Anonymous Authentication using ABE for Securing Cloud Storage

Mr. Sadanand H. Bhuse
M.E.- II
Department of Computer Engineering
SAE, Kondhwa, Pune.India

Mr. Santosh N. Shelke
Assistant Professor
Department of Computer Engineering
SAE, Kondhwa, Pune.India

Abstract

In recent days cloud is the best option to store data and provide various services such as Infrastructure as a service cloud, Platform as a service cloud, Software as a service cloud and also communication as a service cloud. Cloud can be used for the various purposes, may be publically open or privacy based secured for sensitive information. The information in cloud can be secured in many ways as per the needs of the users. The authorization and authentication is the main issue in any service from such clouds. The attribute based encryption is the way to secure the authentication process to access and to control the access to the cloud and cloud services. Using same theme the authentication can be done without knowing the identity of the users i.e. to keep user anonymous for the curious system as well as administrator of the system. Considering decentralized access control and need to hide identity of the user, the concept of anonymous authentication is introduced and discussed in this paper. The multitenant SaaS is considered here and few issues related to ABE are focused.

Keywords- Cryptography, CP-ABE, KP-ABE, Anonymous Authentication, Multi-Tenancy

I. INTRODUCTION

As everyone is preferring for e-life, Digital information is the part of human being in day today life. For processing these information contents, clouds are preferably used to store the data due to its flexibility. Cloud storages are used in various manners. As far as services are concerned, Infrastructures, Software, Platform and communications are used as a service from clouds. Nowadays, there are many cloud hosting service providers for different purposed. In case of sensitive information security for the data and the person who is processing the data is necessary. The traditional encryptions are not sufficient for this purpose. The identity based authentication and role based authentication are insufficient in this case. The attribute based encryption as well as authentication is the main mechanism that can be used for keeping user info secret. That means user can be anonymous in case of identity of the user. It is also important to hide contents using attribute based encryption. In this paper we have implemented system which has decentralized access control and the anonymous authentication by using attributes as the factor for encryption.

There are various checksums for the user verification and access provision as per the user's authority. To receive services like any transaction, user must go through process of authentication. In case of outsourced cloud, there should be assurance to get protected from data tampering. As per Wang, Ron and Lon, In Cloud servers there are chances to Byzantine failure, where a storage server can fail in arbitrary ways. There is also possibility of data modification and server colluding. There are some major issues regarding the clouds such as keyword search, accountability, encryptions etc. In keyword search, the records must be associated with the particular keyword. In such cases cloud may not be familiar with the query but it is expected that it should satisfy the user's requirement. In accountability it is there are various checksums for the user verification and access provision as per the user's authority. To receive services like any transaction, user must go through process of authentication. In case of outsourced cloud, there should be assurance to get protected from data tampering. As per Wang, Ron and Lon, In Cloud servers there are chances to Byzantine failure, where a storage server can fail in arbitrary ways. There is also possibility of data modification and server colluding. There are some major issues regarding the clouds such as keyword search, accountability, encryptions etc. In keyword search, the records must be associated with the particular keyword. In such cases cloud may not be familiar with the query but it is expected that it should satisfy the user's requirement. In accountability it is expected that cloud should not deny for the particular service requested by the user but it should maintain the activity log for the same. To maintain such logs, cloud should decide that how much information should bekept in the log [4]. In case of cryptography issue, the user must go through the encrypted credential verification from cloud but cloud should not be able to read the data while on computations.

II. RELATED WORK

Waters and Sahai invented first attribute based encryption model in which the attributes are the additional to the identity parameters. Mainly there are two categories of the attribute based encryption methodologies. First one is Key Policy Attribute Based Encryption and second one is Cipher text Policy Attribute Based Encryption. In first category the data is encrypted by sender. The writer with

keys and featured attribute, is unable to write back if he is declined by. Here using set of attribute and secret key, receiver decrypts the [2] [4] [5].

In Cipher text policy methodology receiver receives attribute from tree structured access like Boolean operation such as AND, OR etc. [1-10].

Generally these method belongs to centralized approach. In this method, there is single key distribution centre. That causes single point failure. [3][4][9][11]. As per Chases, there are multiple key distribution centres in multi authority system [16] [19]. Lewko and Waters presented the system with decentralized approach and attribute based encryption where zero or more attributes were used by each authorized user. The process of decryption in all these case was computation centred. In all these cases, the performance is less or inefficient in use of mobile devices by the user as far as locations are concerned. To overcome these issues, Mathew Green et al. proposed system in which the decryption was outsourced using proxy servers to avoid extra resources in use.

