ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 8, August 2015

KEY DISTRIBUTED CENTERS PREVENT UNAUTHORIZED USERS ACCESSING CLOUD STORAGE

S.Reshma[1], A.Vijaya[2]
[1]Assistant Professor, Dept. of CSE, S.V.Engineering College for Women, Tirupati, AP, India.

[2]M.Tech CSE Student, S.V.Engineering College for Women, Tirupati, AP, India.

ABSTRACT

Every day, millions of users are accessing the cloud storage through some interfaces. Among them, some are cloud tenants and other were new/unknown users they may request for different types of resource usage. But the cloud has to verify their series of authorization before offering the service to the requested users. Here our new proposal concentrated to protect an individual person's privacy and right to respond/report on illegal activities to higher officials. The cloud is not in a position to reveal the posted persons identities when authorized user request for posted person's details, but it shows the posted content only. Along with these it allows only the authorized users to decrypt the encrypted stored data in clouds based on their privileges. Apart from these it avoids repeated attacks and it allows an authorized person to create, update and read the information from storing data. To perform this whole operation. It becomes a headache process to the cloud, for this we separately maintain a new designed architecture called the Key Distribution Center (KDC) to check all these things, and also enables the process to avoid repetitions of the cloud storage at same time.

Keywords: Attribute based encryption, Attribute based signature, Cloud storage.

1. INTRODUCTION

Cloud computing is the concept of extending the resources and infrastructures that enables cloud services to all the users with the "pay only for use" way. This kind of cloud computing technology that serves users to handle the resources in better way. The real time benefits of cloud are extensively, the critical in the current information service outsourcing scenario is the enforcement of security scheme for data storage, data transmission and also handling in the cloud.

The cloud information is often complex in nature. These kind of data are used for health records and user-determined data made in social websites are stored in public or private clouds. Enabling privacy and security of those data is vital for users to reliable the network services. To acquire those, arequired authentication and access policy mechanisms are essential to

be used. The majority of the security system too confirms that only checked and valid services are given to authorized users. The procedure of authentication will be originated to all valid data operations can be performed using cloud.

The significant objective of this work is to implement unknown user authentication of users. In this, the discussion is on the anonymous authentication of users then highlights its significance. Confidentiality preserving setup of users must be considered in such a way that the identity of the user shouldn't become the proof to either the cloud service providers or others. Hence the anonymous access of users is conserved.

In order to make the cloud data storage secure, the data needs to be encoded. And also the cloud should have the data privacy and security to achieve this many homomorphism techniques. While doing encryption, enables that many computations are performed on the cloud services, where the suitable available to encode before encrypted process.

As Cloud has versatile usage in internet. Hence the cloud is disposed to to malfunction and attacks. Service providers should provide trustful and intermittent services to users by providing actual and effective accessing of data and storage mechanisms. Another aim is to improve the accessibility of cloud services. Wang et al. addressed the issue of secure and trustworthy cloud storage. They specially conferred in the concept of Byzantine failure, where the storage servers failed in arbitrary ways leading to data updatation and loss. Hence the working concept of avoiding traffic and allow others to continue in doing transactions like downloading repeatedly same file.

2. RELATED WORK

In the decentralized system architecture, maintaining many KDCs for the key generation is helpful in achieving the security and data preserving. Distributed way of access control in cloud data stored can allow access to the users with valid attributes only. Access control mechanisms are provided to achieve privacy preserving as well as to authenticate the accessed users whoever stores update data based on access privileges provided in the system.

ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 8, August 2015

3. DECENTRALIZED SYSTEM ARCHITECTURE

In this approach, privacy preserving authenticates the user access control mechanisms. Based on the method the user can able to prepare a file and store safely in the cloud storage. Here in this mechanism exists with the use of the two mechanisms ABE for encryption and ABS for validation that are followed.

The user Alice gets a token from the trustee, who is the creator, where the trustee is the authority that enables to take care all the important user information. Then the trustee checks the user is authorised or not, based on that the token is provided. There are multiple KDCs, which can be placed apart. These can be served various locations anywhere in the world.

The creator on providing the token to one or many KDCs that gets keys for encryption or decryption and signs it. In the Figure 1 below, SKs are secret keys given for decryption, K_x keys for signature. The message MSG is encoded using the access mechanism ɣ. Based on the access policy mechanism; the system decides who are authorized to right to access the data available in cloud system. The creator selects a appropriate claim policy ɣ, to prove the authentication and sign of the message against this claim policy. The cipher text C with sign is c, and is sent to the cloud system. The cloud verifies the sign and stores the cipher text C. If the reader required to read, the cloud provide C. If the user has matching attributes with access policy, it can decryption process takes place and gets the original data message. Write transaction continues in the same way as file creation. By assigning the verification process to the cloud, it releases every user with more time required for verification. If the reader desires to read some data stored in the cloud, it proceeds with decryption of data using the secret keys and those are receives from the KDCs. Check whether it has required attributes matching with the access policy ɣ, then decryption process takes place for the data available in cloud.

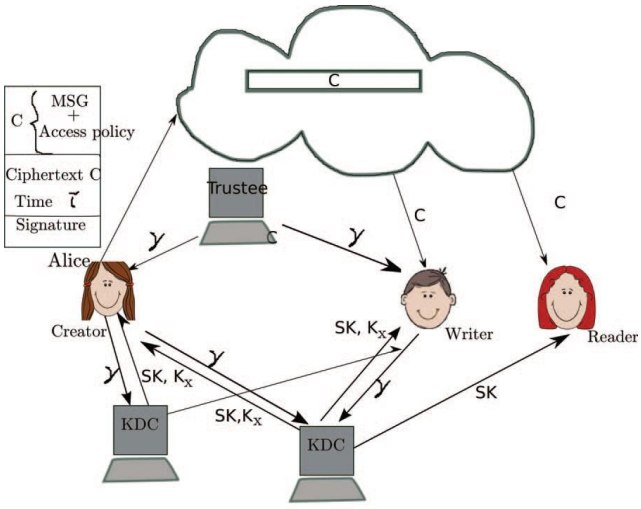

Figure 1: Cloud Storage Model with multiple KDCs

Symbols	Computation
ɣ	Token from the trustee
SK	Secret key for KDC.
K_x	K_x are keys for Signatures
C	Ciphertext
MSG	Message from user

4. PRIOR WORK

The centralized system prototype implements single key from the Key Distribution Center (KDC) and also by applying security schemes. Many available flows discuss regarding the centralized access control schemes. However application of a single KDC model is flexible, nevertheless that have various major problems:

4.1 One of the major problems is that of single point failure which is not at all desirable to proceed in a cloud system in which there are huge users those are actively accessing.

4.2 An important overhead available since a single KDC is utilized to issue secret keys and user attributes to all the cloud users.

4.3 According to the mentioned problems, a decentralized cloud mechanism that is focused in which the task of key management is made by the multiple KDCs. The Decentralized system architecture is for distributed key management. Hence, this scheme, access policies defined by a user from others of the data file. Thus, the access privilege's connected with individual users are exposed from the cloud.

4.4 Abbreviations and Acronyms

Abbreviations	
ABE	Attribute Based Encryption
ABS	Attribute Based Signature
KDC	Key Distribution Centre
RBAC	Role Based Access Control

5 SYSTEM ARCHITECHTURE

5.1 ACCESS CONTROL TECHNIQUES

The access control techniques that are to be followed for the decentralized Access control.

A. **ABE:** Attribute-based encryption systems used attributes To Describes the encoded data and develop the policies into user's keys; while in our system attributes are used to describe a user's login credentials, and a party encrypting data states that the policy for those can decrypt.

B. **ABS***:* A extensive primitives that allows a group to sign a message with fine-grained control over identifying information. In ABS, a signer, who avails a bunch of attributes from the authority, can sign a message with a predicate values that is satisfied by his attributes. The signature provides no more than the evidence that a single user with few set of attributes satisfying the predicate has attested to the data message. In particular, the signature hides the attributes used to satisfy the predicate and any identifying information about the signer. Furthermore, users are not colluding to pool their attributes combined.

In our proposed system, we try to implement the Role Based Access Control (RBAC) prototype. We chose the RBAC access control technique where users are categorized based on the task and the access policies are created accordingly. The application of anonymous authentication in RBAC is a significant and critical mechanism and formed a new set of secured crypto graphical methods in a cloud system.

There is a centralized process controls that specifies the organization for interaction between "subjects" and "objects".

The subjects are items to which execution can be attributed such as users, processes, threads, or even methods activations. Objects are items on which transactions are created including storage concepts such as memory or files with read, write, and execute transactions and code abstractions, such as components or services with transactions to initiate or stop execution. Different privileges are associated with distinct operations on dissimilar objects.

In the existing process that allows the registered cloud users to download the data from the cloud, the user validation is done and also followed with the process that the user enters the key, generated from KDC. And the key validation is done along with the user attribute details. This verification will be done at the server. Once the server allows the file to download, the file will be downloaded.

5.2 In the Table.1, the comparison specifies that the differentiation in the number of schemes for access control with the scheme proposed by us. All the access control schemes are specified with Write (W), Many users (M) and Read(R) in detail.

It is quite evident that our decentralized scheme given in the last row is powered by the maximum number of features.

It has multiple read and multiple write access, homomorphism encryption and performs the anonymous authentication all over while hiding user attributes.

Table 1: Differentiation of Schemes

Centralized / Decentralized	Write / read access	Type of access control	Privacy preserving authentication	User revocation ?
Centralized Cloud	1-W-M-R	Sysmmetric key cryptography	No	No
Centralized Cloud	1-W-M-R	ABE	No	No
Centralized Cloud	1-W-M-R	ABE	No	No
Decentralized Cloud	1-W-M-R	ABE	No	Yes
Centralized Cloud	1-W-M-R	ABE	No	No
Decentralized Cloud	1-W-M-R	ABE	No Privacy preserving	Yes
Centralized Cloud	M-W-M-R	ABE	Authentication Success	No
Decentralized Cloud	M-W-M-R	ABE	Authentication Success	Yes

6 SYSTEM IMPLEMENTATION

In the proposed process, we are trying to introduce the idea of reducing the contact of cloud servers for every validation. Which implicitly implements the privacy preserving authentication scheme? As we already know that the ABE and ABS schemes are used as part of the model. The model describes as in the Figure 1, when the user requested for an operation on cloud, the secret keys are generated which are given for he decryption. And the K's are the keys, where the data is decrypted based on the access policy.

According the access policy, we will come to know which data is store or retrieved from the cloud storage. The creator had the right to define the claim policy to prove the access policy as well as signature of the message. The cipher text C with signature is c, and is sent to the cloud. The cloud validates that sign and saves the ciphertext C. When a reader wants to read, the cloud sends C. If the user contains matching attributes along with the access mechanisms, it can decrypt and gets the previously available original message. Write also works in the same fashion as in file creation. By assigning the verification process in cloud, it releases every user with more time required for verification. If the reader wants to read some data stored in the cloud, it proceeds with decryption of data using the secret keys and those are receives from the KDCs. If it has required attributes matching with the access policy ϒ, then decryption process takes place for the data available in cloud.

.

6.1 Process or Retrieve of data stored in cloud

As the user first registered in the cloud, the trustee provides a token. Then the message encrypted in based on the access policy.

C= ABE. Encrypt (MSG, χ), where χ is the access policy that determined while creation. When the user tries to download the data from the cloud, the user validation is done and also followed with certain process to reduce the access the cloud server several times for the same purpose. This way we can

achieve more users without hampering the other traffic. The process can be done as follows.

A. An user tries to download a file which is already Downloaded earlier, user should be able to provide the indication to proceed further to download or not. This way, the user can be allowed to access the same data from the cloud can be restricted for the time being with time stamp and can be allowed for doing the same later.

B. If the user tries to download file for the first time, the user will be provided with the key from the KDC to authenticate.

Once the user enters the key, the KDC validate the key. While doing this process. Instead of the validation and verification done by the server, the KDC will tag the file with the "Tag" which is the tag name for the file that is to be downloaded. The tag contains the required information to validate the user and also decryption process. This whole process validation is done at the client side (at KDC level) without contacting the server. Hence, the key applied, and the client program is responsible to perform the decryption process.

7 RESULT

With the approach of the proposed mechanism achieved the change in the result will be same whereas the authentication and validation done at the KDC itself. Hence, we can say that the traffic is reduced and allows other anonymous user for performing their transaction by providing a delay for the repeatedly accessing cloud storage. With this the performance of the system is increased as well as server processing burden is reduced.

REFERENCES

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access
Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing,"IEEE Trans. Services Computing, vol. 5, no. 2, pp. 556-563, 2012

[3] S. Bharath Bhushan, Pradeep Reddy, Dhenesh V Subramanian, X. Z. Gao, "Systematic Survey on Evolution of Cloud Architectures", International Journal of Autonomous and Adaptive Communications Systems, Inderscience, 2015

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[5] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992.

[6] 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, June 2010.

[7] 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," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.

[9] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[10] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation,"Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.

[11] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

[12] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access
Control for Multi-Authority Cloud Storage Systems," IACR Cryptology ePrint Archive, p. 419, 2012.

[13] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.

[14] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M.Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.