International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

USER REVOCATION MECHANISM ON ANONYMOUS ABE IN CLOUD COMPUTING

K satyanna[1]
Assistant professor(c)
University P.G.College O.U.
Secunderabad.

J. Kalyani [2]
Assistant Professor(c)
University P.G.College O.U.
Secunderabad

ABSTRACT :- Internet utility has been increasing day to day lives since its inception. Internet provides many utilities such as distributed computing, grid computing and many services such as pay-per-usage, virtualization. These utilities are main cause to play with any application irrespective of needs. Research surveys on data security convey that the sensitive data stored on hard drives or USB's is not secured for the business organizations. The objective of this paper is to achieve a multi-authority ciphertext-ABE which provides the protection for user privileges. It provides the security from compromising attack on the authorities or the collusion attacks by the authorities. Attribute based encryption is not different from other key encryption techniques. Instead of using public key to encrypt the files, it uses attributes or a key based on attributes. In this paper we enhance the security from the revocation of user. If any user removed from group, the user could not be able to access the data from the cloud.

[Key words: Cloud Computing, Attribute Based Encryption, User Revocation.]

1. INTRODUCTION

Internet has been enhanced its activities present days by utilizing its powerful services by providing pay per usage. Storing privacy data in external devices (such as USBs or CD etc...) is not secured. USBs were more dangerous since the data might not be held in encrypted form. Different techniques are proposed to protect the data privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir [1], in this sender's identity can recognized by receiver only.So the receiver can only decrypted the message of the sender. After, Fuzzy Identity-Based Encryption [2] 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 descriptor's identity has some overlaps with the one specified in the ciphertext. In this paper we proposing a security policy in cloud computing with handled with user attributes to generate encrypted data.

2. LITERATURE SURVEY:

Shamir introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. **"Fuzzy Identity Based Encryption"** It is also ABE, in which identity is obtained from a set of attributes and decrypt if its identity has the same. 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 ciphertext. A Fuzzy IBE scheme that uses set overlap as the distance metric between identities. **"Attribute-based encryption with verifiable Outsourced decryption"** The short comes of ABE and ABE with Outsourced Decryption motivate us to study ABE with verifiable outsourced decryption,

The new CP-ABE scheme consists of the following algorithms:

1. Setup(): Produces public key parameters and secret key.
2. Keygen(): Generates private key and transformation key for user.
3. Encrypt(): It uses public parameters, message and access policy to produce cipher text.
4. GenTKOut(): produces TK (transformation key) and its corresponding Retrieving Key by using PubKey and priKey .
5. Transformout(): It uses public parameters, cipher text, transformation key and provides partially decrypted ciphertext.
6. Decryptout(): It uses public key parameters ,cipher text, partially decrypted cipher text and retrieving key and produces final decrypted message.

The upload process involves following steps-

UPLOAD

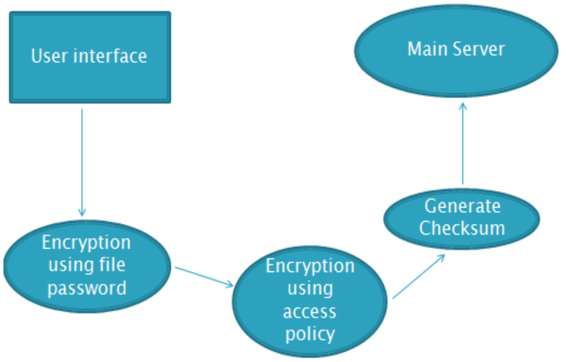
User interface
Main Server
Generate Checksum
Encryption using file password
Encryption using access policy

Fig.1. Upload Process

An access policy is defined by user when he upload a file. The system encrypts that file using the file password and also, performs second encryption using the access policy defined by the owner of the file. Alongside it generates the checksum and stores the encrypted checksum along with file in the main server. The user is unaware about the processes of backend.

ACCESS

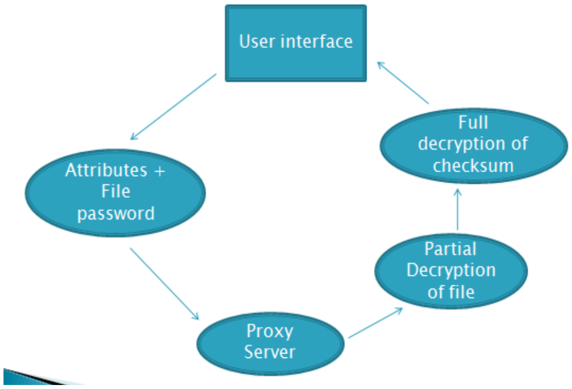
User interface
Attributes + File password
Full decryption of checksum
Partial Decryption of file
Proxy Server

Fig.2. Access Process

The file can be accessed by user and he should match the attributes of access policy which is defined by the owner. Access policy is examined to be satisfied and can perform first decryption using proxy server and produces decrypted checksum. Now the proxy server asks for the file password from the user. This file password has been checked to perform second decryption and the check sum is forwarded to user. The user's system will now generate the checksum of the received decrypted file and compares it with the received checksum.

Thus, the entire process provides outsourced decryption as well as checks integrity of the file.

3. A B E SCHEME

ABE is an encryption mechanism using public key. In ABE, users can define a policy with their attributes such as email, id, name, course, DOB etc… the attributes should satisfy the policy to get access of the document.

Attributes based encryption schemes are

i. Key policy-ABE

ii. Cipher text policy-ABE

i. Key Policy-ABE

In this, ciphertext is created with a set of attributes and a private key. It is associated with a monotonic access structure like a tree.

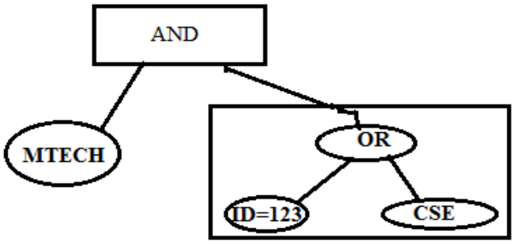

Figure 3. ABE Scheme

User decrypts the ciphertext, if it satisfies the access tree with its secret key.

ii. Cipher Text-ABE In this scheme, cipher texts are created with an access structure with encryption policy and private key. User can decrypt the ciphertext if the attribute in the private key satisfy the access tree specified in ciphertext. In both schemes user's identities are disclosed to key issuers, and the issuers issue private keys according to their attributes.

So, it is a natural scheme like other encryption mechanism. But users always wish to keep their attributes secretly. There are other schemes to control users to access privileges.

1. AnonyControl
2. AnonyControl-F.

These schemes protect user's attributes against every authority.

AnonyControl → Partial information disclosed
AnonyControl-F → Full information disclosed

The above all policies were successfully implemented. But there is another important issue is that if any user is removed then the users of rest group must be getting renewed keys.

To solve this problem of revocation in attribute based system, the *AnonyControl-F* scheme is using in this paper. This scheme can re-generate key and allows the data owner to re-encrypt files which are uploaded by files.

4. ABE USING *AnanyControl* SCHEME.

Phase 1: **Creation of PK and M K**

In this phase, attribute authorities generate public parameter (PK) and compute a master key (MK).

Phase2: Generation of Private Key

In this, private key will be generating by using each user's attribute.

GeneratePrKey(PK,MK)→ SK

Phase3: **Encryption of Message**

The message encryption takes public key and a set of privilege trees {Tp}. It will encrypt the message M and returns a cipher text CT and a verification set VR.

Encrypt (PK, M, {Tp})→ (CT, VR)

Phase 4: **Decrypting Message**

It uses the public key (PK), a cipher text (CT) and a private key (SK) which has a set of attributes of corresponding user. It returns a message (M) and a verification parameter (VR').

Decrypt(PK,SK,CT)→M,verification parameter

5. METHOD OF REVOCATION SCHEME

Step1: User's privileges control using AnonyControl-F scheme when user revoked from the group.

Step 2: Update the public keys for each and every file after revocation of a user from group.

ReKey(PT', FPT)→PK

Step 3: Update public keys will send to the data owner

Step 4: Data owner can encrypt again each file with updated public key and privilege tree and it generates re-encrypted ciphertext.

ReEncrypt (PK, {PT})→CT'

PK-→PUBLIC KEY

PT→PREVILIGE TREE

CT→CIPHER TEXT

6. System architecture

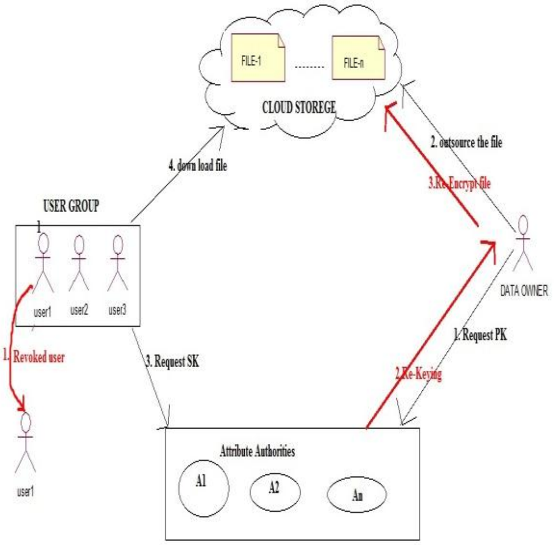

Figure 4. User revocation scheme using

7. CONCLUSION

Objective of this project is to achieve a multi-authority ciphertext-ABE which provides the protection for user privileges. It provides the security from compromising attack on the authorities or the collusion attacks by the authorities. In this paper, we enhance the security from the revocation of user. If any user removed from group, the user is not able to access the data from the cloud.Attribute based encryption is not different from other key encryption techniques. But instead of using public key to encrypt the files, it uses attributes or a key based on attributes.

8. BIBLIOGRAPHY

[1] A. Shamir, “identity-based cryptosystems and signature schemes,”in advances in cryptology. Berlin, germany: springer-verlag, 1985,pp. 47–53.

[2] A. Sahai and B. Waters, “fuzzy identity-based encryption,” in advancesin cryptology. Berlin, germany: springer-verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “attribute-based encryptionfor fine-grained access control of encrypted data,” in proc. 13th ccs, 2006, pp. 89–98.

[4] j. Bethencourt, A. Sahai, and B. Waters, “ciphertext-policy attributebasedencryption,” in proc. Ieee sp, may 2007, pp. 321–334.

[5] M. Chase, “multi-authority attribute based encryption,” in theory ofcryptography. Berlin, germany: springer-verlag, 2007, pp. 515–534.

[6] Boneh, D.,Waters, B.: a fully collusion resistant broadcast, trace, and revoke system. In: ccs ’06 proceedings of the 13th acm conference on computer and communications security. Pp.211 – 220 (2006)

[7]. Chu, C.K., Weng, J., Chow, S.s.m., zhou, J., Deng, R.H.: conditional proxy broadcast reencryption.in: 14th australasian conference, acisp 2009, lecture notes in computer science.vol. 5594, pp. 327–342 (2009)

[8]. Delerabl´ee, C.: identity-based broadcast encryption with constant size ciphertexts and private keys. In: asiacrypt 2007, lecture notes in computer science. Vol. 4833, pp. 200 – 215 (2007)

[9] s. Yu, c. Wang, k. Ren, and w. Lou, “attribute based data sharing with attribute revocation,” in proc. 5th asiaccs, 2010, pp. 261–270.

[10] Alta Van Der Merwe, M. C. (n.d.). Secure cloud computing - benefit,risks,control. Ieee explore

[11] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and D. Pointcheval. Key-privacy in publickey encryption. Lecture Notes in Computer Science, 2248, 2001.

[12] Giannakours, K. (2014). Clould computing stastics on the use of enterprises.

[13] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In eurocrypt, volume 3494 of lncs, pages 457–473. Springer, 2005.

[14]. Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption Taeho Jung, Xiang-Yang Li, Senior Member, IEEE, Zhiguo Wan, and Meng Wan, Member, IEEE