International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Ciphertext Policy Attribute Based Encryption

Sneha Chandrashekhar Parit[1], Dr. Rashmi Rachh[2]

[1]*Assistant professor VCET Puttur*

[2]*Associate professor VTU,Belagavi*

Abstract - – The cloud computing has fundamentally changed the landscape of computers, storage and services. But the main hindrance to its adaptation is security. In literature, various counter measures are used to address this issue. One of them being attribute based encryption for "fine grained access control". In this project, "ciphertext policy attribute based encryption" scheme is used for providing cloud security and fine grained access control which allows encrypting data based on set of attributes called policy. Attributes are selected by owner who uploads file. Owner will choose the eligible users to access information. The cipher text produced will be accessible only if the policy is satisfied.

Key Words: policy, fine grained access control, attribute based encryption.

1.INTRODUCTION

Due to emerging technologies day today life has become faster. Now a day people want to store their data on cloud. Cloud is an Internet storage area where users can use storage efficiently and the services of cloud without having to worry about how they work. We can say that cloud is an abstraction for internet. Now a day attribute based encryption has paid a lot of attention. The main goal was to provide security and access control.In this scheme it allows encryption and decryption of data that depends on attributes of users. Policy has been defined here associated with access tree structure. The ciphertext produced will be accessible by user only if the policy is satisfied[12].

A. Cipher text policy attribute based encryption

The new technique of encryption and decryption method is CP-ABE where users without fear can store their information in any servers. This is an improvement of identity based encryption. Provides faster and secure access of data by restricting access to specified users[1,2]. This scheme considers attributes or credentials that describe users. Using those attributes files will be encrypted. This indicates the owner who is uploading files is going to select recipients, only those can access information.

Elliptic curve has been used in CPABE scheme. The main advantage of using this scheme is its key size and faster speed [3]. Elliptic curves uses smaller key sizes compared to other methods. Some of the crypto systems like AES,DES are said to be secure but they require their key to be distributed among number of users which may cause unauthorized people to get the information. That problem has been overcome in CPABE. It does not require a key to be distributed for encryption and decryption. Each user will have their own unique keys generated. Each keys are generated by using the attributes given by users.

B. Access tree structure

CPABE scheme requires attributes for encryption[10]. This can be represented by the tree structure. There are number of levels in the tree. The top most root in the tree is called root node lower level nodes are leaf nodes. Threshold value has been set that can be any value in between. This has to be satisfied for example having 3 attributes or nodes among them all 3 should be satisfied. Given as "3of3" is also called as policy.

C. Elliptic curve cryptography

In a cryptosystem we know that securing data has a major role.[3] Consider Alice and Bob both want to share their data securely. There may be a problem of EVE who can trap that information so Alice gets the public key of Bob encrypts the message and sends him. This key will be available to everyone but only Bob can decrypt it because only he is having private key to decrypt. At the same time they can add their signature and send that information. For example Alice sends message encrypting it with her signature when Bob gets that message he checks whether this message has sent from Alice or not if yes then he gets that authentic message. If that message is used by an eavesdropper then he gets garbage then Bob will get to know that message has been eavesdropped. Similarly for providing more security we use this elliptic curve which makes difficult to get that public and private keys.

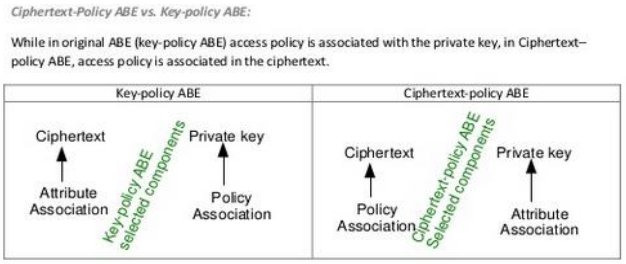
"Elliptic curve is a curve of the form Y^2=X^3+aX+b where these x,y,a,b are points on the curve. This condition also satisfies the point at infinity[13]."

The publish/subscribe system has gained very much attention because of decoupling of publishers and the subscribers in the terms of space ,time and synchronization. The publish-subscribe system has two important features. First is loose coupling i.e communicating users in publish-subscribe system are loosely coupled means that publishers does not need to know who are information receivers and the receivers also do not need to know from where the information coming[2]. Publishers and subscribers can remain ignorant of system topology and thus regardless of the other they can continue to operate normally. Second is the scalability i.e publish-subscribe system allows for dynamic and flexible communication environment for large number of users. Publish-subscribe system provides the opportunity for better scalability through parallel operation, network-based routing, etc[2]. Publishers publishes information to the publish/subscribe system, and by means of subscriptions the subscribers specify the events of interest. Traditionally sending and receiving data over a broker network ensures this decoupling[1]. Nowadays in more recent systems, publishers and subscribers use broker-less routing infrastructure to organize themselves, forming a secure network [1].

