An Attribute Based Encryption for Accessing Data on Cloud

Avinash N
Student M.Tech, Department of CSE
Sai Vidya Institute of Technology
Bangalore, India

Divya C
Assistant Professor, Department of CSE,
Sai Vidya Institute of Technology
Bangalore, India

***Abstract*—Whenever an access control is being considered on cloud, there exists a mechanism to reduce the common overhead of the internet and to provide a fine-grained access control. An attribute based encryption can be used to address these issues. In the existing system a centralized attribute based encryption is proposed, where there is a single key distribution centerto distribute secret keys and attributes to the users.In this paper a decentralized attribute based encryption mechanism is proposed, in which any party will act as authority by creating a public key and issuing private key to different users. The proposed mechanism also supports the features of anonymous authentication and user revocation. It is also possible to compare the performance between attribute based encryption and decentralized Ciphertext attribute based encryption.**

Keywords- Access control, Key Distribution Center (KDC), Authentication, Revocation, Attribute Based Encryption(ABE).

I. INTRODUCTION

Cloud computing is a promising computing model which hascurrently drawn far reaching consideration in all fields. Now a day’s companies are able to purchase the computing resources which are needed from many cloud service providers instead of establishing and maintaining their own computing environment.Much of the highly sensitive data is stored on clouds. The very important issues in cloud computing is security and privacy. On one hand the user should be authenticated before initiating transaction,and on the other the user should be ensured that the cloud does not tamper the outsourced data. The privacy of the user is required, so that other users or cloud don’t know the identity of the user.

Access control on clouds is gaining attention on clouds because it is important that access to the valid service can be accessed only by authorized user. A huge amount of data and information is stored on clouds, and much of this has more sensitive data information. Access control are broadly divided into three types: Role Based Access Control (RBAC) [2], UserBased Access Control (UBAC), and AttributeBased Access Control (ABAC) [1]. In Role Based Access Control, based on individual roles users are classified. In User Based Access Control, the access control list contains the authorized users list to access data. In ABAC, attributes are given to users, and access policyis attached to the data, the users who have valid set of attributes and satisfy the access policy can access the data.

In existing scheme such as Fine-Grained Data Access Control[3], Attribute Based Data Sharing[4], Hierarchical Attribute Based Encryption[5], Distributed Access Control[7] access controls on cloud are centralized in nature and also uses a symmetric key approach, where only one key distribution center (KDC) distributes attributes and secret keys to all users. As large number of users are supported on a cloud environment a single KDC is very difficult to maintain. In this paper the added feature is that it enables the authenticity and validity of the message without revealing the user identity whohas stored information on the cloud,andthis scheme can also be extended to user revocation. In this paper, Attribute Based Signature(ABS)[8] schemeis used to achieve authenticity and privacy. This scheme is also resistant to replay attacks wherethe fresh datacan be replaced with stale data by users. This scheme is an important property because a user who has been revoked will not be able to write to the cloud.

To accomplish secure data transaction on clouds, appropriate cryptography technique is utilized. The data possessor should encrypt the record then store the record on the cloud. Assuming that the recordis downloaded by a third person, the user can see the record if that, they had the key that is utilized to rewrite the records which is encrypted. Once in a while because of the programmers and the technology improvement this might be failure. To overcome the problem there's lot of procedures and techniques to form secure transaction and storage.

Sushmitha Ruj et.al[15] proposed an anonymous authentication for data archiving to clouds. Anonymous authentication is a procedure of in which accepting the user without the details of the user. So the cloud servers does not know the details of the user, which gives security to the user to conceal their details from other users of that cloud.

II. RELATED WORK

Access control[9] in clouds is gaining consideration and is important so that only authorized users have access to cloud services. A huge amount of data is constantly archived on the cloud and much of this has more sensitive data. By using Attribute Based Encryption, the records are encrypted under access policy strategies and are saved on the clouds. Users are given sets of corresponding keys and traits. When the user has matching set of attributes, User will be able to decrypt the data saved on the cloud.

F. Zhao et.al [6], proposed privacy preserving authenticated access control in cloud. Here, the researcher'sconsiders a centralized methodology where single key distribution center (KDC) disperses attributes and secret keys to all users. But a single key distribution center is justnot a single point of failure and it is also very difficult to maintain vast number of users on clouds. ABS scheme was introduced by H.K. Maji et.al[13], to ensure anonymous user authentication but it was a centralized approach.

Recent scheme by H.K. Maji et.al[8] proposed decentralized approach which provides authentication without disclosing the users identity but it is prone to replay attack.A. Sahai and B. Waters[14] proposed Fuzzy Identity-Based Encryption, that consists of one fully trustworthy centralized authority (CA) and multiple attribute authorities. Each user is assigned a unique global identifier and also the keys from different authorities are bound together by this identifier to counteract the collusion attack multiple users can pool their secret keys obtained from different authorities to decrypt a ciphertext that they are not individually entitled.

