Decentralized Anonymous User Authentication For Securing Data Storage in Cloud

Shital S. Pagar[1]
Student of BE Computer Engineering
BVCOE & RI, Nasik, India
University of Pune
shtlpagar@gmail.com

Snehal M. Baviskar[2]
Student of BE Computer Engineering
BVCOE & RI, Nasik, India
University of Pune
Snehalbaviskar8@gmail.com

Vandana N. Chalwadi[3]
Student of BE Computer Engineering
BVCOE & RI, Nasik, India
University of Pune
Vandanachalwadi8@gmail.com

Prof. Kavita S. Kumavat[4]
ME Computer Engineering
BVCOE & RI, Nasik, India
University of Pune
kavitakumavat26@gmail.com

Abstract— The main objective of system is secure data storage on clouds. Cloud checks the authentication of the user without knowing the user's identity. For encryption use Attribute Base Encryption algorithm (ABE) in which encryption is takes place and also set access policies. Decryption is only possible for valid users in Access control policy. System prevents replay attacks because of Attribute Base Signature algorithm (ABS) and provides the facilities for creation, modification, and reading data stored in the cloud. This scheme provides facility for user revocation by that user cannot access the data. Therefore, emphasize that cloud should take a decentralized approach which is robust instead of using access control schemes designed for clouds which are centralized. In this scheme there is one limitation is that the cloud already know the access policy for each record or user stored in the cloud. In future, system can also hide the attributes and access policy of a user.

***Keywords** - Authentication, Access control, Attribute-based signatures, Attribute-based encryption, Cloud storage, Key Distributor Center (KDC), trustee.*

*****

I. INTRODUCTION

In cloud computing, users can outsource their computation and storage to servers (also called clouds) using On the cloud various resources are managed and stored .We saves very sensitive data ion clouds example military data and banking data .In a cloud security and privacy is very essential issue. The cloud computing is use of computer technology which provides access of resource as a service such as storage, network, server and processors. The security gets attention because the outsource data used by user [9]. In general data center in cloud holds information that users have store on their computers. Suppose cloud data is dynamic in data storage. The data stored in the cloud supports dynamic operations like insertion, deletion, appending and modification. This dynamic feature into the cloud gives the storage correctness .Assurance .In case of static data operation like applying multiple servers could be straight forward and all are focusing on static data. Dynamic data support to ensure the integrity and availability of users outsourced data in the cloud server. We depend on Fermat Number Transform, it is based Reed-Solomon erasure code in the file distribution provision instead of Vandermonde Reed- Solomon code to provide redundancies and guarantee the data availability against Byzantine servers. This construction significantly reduces the computation time and storage over. System practice consists of four phases: 1) File Encoding 2) Token Computation 3) Data Integrity Checking 4) Dynamic Data operations also Cloud provides following facilities such as Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS).Uses of different services: 1.In SaaS, software can be read from cloud by the user.2 PaaS comprises Operating System(OS), implementation atmosphere for software design language.3.Iaas delivers database controlling and web server facilities .In cloud environment the confidentiality is an challenging issue, but through the proposed approach the user can enjoy in secure platform even it is trustworthy since it is from client side security. User should have to be validating itself before starting an transaction, also it must be ensure by cloud. User discretion should be maintained so that cloud or other users on cloud cannot understand identity of user.

In a latest, Wang et al [1], enables protected and trustworthy cloud storage in this scheme averts from server colluding attack. Now a day in cloud access control is very important only because of access control authorize users have rights to access valid services .A large amount of information is exists on cloud and maximum information is very subtle and we should secure this information. Fundamentally three types of access controls are available: User Based Access Control (UBAC), Attribute Based Access Control(ABAC) and Role Based Access Control (RBAC).In the UBAC there is access control list ,that contains list of genuine user that can access data but it is suitable for less amount of user .In RBAC includes individual roles data can be access by only those user who have matched roles that roles are system define .In ABAC users have given attributes and access policy is attach with data .The advantage and disadvantage of ABAC and are RBAC converse in [2].