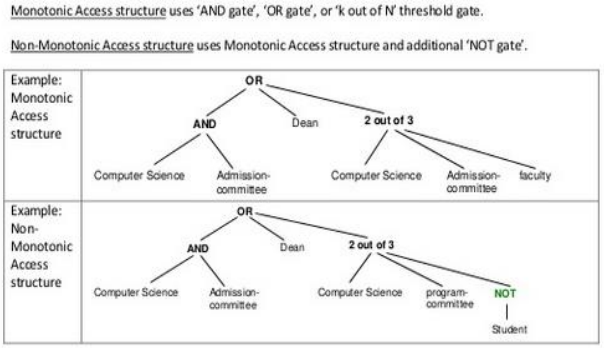
II. RELATED WORK

ABE was developed by sahai and Waters in the year of 2005 and their goal was to provide access control and security. In this scheme it allows encryption and decryption of data that depends on attributes of users. The ciphertext produced is completely based on these attributes like age of a person and city they stay etc. Decryption is possible only if users attribute matches with the attributes of ciphertext. Problem with this approach that owner has to use public key of every users. This is complicated to implement it in real time[2].

"Key policy attribute based encryption" here private keys are associated with an access tree and its ciphertext is associated with users attributes. Access tree is nothing but the tree with number of nodes. Attributes of user are called leaf nodes. Since private keys associated with access tree and ciphertext with attributes indicates which ciphertext user is able to decrypt[10]. Compared to ABE scheme this technique is more flexible and fine-grained access control but the drawback with this approach is that it will not decide the user who is eligible to decrypt the data. It can only select descriptive attribute for that data.



ABE scheme with non-monotonic access structure Ostrovsky et al. proposed this scheme in the year of 2007. Where they indicate access tree can use negative words to praise the credentials[6]. Previously this ABE scheme was monotonic which did not use negative values. But the problem with this approach is that there were many negative attributes in an encrypted data which were not related. So these attributes will become useless. It can cause increase in the size of encrypted data which is inefficient to use.

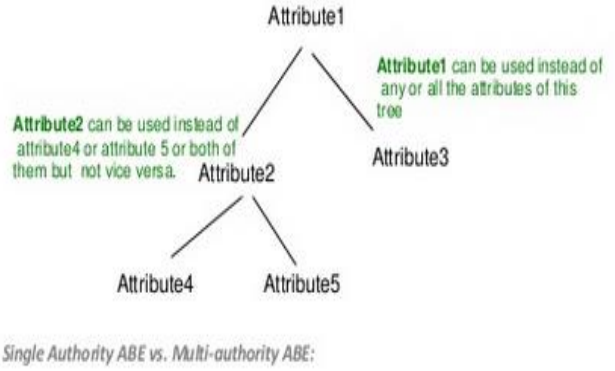


M. Srivatsa, et al.[14] have proposed a system called EventGuard which is a framework for securing the publish-subscribe system with brokers. EventGuard depends on a trusted meta-service (MS) responsible for creation of keys which are used for securing data and control the access in the publish-subscribe network. EventGuard generates public/private key pairs and certificates for meta-service and for the publishers and subscribers.

Hierarchical attribute based encryption was developed by Wong et al. It consists of root master and domain masters. This scheme hierarchically generates keys. This scheme is helpful for proxy re-encryption and it can also share data on cloud. But in practical it is not easy to implement.

Multiple authority ABE scheme was developed by V Bozovic et al. There will be multiple authorities who can distribute attributes to users and there is a central authority

who handles them. It allows independent authorities to manage the attributes. It can handle any number of corrupted authorities. Complication with this approach is that attribute set be disjoint[7,8].



Single Authority ABE vs. Multi-authority ABE:

In this paper to overcome from these problems we aim to implement CP-ABE for providing more security and achieving "fine grained access control" for the data stored on cloud. Data owner can decide the access tree structure .The owner who uploads file selects certain set of attributes. These attributes are related to user, so no one can easily identify these attributes. This technique is applicable for group of users. Policy specifies a condition for data access. User with set of attributes can access encrypted file only if it satisfies the policy.