Kan Yang et.al[11] proposed A decentralized approach and this strategy doesn't assure about users, who need to stay anonymous while accessing the cloud. On the other hand, the approach failed to provide user verification. S. Ruj et.al[7] have proposed distributed access controls module on clouds. In this approach user verification was not provided. The other weakness was that users can create and store a record and different users can simply read the record. Write access was not allowed to users other than originator.

Perlman[12] proposed Time-based assured deletion that was conferred earlier which implies that records can be safely erased and stay forever tough to reach after a predefined time. The first thought is that the possessor encrypts records with an information key of the records and this information key is encrypted further with a sway key by a separate key Manager.

III. PROPOSED SYSTEM

Data stored on cloud follows Distributed access control scheme so that users who are authorized and with valid attributes can access the data. Authentication of users performs store and modification of the data in the cloud. During authentication the users identity is protected from the cloud. The cloud architecture is decentralized, which means that key management can be done by several KDCs. Both access control and authentication schemes are collusion resistant. The collusion resistant attack means that no two users can collude and authenticate themselves or access data, even though they are not individually authorized. Users who are revoked cannot access data after he/she have been revoked. The proposed scheme is flexible to replay attacks. This proposed protocol also supports multiple writes and reads on the data stored on cloud. The costs of decentralized approach should be less comparable to the existing centralized approaches.

IV. PROPOSED ARCHITECTURE

The architecture of proposed system depicted in Fig.1. There are three users, a creator, a writer and reader. Creator Alice who is assumed to be honest receives a token from the trustee. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id social insurance number/ like health etc., the trustee gives her a token. There are multiple (here 2) KDCs, which can be scattered. These KDCs can be servers present in different parts of the world. A creator receives keys for encryption/decryption and signing on presenting the token which is received from trustee to one or more KDCs. In the Fig. 1, secret keys (SK) are given for decryption; the keys are *Kx* for signing. Under the access policy X the message MSG is encrypted. The access policies decide who can access the data stored on the clouds. On a claim policy Y the creator decides, to prove her signsand authenticity ofthe message. The cipher text C with signature is sent to the cloud. The cloud by verifying the signature stores the cipher text (C).If a reader wants to readdata the cloud sends cipher text C. The cipher text C can be decrypted and can retrieve back the original message if the user has matching set of attributes with access policy.

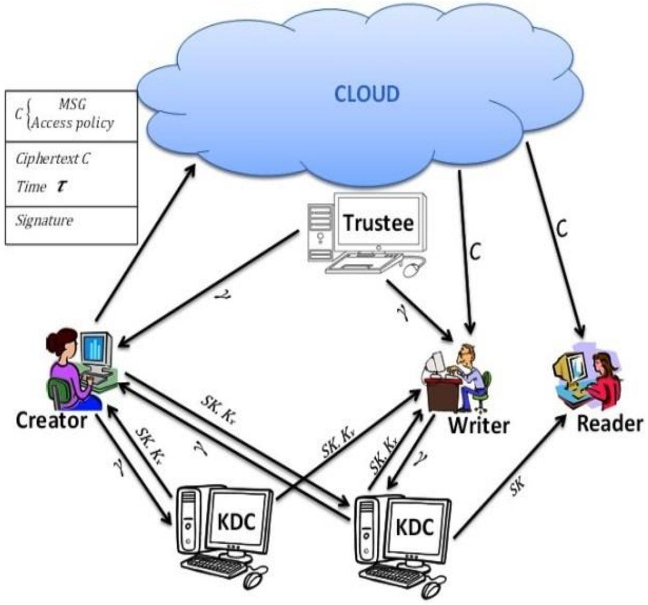

Figure 1: Cloud Architecture

A. *Attribute-Based Encryption*

The attributebased encryption concept was first proposed by A. Sahai and B. Waters[14]. ABE is a type of public-key encryptionis in which the ciphertext andsecret key of a user are dependent upon attributes. A crucial security feature of ABE is collusion resistance, an opponent holds multiple keys should alone be able to access data and information if at least single individual key grants access.In ABE the ciphertext decryption is possible only if the valid set attributes of the user key matching the attributes of the ciphertext.The ABE consists of four algorithms as follows

System Initialization

Select a prime q, generator g of G_0, groups G_0 and G_T of order q, a map e : $G_0 X\ G_0 \rightarrow GT$, and a hash function H : $\{0,1\}^* \rightarrow G_0$ that maps the identities of users to G0. The hash function used here is SHA-1. Each KDC Aj ϵ A has aset of attributes L_j. Each KDC also chooses two random exponents.