Access Controls are very widely used in medical or health care field. Clouds are frequently used to store sensitive data of patients for permitting access to medicinal experts, staff and policy developers. We can encrypt the data with some access policy by using an ABE Algorithm for each patient record and after that kept in clouds. here users are having a set of attribute and keys ,if users are having a matching attributes then and then only user can decrypt the information that are stored on clouds. Securing personal health record is studied in [3] Access Control has gaining reputation in online communal networking. In Online communal networking user saves his personal information, snaps, videos and they can share them with their selective Friends [5]. Write access was not permissible to user other than the creator.

Attribute based Encryption is a cryptographic primitive for access control shared data. Each user is associated with a set of attributes and data are encrypted with access structures on attributes. Attribute revocation is an stimulating issue which can be resolve by uniquely integrate the technique of proxy re-encryption with cipher text- policy Attribute Based Encryption and it gives permission to delegate most of task to the proxy server [4]. In a cloud procurement of efficient exploration is also imperative task. In that the cloud should not know anything about the query sends by the user but it should be able to return the record or result and result should satisfy the query effortlessly. This can be accomplished in [6] [7].

II. LITERATURE SURVEY

In existing work [10] use a centralizing Approach for KDC. In case if that single KDC Fails then total System will get Collapse. Access Policies are Also Centralized in nature and this centralization has lack of reliability. If we assume that outsource data is very huge, then we should have to reduce overhead at the originator side. In this system every data block has to be encrypted and for that every time different keys are used so the flexibility is achieve for access controls. Originator need to maintained very few keys because key derivation scheme [12].This system having limitation of many-write-many-read applications. Work in Multi-authority attribute based encryption [11] any party is authority and that party has gain authority by simply producing a public key and gaining a secret key from different users.it will reflects their attributes. There is no prerequisite of conscious about each other authorities. It is having several KDC's in Distributed manner. That multiple KDC's are place all Over World. In the system Boolean formula is used over the attributes allotted from any selected set of specialists. So, it should not require central specialist [5]. Sahai and waters are the discoverer of ABE algorithm. In ABE algorithm user keys and cipher text are branded with a set of different evocative attributes. In that particular key can decrypt only a particular cipher text if there is having a matching user key and attribute policy of cipher text [8].

As shown in figure 1, system uses a centralized approach for KDC, there is no role of trustee server, so the cloud easily reveals the identity of user also the users of cloud also aware about a originators. So confidentiality is not maintained here.

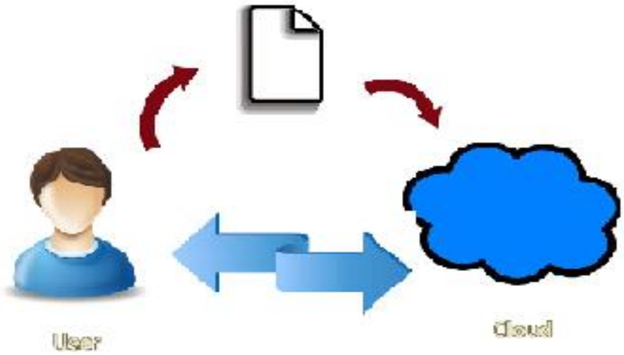
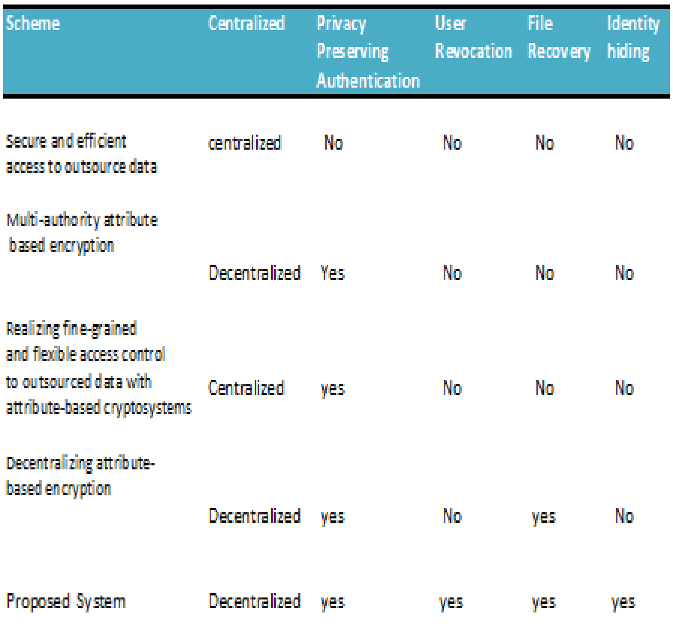


Figure 1.Existing System

Following table 1 shows the basic comparison between all different existing technologies. As compared to other technology proposed system is precise to maintain and contributes more by providing several services like privacy preserving authentication, user revocation, file recovery, hiding identity.

Table 1: Comparison Chart



Scheme	Centralized	Privacy Preserving Authentication	User Revocation	File Recovery	Identity hiding
Secure and efficient access to outsource data	centralized	No	No	No	No
Multi-authority attribute based encryption	Decentralized	Yes	No	No	No
Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems	Centralized	yes	No	No	No
Decentralizing attribute-based encryption	Decentralized	yes	No	yes	No
Proposed System	Decentralized	yes	yes	yes	yes

For user revocation, the owners should change the stored data and send updated information to other users. The set of attributes Iu possessed by the revoked user U_u is noted and all users change their stored data that have attribute $s_i \in I_u$. In revocation involved changing the public and secret keys of the minimal set of attributes which are required to decrypt the data. We do not consider this approach because here different data are encrypted by the same set of attributes, so such a minimal set of attributes is different for different users Therefore, this does not apply to our system.

III. SYSTEM OVERVIEW

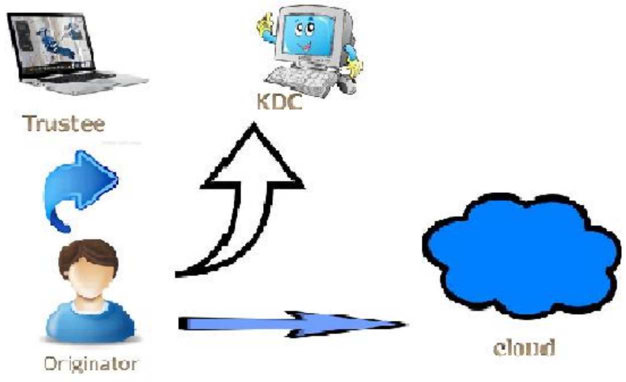


Figure 2.System Architecture

Figure2. shows general architecture of system in which originator can create a file. In this scheme we use two algorithms ABE and ABS. we refer above example to understand clearly the architecture of System. There are 3 users: originator, writer and reader. First the originator John logs on to the trustee and trustee sends a token to the John and John receives it. John sends that token to the KDC .here we are using 2 KDC but in originality we can use multiple KDC which are place on all over world. Then Jon receives the keys for encryption/decryption and signing. Then that message are encrypted with the access policies and cipher text C is created with the signature by using attribute based signature algorithm and cipher text is sends to the cloud On the cloud side cloud verifies the cipher text c and signature by using verify algorithm and stores the cipher text c. When reader request to read then cloud sends cipher text c.

A. *Terms and Definitions*

Anonymous authentication

Anonymous authentication is the process of giving access to user which is having unrecognizable identification. This gives security to the clients to conceal their details from other clients of that cloud.

Replay Attack

Replay Attack is a process of capturing information of the communication between two parties and attacker capture sensitive information and uses this information for communication starts Conversation with one of party between them by giving authenticated information or identity Proof.

Trustee

Trustee is the third party federal server who manages the insurance number etc. and on presenting an ID he will generate a token.

KDC

KDC is the Key Distributor center which generates different keys for a user for e.g. Secret key for decryption and public key for encryption and sends it to the user.

User revocation:

It should be ensured that users must not have the ability to access data, even if they possess matching set of attributes.

B. *System Flow*

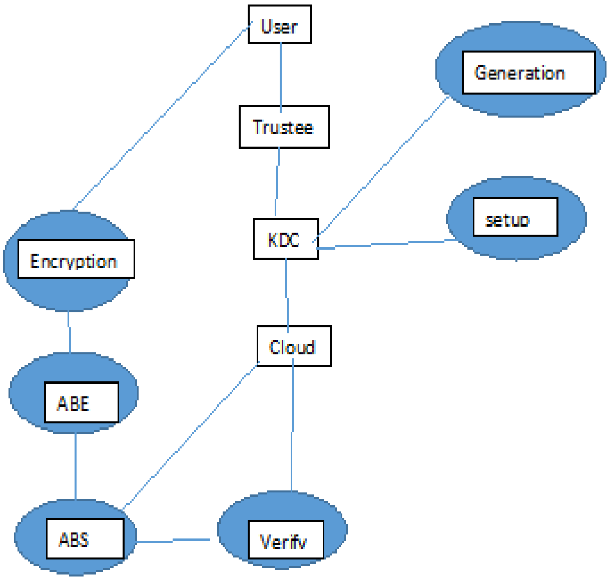


Figure 3.System Flow Diagram

Figure 3 shows complete flow of system is as follows:

1. Registration and Login:

User register on the trustee and trustee gives a token to the user with it is a private key (certificate).It is use for authentication purpose.

2. Sign

The message is selected, access policy are set and then encrypt the message using ABE and upload the message in the cloud. The cloud sends cypher text to the user. The access policy decides who can access the data saved in the cloud. The originator decides on a claim policy, to prove her authenticity and signs the message under this claim. The cloud verifies the signature and saves the ciphertext C. When any user wants to read the data, the cloud sends Cipher text. If the user has attributes matching with access policy, it can decrypt and get back original message. If attribute doesn't match then decryption is impossible. So, we also develop encryption and decryption module.

3. Design of KDC

KDC accept a token from trustee which includes a signature of trustee and KDC verifies the signature for authenticity of user. KDC has a set of numbers, form this combination it generates key for user. It generates the key (Attribute Base Encryption ,Attribute Base Signature ,Key Generation ,Verification Algorithm.) and all keys are delivered to the user securely using the user's public key, such that only that user can decrypt it using its secret key.

4. Database Designing for Cloud

At a cloud side verification access policy are checked. If the user is an authenticate user then he can modify the data by using ABS technique .If user is authenticated then it allows to write the message on cloud while uploading the message user sign the message using ABS technique.

5. Database Design for trustee

User register on the trustee and trustee gives a token to the user with it's a private key (certificate).It is use for authentication purpose.

IV. Algorithmic Strategy

1. Attribute based encryption:

Attribute based encryption algorithm is use for encrypting access policies.

1) Select a prime q, generator g of G0, groups G0 and GT of order q, a map
E: G0 × G0 → GT

2) A hash function H: {0, 1}* → G0 which maps the identities of users to
G0. Each KDC also chooses two random exponents
a_i y_i ∈ Zq. The secret

3) Key of KDC Aj is
SK[j] = {α_i, y_i, i ∈ L_j}. C Aj , and corresponding

4) Secret key ski, u for each i ∈ I[j, u]
ski, u = gαiH(u)yi ,
Where α_i, y_i ∈ SK[j].

2. Encryption by sender*:*

The encryption function is ABE. Encrypt(MSG,X). Sender decides about the access the X.

1) Choose a random seed s ∈ Zq and a random vector v ∈ Zq^n, with s as its first entry, n is the number of leaves in the access tree.

2) Calculate λx = Rx · v, where Rx is a row of R.

3) Choose a random vector w ∈ Zq^n with 0 as the first entry.

4) Calculate ωx = Rx · w.

5) For each row Rx of R, choose a random ρ_x ∈ Zq.

6) The following parameters are calculated:
C0 = MSGe(g, g)s
C1,x = e(g, g)λxe(g, g)απ(x)ρx , ∀x
C2,x = gρx∀x
C3,x = gyπ(x)ρxgωx∀x,
Where π(x) is mapping from Rx to the attribute i that is located at the corresponding leaf of the access tree.

7) The cipher text C is sent by the sender
C = R, π, C0, {C1,x, C2,x, C3,x, ∀x}

3. Decryption by receiver:

The decryption function is ABE. Decrypt(C, {ski, u}), Where C is given by equation .Receiver $_{Uu}$ takes as input cipher text C, Secret keys {ski, u}, group G0, and outputs message msg. It obtains the access matrix R and mapping π from C. It then executes the following steps:

Step 1: U_u calculates the set of attributes {π(x) : x ∈ X}
common to I_u the itself and the access
matrix.

Step 2: It checks if there is a subset X' of rows of R, such
that the vector
(1, 0 . . . , 0) is their linear combination.

Step 3: it calculates constants cx ∈ Zq, such that
Σx∈X' cxRx = (1, 0, , , 0).

Step 4: Decryption proceeds as follows:
a) For each x ∈ X' $\text{dec}(x) = \frac{\text{C1,xe(H(u),C3,x)}}{\text{e(sk}\pi\text{(x),u,C2,x)}}$

4. Verify Algorithm:

1) ABS. verify (TPK, σ = (Y,W, S1, S2, . . . , St, P1, P2,
. . ., Pt),MSG, Y),
Converts Y to the corresponding monotone program M∈ Zl ×t, with rows labeled with attributes. Compute μ = H(MSG||Y).

2) If Y = 1, ABS.
Verify = 0 meaning false. Otherwise, the following constraints are checked.
ệ (W,A0) ?= ệ(Y, h0)
Π I∈l ệ (S_i, A_i_jBπi_(i) _j)M_{ij}) = ệ(Y, h1) ệ(g2gμ1,P1), j = 1
ệ(g2gμ1, Pj), j > 1,
Where i_ = AT[i].

Table 2 shows all different variables included in above four algorithms specifications. Variable specifications must help in understanding of algorithms.

Table 2: Algorithmic specification

Symbol	***Meaning***
U_u	u-th User/Owner
A_j	j-th KDC
A	Set of KDCs
L_j	Set of attributes that KDC A_j possesses
$l_j = \|L_j\|$	Number of attributes that KDC A_j possesses
X	Boolean access structure
Y	Claim policy
τ	Time instant
R	Access matrix of dimensionm×h
M	Matrix of dimensionl×tcorresponding to the claim predicate
MSG	Message
|MSG|	Size of message MSG
C	Ciphertext
H,H	Hash functions, example SHA-
	I_u Set of attributes that user U_u Possesses
J[j, u]	Set of attributes that A_j gives to user U_u for claim attributes
Ju	Set of attributes that user U_u possesses as claim attribute
AT[j]	KDC which has attribute j
PK[j]/SK[j]	Public key/secret key of KDC A_j for encryption/decryption
$sk_{i,u}$	$sk_{i,u}$ Secret key given by A_j corresponding to attribute i given to user U_u
TPK/PSK	Trustee public key/secret key

V. Conclusion

For securing data stored in cloud use of decentralized anonymous method is very effective by which easily hide the identity of user. In which trustee can generate the token for valid user. Attribute based signature algorithm is very effective for checking user validity. System can prevents replay attacks and also handle user recalling. Public and private keys are generated by Key distribution center for valid user for encryption. Key distribution is done in a distributed way. The cloud does not recognize the user who stores information, but only inspects the user's activities.

References

[1]] C. Wang, Q. Wang, K. Ren , N. Cao and W.Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T. Service Computing*, vol. 5, no. 2, pp. 220–232, 2012.

[2] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based Access control," IEEE *Computer*, vol. 43, no. 6, pp. 79–81, 2010.

[3] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Secure Comm , pp. 89–106, 2010.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," inACM ASIACCS, pp. 261–270, 2010.

A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 6632. Springer, pp. 568–588, 2011.K. Elissa, "Title of paper if known," unpublished.

[5] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou,"Fuzzy keyword search over encrypted data in cloud computing,"in IEEE INFOCOM. ,pp. 441–445, Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[6] S. Camera and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol .

[7] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS , pp. 735–737.

[8] 2010F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in ISPEC, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.

[9] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011.

[10] M. Chase, "Multi-authority attribute based encryption," in TCC, ser. Lecture Notes in Computer Science, vol. 4392. Springer, pp.515–534,2007

[11] W. Wang, Z. Li, R. Owens, and B. Bhargava, “Secure and efficient access to outsourced data,” in ACM Cloud Computing Security Workshop (CCSW),

Shital S. Pagar she is BE student of Computer Engineering at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. She is interested in java programming.

Snehal M. Baviskar she is student of Computer Engineering student at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. She is interested in Cloud Computing.

Vandana N. Chalwadi she is student of Engineering student of Computer Engineering at Brahma Valley College of Engineering And Research Institute, Nasik under University of pune. She is interested in the field of java programming.

K. S. Kumavat, ME, BE Computer Engg. Was educated at Pune University. Presently she is working as Head of Information Technology Department of BVCOE & RI, Nasik, and Maharashtra, India. She has presented papers at National and International conferences and also published papers in National and International Journals on various aspects of Computer Engineering and Networks. Her areas of interest include Computer Networks Security and Advance Database.