III. PROPOSED SYSTEM

In this paper an attribute based encryption scheme is proposed which uses set of attributes or credentials of users to encrypt the data stored on cloud. Provides security and fine grained access control. Here owner is going to select the recipients to access his data.

A. Architecture of ciphertext policy attribute Based Encryption

Ciphertext policy based encryption scheme is a public key encryption scheme where the public keys are generated by taking implicit parameters from the elliptic curve. While generating the private keys it considers the policy. To encrypt the data it mainly requires the attributes of users which were specified in the form of access tree structure, we call it as policy. Suppose owner who is uploading the information will specify the policy as "3 of 3" it indicates at least 3 attributes of the user who are trying to access the information should be satisfied. Here user will be able to access the information only when user possesses certain set of attributes that satisfy the policy.

Pairing-based cryptography is used here. A mapping is established between two groups of elements selected from an elliptic curve with the use of bilinear maps. A bilinear map is defined by a function

" let G1 and G2 be two groups of order q where q is a prime value. Two groups have been mapped as $e:G_1*G_2->G_T$

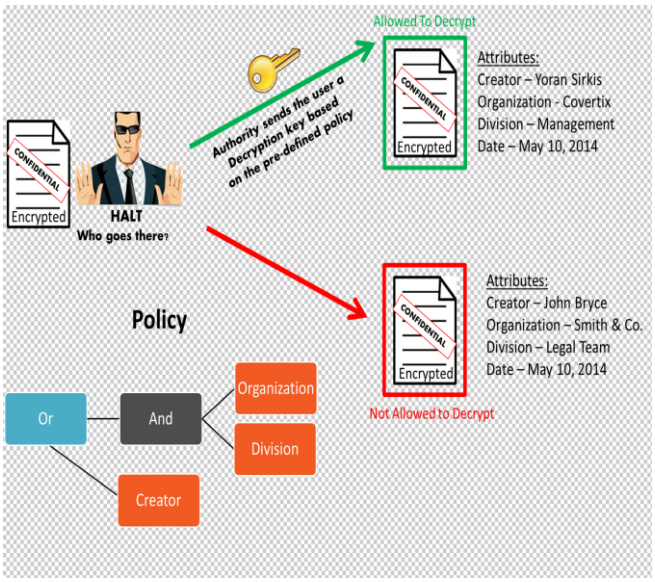


Fig. 1. Architecture of CPABE

Fig 1 shows the working of ciphertext policy attribute based encryption. User will initially request for a file. Owner may accept or reject the permission. Suppose he accepts the request then user will get the intimation. User tries to download the file. Even though permission is granted by owner, he/she can access file only when their attributes satisfy the policy. If attributes are matched file can be decrypted and downloaded. After downloading owner will get the intimation about the user.

B. Cipher text policy Based Encryption Scheme

Attribute Based Encryption is specified by four algorithms namely Setup, Encrypt, key generation, and Decrypt.

1) Setup: This step takes no input but considers implicit parameters and produces public key PK and master key MK.

2) Encrypt(PK,M,A): For encryption it uses public key PK , message M and access structure A for set of attributes.

Produces the cipher text CT. User whose attributes match with the policy only can access the information.

3) Key Generation(MK,A[ ]): this step takes master key and array of attributes as input and generates private key SK.

4)Decrypt(PK,CT,SK):It takes public key, ciphertext which includes policy and private key for array of attributes and if the array of attributes satisfies the policy only then he can decrypt and get the message M.

IV. IMPLEMENTATION

Here owner is going to upload file. While uploading owner selects certain set of attributes or credentials which describes user. Using those credentials access tree structure is formed called policy. To encrypt the data along with public and private keys, policy is also used. This provides fine grained access control and security for the data.

An Elliptic Curve is curve of the form:

$$y^2 = x^3 + ax + b \qquad (1.2)$$

where a, b, c and x, y are elements of some Field. A finite field is a field where the set is having a finite number of elements. The algorithms based on elliptic curve uses smaller key size compared to other algorithms". This is the main advantage of elliptic curve cryptography. In this paper "fine grained access control of data is provided by using Ciphertext Policy Attribute Based Encryption (CP-ABE)" .

A. Fine grained access contol

While uploading file owner will register himself first. Owner will select certain set of attributes related to user that means owner is restricting the access of information to specified user. Only those users who satisfy the policy can access the information. Restricting access of information possesses fine grained access control. During uploading owner will select the attributes. Those attribute sets are sent as parameter to encrypt the file that is called as policy. At the user end any user can send request to access the file. Owner may accept or reject the request. If at all owner accepts the request even though sometimes user cannot download the file. Because his credentials may not match with the policy. So even if it is an untrusted network also owner can upload the file without any tension.