Key Generation and Distribution

User U_u receives a set of attributes I[j,u] from KDC A_j, and corresponding secret key $SK_{i,u}$ for each iϵI[j,u]. Where $\alpha_i, y_i \epsilon SK[j]$. Note that 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.

Encryption

In the encryption function by using the method ABE the message MSG is encrypted with the access policy X and the encrypted message which isciphertext C is sent.

Decryption

In the decryption function the ciphertext C is decrypted by using the secret key SK to obtain the original message MSG.

B. CP-ABE System

A decentralized CP-ABE system is composed primarily of a set of *A* authorities, a trusted initializer and users. The only responsibility of trusted initializer is generation of system global public parameters that are system wide public parameters available to each entity in the system. During system initialization, every authority $A_j \epsilon A$ controls a different set U^j of attributes and issues corresponding secret attribute keys to users. It has been observed that each authorities can work independent. As such, each authority is totally unaware of the existence of the other authorities in the system. In the system every user is identified with a unique global identity ID ϵ {0,1} and allowed to request secret attribute keys from the various authorities. In the system at any point of time, every user with global identity ID possesses a set of secret attribute keys that reflects a set L_{ID} of attributes, that we call an attribute set of the user with identity ID. Let $U_{Aj\epsilon A}U^j$, where $U^{j1} \cap U^{j2} = \phi$, for $j_1 \neq j_2$ be the attribute universe of the system. As a result of lack of global coordination between authorities, different authorities might hold identical attribute string. To overcome this, we can treat every attribute as a tuple consisting of the attribute string and also the controlling authority identifier. The decentralized CP-ABE consists of five algorithms

System Initialization(k): Initially, according to the security parameter *k* a trusted initializer choses global public parameter GP. Any user or any authority in the system can make use of these GP in order to perform their executions.

Authority Setup(GP, U^j): Once during initialization every authority $A_j \epsilon A$ runs this algorithm. It accepts global public parameter GP and a set of attributes U^j as input and outputs public key $PubA_j$ and master secret key MkA_j of the authority A_j.

*Authority KeyGen(GP,ID,a,MkA_j):*On receiving a secret attribute key request from the user every authority executes this algorithm. It takes global public parameter GP, global ID of a user, attribute *a* hold by authority and the master secret key of the corresponding authority as input and it returns a secret attribute key $SK_{a,ID}$ for the identity ID.

*Encrypt(GP,M,A,{$PubA_j$}):*An encryptor runs this algorithm and takes global public parameter GP, an access structure, message M to be encrypted and public key of relevant authorities corresponding to all attributes as input. Then it encrypts message M under access structure and returns the CT ciphertext.

*Decrypt(GP,CT,{$SK_{a,ID}$|aϵL_{ID}}):*Decryptor with identity ID runs this algorithm on receiving ciphertext CT by inputting GP, CT and {$SK_{a,ID}$|aϵL_{ID}}. Then it outputs the message if the user attribute set L_{ID} satisfies the access structure, if not satisfies decryption fails.

V. CONCLUSION

In this paper a mechanism called decentralized access control technique with anonymous authentication has been presented, that provides prevents replay attacks and user revocation. The identity of the user who stores data and information is not known by cloud, but only user credentials are verified. The distribution of keys is done in a decentralized way which hides the access policy and attributes of a user. Further, the performance between attribute based encryption and decentralized attribute based encryption can be compared.

REFERENCES

[1]. D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls" Proc.15th National Computer Security Conference, 1992.

[2]. E.J. Coyne, D.R. Kuhn and T.R. Weil, "Adding Attributes to Role-Based Access Control" IEEE Computer, vol. 43, no. 6, pp. 79-81,June 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" Proc. Sixth International ICST Conference Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

[4]. 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.

[5]. G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services" Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

[6]. F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems" Proc. Seventh International Conference Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.

[7]. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th International ICST Conference Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

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

[9]. S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation" in *ACM ASIACCS, 2011.*

[10]. F. 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, 2011.*

[11]. Kan Yang, Xiaohua Jia and Kui Ren, " DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems" *IACR Cryptology ePrint Archive*, 419, 2012.

[12]. Perlman, "File System Design with Assured Delete," *Proc.Network and Distributed System Security Symp. ISOC (NDSS), 2007.*

[13]. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance" IACR Cryptology ePrint Archive, 2008.

[14]. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption" Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[15]. Sushmita Ruj, Milos Stojmenovic and Amiya Nayak,"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" *IEEE Transactions On Parallel And DistributedSystems*