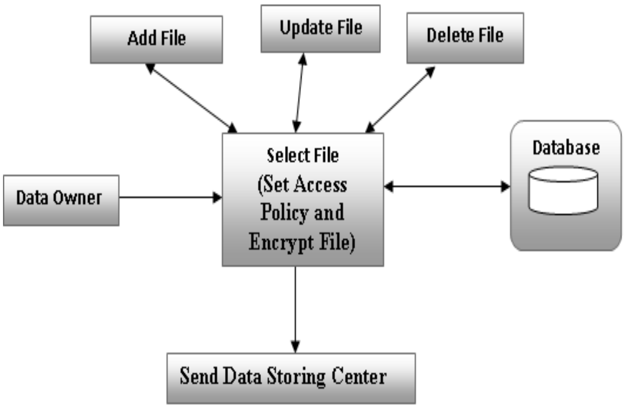

Fig 2 Data Owner (Set Access Policy, Encrypt File)

D. Key Generation Centre

It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted.

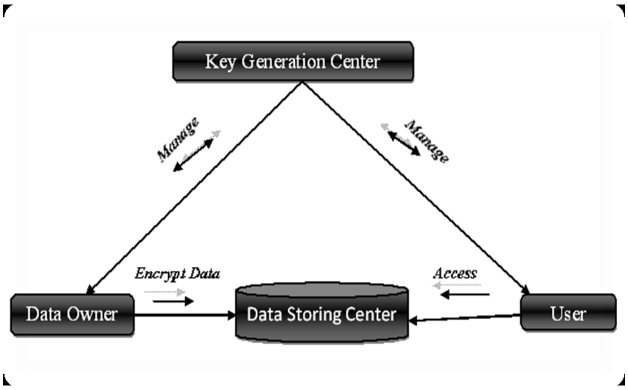

Fig 3 Node Structure of a Data Sharing System

The node structure of the Attribute based data sharing system[2] is shown in Fig. 3. The nodes involved are admin and clients which stands as UI for the system. The nodes are Key Generation Centre (KGC) is a key authority that generates public and secret parameters for CP-ABE. Data storing center is an entity that provides a data sharing service. The data storing center is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control. It is a client who owns data, and wishes to upload it into the external data storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. User is an entity who wants to access the data.

II. ATTRIBUTE BASED ENCRYPTION

Attribute-Based Encryption (ABE) algorithms. The Sahai-Waters [3] (ABE) cryptosystem as implemented in this paper is specifically detailed. We focus our efforts on providing the description of the scheme and intuition for its construction. For the proof of security see Sahai and Waters [3].Attribute-Based Encryption can be viewed as a generalization of Identity-Based Encryption (IBE) [5, 6, 7]. In IBE a user's identity is a string such as "bobsmith@yahoo.com". A party in the system can encrypt a message to this particular user with only the knowledge of the recipient's identity and the system's public parameters. In particular the encryption algorithm does not need to have access to a separate public key certificate of the recipient. In Attribute-Based Encryption a user's identity is composed of a set, S, of strings which serve as descriptive attributes of the user. For example, a user's identity could consist of attributes describing their university, department, and job function. A party in the system can then specify another set of attributes S0 such that a receiver can only decrypt a message if his identity S has at least k attributes in common with the set S0, where k is a parameter set by the system.

KGC with Data storing centre are involved in 2-PC protocol. The user needs to get connected with both the parties before getting the set of keys. The work of KGC is to authenticate users, along with the distribution of the set of attribute keys. The generation of secure 2-pc protocol takes places via. KGC and Data Storing Centre. It does the work of issuing the key components to user. So that user is able to generate secret key by combining the key components received from the both authorities. Thus in order to overcome the problem of key-escrow, 2-pc is introduced.

1. Init←setup ($1^{\wedge}$), works as trusted initialize and gives public key as output.
2. KGC generates public key and private key (PK_k,MK_k) ←KKGC()
3. Same as KGC generates the keys,Data Storing Center also generates the key,publiv and private key(PK_k,MK_k) ←KDSC()
4.KeycommD($MK_{D,}$$ID_t$)↔$Keycomm_k$($MK_{k,}$$ID_{t,}$aux)
5.$SK_{K,ut}$←$IssueKey_K$(aux,s)
6. $SK_{u,ut}$←$IssueKey_D$()
Access tree T

Let T be a tree representing an access structure. Each non-leaf node of the tree represents a threshold gate, described by its children and a threshold value. If numx is the number of children of a node x and kx is its threshold value, then0 < kx ≤ numx. When kx = 1, the threshold gate is an OR gate and when kx = numx, it is an AND gate.
Each leaf node x of the tree is described by an attribute and a threshold value kx = 1. To facilitate working with the access trees, we define a few functions. We denote the parent of the node x in the tree by parent(x). The function att(x) is defined only if x is a leaf node and denotes the attribute associated with the leaf node x in the tree. The access tree T also defines an ordering between the children of every node, that is, the children of a node are numbered from 1 to num. The function index(x) returns such a number associated with the node x. Where the index
values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner[14].

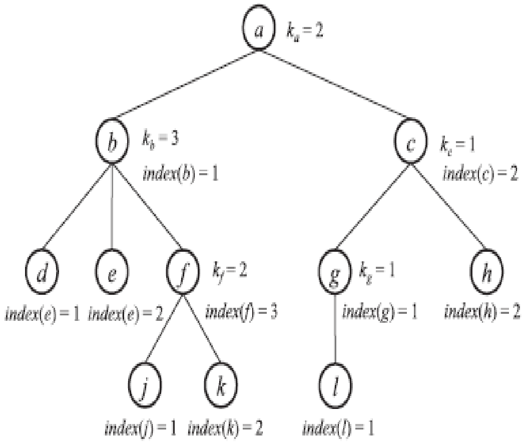

Fig 4: Access Tree

Fig. 6 shows an example of the access tree structure. In Fig. 4, nodes a, b, f represents AND gates, and node c represents OR gate, respectively .Satisfying an access tree. [14] Let T be an access tree with root r. Denote by Tx the subtree of T rooted at the node x. Hence T is the same as Tr. If a set of attributes γ satisfies the access tree Tx, we denote it as Tx(γ) = 1. We compute Tx(γ) recursively as follows. If x is a non-leaf node, evaluate Tx′ (γ) for all children x′ of node x. Tx(γ) returns 1 if and only if at least kx children return 1. If x is a leaf node, then Tx(γ) returns 1 if and only if att(x) γ.

III. REVIEW OF ANALYSIS & SECURITY BASED ON ABE FOR DATA SHARING.

In this section we are present the different methods those are for ABE with their advantage and problem.

In [13], L. Ebrahimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker proposed a mediated Cipher text-Policy Attribute-Based Encryption (CP-ABE) which extends CP-ABE with instantaneous attribute revocation. Furthermore, they demonstrate how to apply the proposed mCP-ABE scheme to securely manage Personal Health Records (PHRs).

In [3], A. Sahai and B. Waters introduced the concept of Fuzzy Identity Based Encryption, which allows for error-tolerance between the identity of a private key and the public key used to encrypt a cipher text. They described two practical applications of Fuzzy IBE of encryption using biometrics and attribute-based encryption. They presented our construction of a Fuzzy IBE scheme that uses set overlap as the distance metric between identities. Finally, they proved our scheme under the Selective ID model by reducing it to an assumption that can be viewed as a modified version of the Bilinear Decisional Diffie Hellman assumption. As more sensitive data is shared and stored by third-party sites on the Internet, There is on these sites will need to encrypt data stored. Encrypt data to a drawback is that it selectively only a coarse-grained level can be shared (i.e., give your private key to another party). They say that we attribute Key-fine-grained Policy-Based encryption (KP-Abe) to share encrypted data to develop a new cryptosystem. Features of working in our cryptosystem texts are labeled with sets and private keys which are able to decrypt cipher strength texts users are associated with access control structures.

In [11], J. Bettencourt, A. Sahai, and B. Waters presented system for Cipher text-Policy Attribute Based Encryption. Our system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt.

In [1], Chase and Chow presented a distributed KP-ABE scheme that solves the key escrow problem in a multi authority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this kind of fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with the other authorities in the system since the master secret is a centralized authority with information, system featuring all officials to generate secret key a user to communicate with other officials. M to generate a user's secret key.

In [14], Junbeom Hur specified the cause cases of corruption of KGC and corrupted data storing center, He has provided with a proof of 2pc protocol. And presented new efficient and secured method for data sharing systems. But the limitation of this system was reliability and load balancing under real time environment.

IV. CONCLUSION AND FUTURE SCOPE

In this paper, we are survey attribute-based encryption schemes: ABE that by using various access policy we are securing the system. And by using 2-pc protocol, the issue of key escrow problem is over come. And by using the time rekeying session we are overcoming the problem of fine revocation problem. Hence now a day's security of distributed system is pointing problem. And the key terms are used to keep the system more safe and secure, with the external attackers. In future we can consider these solution on the multimedia files and the system is lacking reliability factor, improvement in these pin holes can be done.

REFERENCES

[1] M. Armbrust, A. Fox, R. Gri±th, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, A view of cloud computing," Communications of the ACM, vol. 53, pp. 50{58, 2010.

[2] B. Sakthi Saravanan., M.Tech#1, R.Dheenadayalu M.Sc (Engg) #2 "Improving Efficiency and Security Based Data Sharing in Large Scale Network" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 1, January 2013, ISSN: 2319-5967

[3] A. Sahai and B. Waters. Fuzzy identity based encryption. In Eurocrypt 2005.

[4] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and Athena Vakali, Cloud computing: Distributed internet computing for it and scientific research," IEEE Internet Computing, vol. 13, pp. 10 {13, 2009.

[5] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer Verlag, 2001.

[6] C. Cocks. An identity based encryption scheme based on quadratic residues. In IMA Int. Conf., pages 360–363, 2001.

[7] A. Shamir. Identity based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in Cryptology, pages 47–53. Springer Verlag New York, Inc., 1985.

[8] Matthew Pirretti , Patrick Traynor "Secure Attribute Based Systems"

[9] Mr. Rupesh Vaishnav "Attribute Based Signature Scheme For Attribute Based Encrypted Data In Cloud" International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 10, December 2012 ISSN: 2278-0181.

[10] D.Khader ," Attribute Based Authentication Schemes," PhD Dissertation University of Bath, 2009.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[12] A. Beimel. Secure Schemes for Secret Sharing and Key Distribution. Phd Thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[13] Pieter Hartel,Willem Jonker" Efficient and Provable Secure Cipher text-Policy Attribute-Based Encryption Schemes "

[14] Junbeom Hur "Improving Security and Efficiency in Attribute-Based Data Sharing" IEEE transactions on knowledge and data engineering, vol. 25, no. 10, October 2013

[15] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.