Apart from all these methods, Ruj et al proposed decentralized scheme, in which the set of attributes are used to encrypt the contents stored. In this scheme replay attack can be prevented. In this system, user can replace fresh data with stale data from a previous write, even if it no longer has valid claim policy.

We are going to implement the decentralized system which is able to resist the replay attack. That has multi tenancy. Each user with particular set of attributes, will get specific appearance as an access control.

In our system following processes are carried out.

1) Data storage for the authorized users (authorization is based on set of attributes).
2) For storing and accessing of data, user must need to authenticate themselves.
3) User is not known by his identity.
4) Key distribution Center
5) Denial of access for rejected users.
6) Protection from replay attack.
7) Multitenant Access as per attributes.

III. SYSTEM IMPLEMENTATION

A. Basic Requirements for the Implementation

1) The administrator is supposed to be curious to know the user details
2) User is eligible to access using read and write permissions.
3) For all the transactions, SSH protocol is essential.
4) User are separated by means of set of attributes so as to get specific appearance.

B. Access Policies

Following are the access policies for the cloud storage's

1) The logical (Boolean) functions of attributes
2) LSSS (Linear Secret Sharing Scheme)
3) Monotonic span programs e.g. Boolean functions may be ANDing ORing of attributes a are : ((a1 _ a2 _ a3) ^ (a4 _ a5)) ^ (a6 ^ a7))

monotone span program for Y over a field F is an lt matrix M with entries in F, along with a labeling function a :[l] ![n]that associates each row of M with an input variable of Y. such that, for every(X1;X2:::::Xn) (0,1) the following condition is satisfied: Y (X1;X2:::::Xn) = 1 () 9_ 2 F1l : vM = [1; 0; 0; :::; 0] and (8i : xa(i) = 0) vi = 0) In other words Y (X1;X2:::::Xn) = 1 if the rows f M indexed by (i j Xa(i) = 1) span the vector [1, 0, 0, . . . , 0].

C. Mathematical Issues

Let GT be a group of order q. We can define the map e GG! GT The map fulfills the following properties: e (aP; bQ) = e (P;Q)ab8P;Q 2 G:anda; b 2 Zq Nonde generate:

e (g; g) = 1: By ignoring pairing function (Bilinear Prop) which uses Weil and Tate pairings [1][2][3] and computed using Millers algorithm.

D. Encryption

The encryption (PK, M,τ) is carried out in this stage. The input public parameters PK, The message M is encrypted with access treeτ. Here set of attributes areΓ. The partial cipher text is CP, which includes the access tree structureτ. There is no encryption access policy associated with this structure. [3]

E. Policy Creation

To create final cipher text by means of encryption policy there should be policy. We are using policies. Those are working on the input which is generated through partial cipher text. The cryptographic access policy are for the access tree.[3]

F. Policy Verification Process

This is nothing but the input for partial decryption. The set of attributes is the factors used for partial decryption.[2][3].

G. Decryption

This process is to get original contents from the partially decrypted contents. Same encryption policy with the set of attributes are used for the decryption [2] [3].

H. Attribute Based Signature

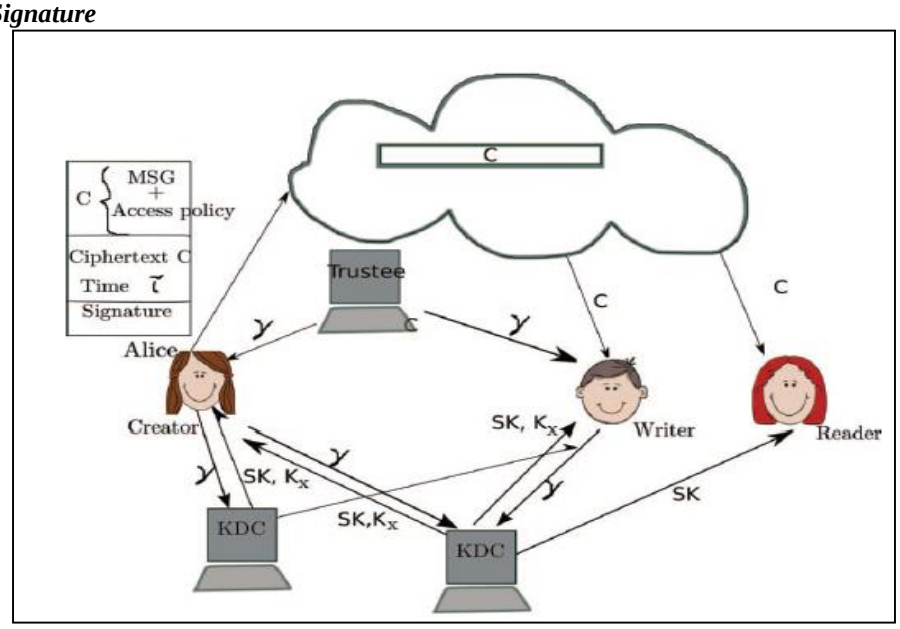

Fig. 1: Cloud Storage Model with High Security

This process is collection of system initialization, user registration, setup of KDC, generation of attributes, Signature etc. This scheme is proposed for: A user is creating a file and storing to cloud. Two protocols are used in this scheme i.e ABE and ABS. as per fig 1 there are three users such as creator, reader, and writer. Here trustee provides token to creator, assuming that trustee in honest. Multiple KDCs are there which can be scattered. On presenting the token a creator or more KDCs receive keys for encryption or decryption and signing. As per fig SKs are secret keys given for decryption and Kx are keys for signing in. MSG is the encrypted message under access policy X. Access for the particular user is decided by access policy e.g. who can access data from the cloud storage. The claim policy is decided by creator to prove his authenticity and signs the message under the claim. The cipher-text C with signature is c and it is sent to cloud. The signature is verified by cloud. And cipher text C is stores by cloud. If any user (reader) wants to read the contents, he must have same attributes for decrypting the data.

The principle of creating file is used for write proceeds. The time required for individual users for verifying themselves is reduced due to the attribute based verification system designed. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

I. Storage Mechanism

The registration of the user is done with one or more trustees. Then user gets tokens, private / public keys, and A key for an attribute x belonging to KDC Ai is calculated as

$Kx = (K_{base}{}^{1\ (a+bx))}$

Where (a; b) 2 ASK[i]

ciphertextC = Encrypt(MSG;X)[ABE]

_ = ABS and c = (C,τ,Y):

J. Retrieval

If some user makes request to the cloud for accessing data, the cipher-text C is sent by cloud with SSH protocol. Decryption is committed using ABE.

K. Writing to the clouds

Using claim policy user requests for access to the cloud for writing something to the cloud. The claim policies are verified by the cloud and only those are permitted who are authentic.

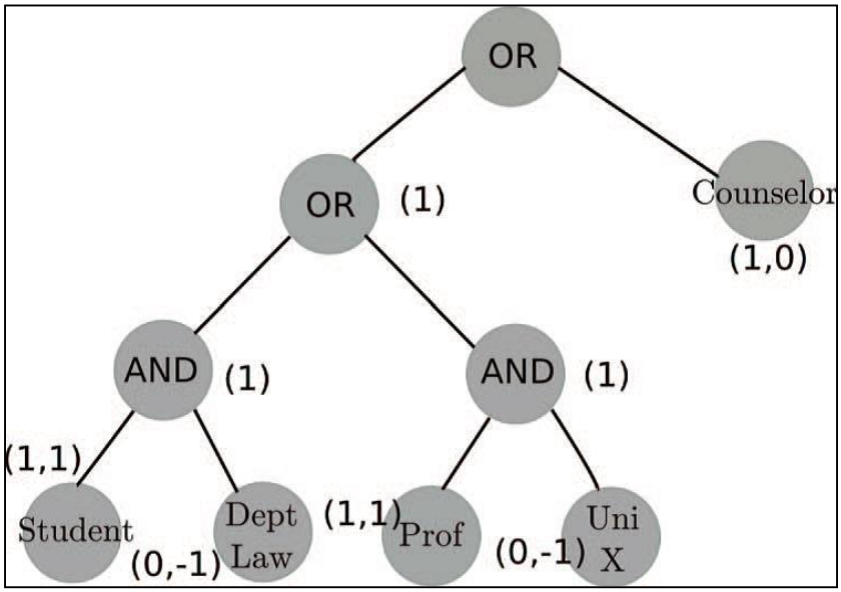

Fig. 2: Claim Policy Structure

IV. RESULTS

Following are the results

1) Fine Gained Access Control
2) Decentralized Access Control
3) Multiple Write Multiple Read
4) Access Control- ABE
5) Privacy: Authentication for the user
6) Revocation is Possible.

V. LIMITATIONS

Due to knowing access policy partial decryption is tempered by highly authorized person such as the administrator of the storage.

VI. CONCLUSIONS

By using attribute can be user to encrypt the data or user content. Using such type of encryption we can preserve the secrecy of the user from the administrator means user is anonymous. Identity of the user is kept secret. The replay attack is also prevented using this technique. As cloud knows the access policy, for the contents stored in the cloud, contents are not secret. The system is decentralized .The efficient and working attribute are the key factors for the success of the system.

ACKNOWLEDGEMENT

Our heartfelt thanks goes to Sinhgad academy of engineering, Kondhwa-Ppune for providing strong platform to develop our skills and capabilities I would like to thank HOD Mr. Gite B.B, guide Mr. Shelke S.N. and all the teachers for their valuable guidance. I would also like to thank everyone who directly or indirectly supported for fulfillment of the paper.

REFERENCES

[1] Sushmita Ruj,Milos Stojmenovic,Amiya Nayak. "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", *IEEE Transactions on Parallel And Distributed Systems*,Vol-25,2014
[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption", *IEEE Symposium on Security and Privacy*. , pp. 321–334, 2007
[3] Muhammad Asim, Milan Petkovic, Tanya Ignatenko,"Attribute Based Encryption and Decryption Outsourcing", *12Th Australian Information Security Management Conference* ,13 Dec 2014
[4] Umech Chandra Yadav, "Cipher text-Poliecy Attribute Based Encryptioin with Hiding Access Structure", *Advance Computing Conference (IACC)*, 2015
[5] GH Gowthami, G.G. Sreeja, B. Rajtha, "Control Cloud Data Access Privilege Using Attribute Based Encryption", *IRACST*, Vol 6 No.2, March April 2016.
[6] Divya L, Hema S, Kayalvizhi C, "Fully Annonymous Attribute Based Encryption for Privilege and Anonymity access control in cloud", *IJETCSE,Vol 21 Issue 2*, April 2016
[7] S.E. Wang, B.G.Lin, " A scheme of attribute based encryption access policy used in mobile cloud storage for personal health record" , *IEEE*, 2014.

[8] M.Sowmiya, M. Adimoolam, "Secure Cloud Storage Model with Hidden Policy Attribute based Access Control", *IEEE International Conference on recent trends in Information Technology,* 2014
[9] Shradhha Mokle, Nuzhat F Shaikh, "Anonymous Authentication for secure data stored on cloud with decentralized access control", *IEEE WiSPNET conference* 2016.
[10] Sadanand H Bhuse, Santosh N Shelke "A Noble Approach for Decentralized Access Control to Secure Cloud Storage Using ABA Authentication" *Fifth post graduate conference of Computer Engineering-cPGCON ,* 2016
[11] Xingbing Fu, Zufeng Wu, "Ciphertext Policy Attribute Based Encryption with Immediate Attribute revocation for fine grained Access Control in Class Storage", *IEEE ,* 2013.
[12] Zechao Liu et al. ,"Dynamic Attribute Based Access Control in Cloud Storage Systems" , *IEEE Trust Com –Big Data SE ISPA,* 2016
[13] Lifeng Li, Xiaowan Chen , Hai Jiang, "P-CP –ABE: Parallelizing Ciphertext –Policy Attribute Based Encryption for Clouds" *IEEE SNPD,* May 2016.
[14] Ms.S. Vijaya Lekshmi, Mrs. M.P. Revathi, "Implementing Secure Data access Control for Multi Authority Cloud Storage System Using Ciphertext Policy Attribute Based Encryption",*IEEE- ICICES2014* Chennai 2014.
[15] Karthik, Chandrashekhar B N Lakshmi H, "Fully Anonymous Attribute Based Encryption with Privacy and Access Pricilege", *IEEE- International Conference on Computational System and Information System for Sustainable Solutions,*2016.
[16] Dr. V.G. Goutham, K. Sunitha, P. Lakshmi, "Manage Cloud Data Access Opportunity and Anonymity with fully anonymous with secure status", *IJARCSSE-Vol. 6 Issue-6 , June 2016.*
[17] Sumeet Pate, Saurabh Gadhari, Vishal Mane, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", *IJREAM,* March 2016.
[18] Ileana Buhan, Emile Kelkboom, Koen Simoens, "A Survey of the Security and Privacy Measures for
[19] Anonymous Biometric Authentication Systems,"*IEEE, Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2010.
[20] Mate Horvath, "Private Key Delegation in Attribute-Based Encryption.
[21] Susan Hohenberger and Brent Waters "Attribute-Based Encryption with Fast Decryption", May 8 2013.
[22] Yingjie Xue et al, "LABAC: A Location-aware Attribute-based Access Control Scheme for Cloud Storage", *IEEE,* 2016.

Web References

[23] gleamly.com/article/introduction-attribute-based-encryption-abe
[24] cryptowiki.net/index.php?title=Attribute-based encryption