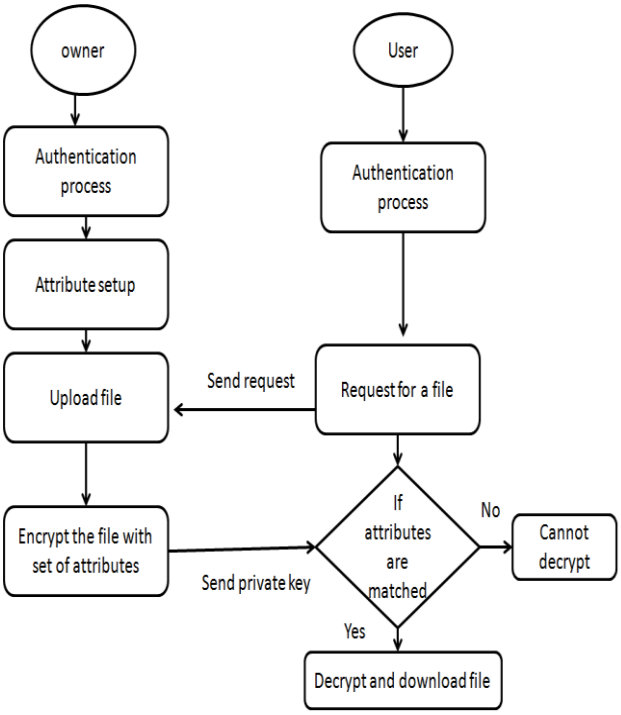


Fig. 2. Ciphertext policy attribute based encryption flowchart.

V. CONCLUSION AND FUTURE SCOPE

In this paper, attribute based encryption scheme has been developed. It supports for "fine grained access control" .Provides security for data storage on cloud. Owner will decide who are eligible to access information by selecting the attributes. Using these attributes policy has been developed. Here owner will consider the credentials of user to encrypt the data. To get the information it is required that user has to satisfy the policy.

In this paper once the attributes are set they cannot be revoked. In future we can implement this for attribute revocation.

REFERENCES

[1] Sascha M¨uller, Stefan Katzenbeisser, and Claudia Eckert. "Distributed Attribute-Based Encryption" CISC 2008, LNCS 5461, pp. 20–36, 2009.Springer-Verlag Berlin Heidelberg 2009.

[2]. Bethencourt, J., Sahai, A., Waters, B.:" Ciphertext-policy attribute-based encryption". In: IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Computer Society, Los Alamitos (2007).

[3]. Shoup, V.: "Lower bounds for discrete logarithms and related problems". In: Fumy, W. (ed.) EUROCRYPT1997. LNCS, vol. 1233, pp. 256–266. Springer, Heidelberg (1997).

[4]Darrel Hankerson. "Guide to Elliptic Curve Cryptography". Springer, 2004.

[5]. Waters, B.:"Ciphertext-policy attribute-based encryption": An expressive, efficient, and provably secure realization. Technical report, SRI International (2008) (to appear).

[6].Peter Mell, and Tim Grance, Draft NIST Working Definition of Cloud Computing, 2009: from http://csrc.nist.gov/groups/SNS/cloud-computing/.

[7]. Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded ciphertext policy attribute based encryption. In: ICALP (2008).

[8]. Cheung, L., Newport, C.C.: Provably secure ciphertext policy ABE. In: Ning, P.di Vimercati, S.D.C., Syverson, P.F. (eds.) ACM Conference on Computer and Communications Security, pp. 456–465. ACM, New York (2007).

[9]. S.G. Akl and P.D. Taylor. Cryptographic Solution to a Multi Level Security Problem. In Advances in Cryptology { CRYPTO, 1982.

[10] Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (2005).

[11].A. Beimel, "Secure schemes for secret sharing and key distribution", Ph. D. thesis, Dept.of Computer Science, Technion, 1996.

[12].Michel Abdalla, Dario Catalano, Alexander W. Dent, John Malone-Lee, Gregory Neven, and Nigel P. Smart. Identity-based encryption gone wild. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *ICALP (2)*, volume 4052 of Lecture Notes in Computer Science, pages 300{311. Springer, 2006.

[12] Attibute based encryption,http://en.wikipedia.org/wiki/Attribute-based_encryption.

[13]Elliptic curve cryptography, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography .