PRIVACY PRESERVING OF STORED DATA IN CLOUD USING DAC AND KEYPOLICY ABE

K. S. Chandrasekaran, A. Abinaya, S. Femina, A. Harshapradhai, S. Sahithya
Saranathan College of Engineering, Trichy 620 002, TamilNadu, India

***Abstract*- We propose a Decentralized Access Control mechanism using ABE and ABS Algorithm for anonymous authentication of data. Only valid user can perform decryption of data. This mechanism prevent replay attack and support creation, modification and reading data stored in a cloud. The proposed scheme is decentralized, robust and user privacy is the key requirement so that other users do not know the identity of the user.It should be ensured that users must not have the ability to access data even if they possess matching set of attributes.This method make use of key policy attribute based encryption for security purpose.**

I. INTRODUCTION

Cloud Computing is a model for enabling ubiquitous, convenient, on demand-network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. In recent times, cloud storage has become one of the most common and affordable ways to store share or back up digital data to a secure location. The data in these remote storage locations can be easily accessed at any time, from anywhere by the users and individuals around the world. Cloud technology lets you to do more and you can play around with your files without consuming any space on your computer’s hard drive or server network.

Cloud storage providers also serves as a backup service to make sure that not a single file goes missing due to any unwanted issue, for instance a hard drive failure, corruption or viruses. At the moment, companies are also on the lookout for unique services suitable to store all official documents safely, spend less on storage appliances and also provide the client documents to their staffs and employees anywhere in the world.

To be precise cloud storage is basically a technique to store, coordinate and protecting the essential data in a virtual cloud that can be readily accessed by multiple users. The users must have to be authorized on a particular network and they can access the data storage from anywhere at any time.

The general concept on how cloud storage works is that data is stored by a third party at a remote location. These service providers have various plans depending on the amount of storage one needs for his computer. Data gets transmitted through internet and the users can have access to their stored data readily regardless of their location via internet. The entire process of cloud storage can be broadly explained from two points of view – the role of the service provider and the role of the consumer. The basic role that a cloud storage provider plays in this process is to regulate a base of storage located at several discrete sites. It’s a simpler and easier way to keep your data stored on cloud storage, since the monitoring techniques and administrative control is far better that any other storing approaches. In a cloud storage, there are thousands of separate servers that are mutually connected in a grid configuration. This is how the entire system works as an individual directory.

A form of cloud storage where the enterprise and storage service provider are separate and the data is stored outside of the enterprise's data centre. With public cloud storage, or external storage clouds, enterprises and small businesses offload their data storage and archival/backup needs to a third-party cloud storage service provider, freeing them from the expensivecosts of having to purchase, manage and maintain on-premises storage hardware and software resources.

In most cases, public cloud storage can also be deployed much faster and with more scalability and accessibility than on-premises data storage. In addition to that storing static data, public cloud storage services can often store live data generated by applications running on a company's on-premises resources.

II. PRELIMINARY

OwnerModule:Owner module is to upload their files using some access policy. First they get the public key for particular upload file after getting this public key owner request the secret key for particular upload file. Using that secret key owner upload their file.

User Module: This module is used to help the client to search the file using the file id and file name .If the file id and name is incorrect means we do not get the file, otherwise server ask the public key and get the encryption file. If u want the decryption file means user have the secret key.

Distributed Key Policy Attribute Based Encryption:KP-ABE is a public key cryptography primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized. The encryptor associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access structure. The proposed scheme consists of four algorithms which is defined as follows

Setup:

This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.

Encryption:

It takes a message, public key and set of attributes. It outputs a cipher text.

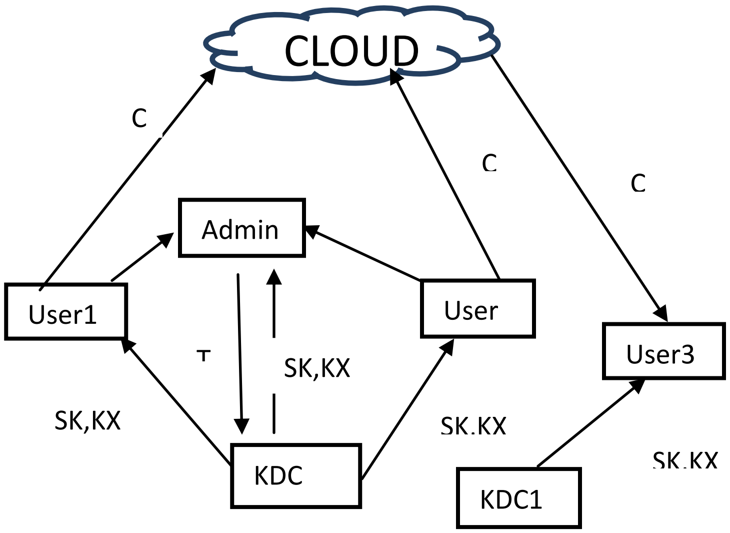
Key Generation: It takes as input an access tree, master key and public key. It outputs user secret key.

Decryption: It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

File Assured Deletion: The policy of a file may be denied under the request by the customer, when terminating the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The point when any of the above criteria exists the policy will be repudiated and the key director will totally evacuates the public key of the associated file. So no one can recover the control key of a repudiated file in future. For this reason we can say the file is certainly erased. To recover the file, the user must ask for the key supervisor to produce the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is verified by means of an attribute connected with the file. With file access control the file downloaded from the cloud will be in the arrangement of read just or write underpinned. Every client has connected with approaches for each one file. So the right client will access the right file. For making file access the key policy attribute based encryption.

III. DETAILED PRESENTATION

In this project we are particularly interested in providing privacy and security data stored in cloud using ABE and ABS algorithms for decentralized access control (i.e.) any of the authorized user can access the data present in the cloud. ABE stands for Attribute Based Encryption in which the data stored in the cloud would be in encrypted format or ciphertext. Here the encryption is based on user attributes like user id. ABS stands for attribute based signature. This is for authentication purpose. To create or modify the cloud data, the authorized user gets token (i.e.) signature from the admin. Admin is same as that of certified authority. With the token, admin approaches the KDC to get key for the authorized user. Key transformation takes place. The KDC generates key to the admin which in turn provide the key to the authorised user. With the encrypted key, the user can access the cloud.



The user approaches the admin to access data in the cloud. The admin checks for authentication. If user is authorized, the admin will generate a token to the KDC, with that token the KDC will generate key to the admin which in turn is given to the user. With that the key the user access data in the cloud. Similarly, for writing data in the cloud, the user is checked for authentication. In this way user can read, write and update data present in the cloud.

IV. ALGORITHMS USED

ABE: Traditional access control techniques are based on the assumption that the server is in the trusted domain of the data owner, and therefore an omniscient reference monitor can be used to enforce access policies against authenticated users. However, in the cloud computing paradigm this assumption usually does not hold, and therefore these solutions are not applicable. There is a need for a decentralized, scalable, and flexible way to control access to cloud data without fully relying on the cloud service providers.

Data encryption is the most effective in regard to preventing sensitive data from unauthorized access. In traditional public key encryption or identity-based encryption systems, encrypted data is targeted for decryption by a single known user. Unfortunately, this functionality lacks the expressiveness needed for more advanced data sharing. Instead of encrypting to individual users, in ABE system, one can embed an access policy into the ciphertext or decryption key. Thus, data access is self-enforcing from the cryptography, requiring no trusted mediator.

ABE can be viewed as an extension of the notion of identity-based encryption in which user identity is generalized to a set of descriptive attributes instead of a single string specifying the user identity. There are two types of ABE depending on which of private keys or ciphertexts that access policies are associated with. In a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are labelled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures an policy (also called the access structure) that specifies which type of ciphertexts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. For example, in a secure forensic analysis System, audit log entries could be annotated with attributes such as the name of the user, the date and time of the user action, and the type of data modified or accessed by the user action.

While a forensic analyst charged with some investigation would be issued a private key that associated with a particular access structure. The private key would only open audit log records whose attributes satisfied the access policy associated with the private key. The system was proved selectively secure under the Bilinear Diffie-Hellman assumption.

ABS: We introduce Attribute-Based Signatures (ABS), a versatile primitive that allows a party to sign a message with fine-grained control over identifying information. In ABS, a signer, who possesses a set of attributes from the authority, can sign a message with a predicate that is satisfied by his attributes. The signature reveals no more than the fact that a single user with some set of attributes satisfying the predicate has attested to the message. In particular, the signature hides the attributes used to satisfy the predicate and any identifying information about the signer (that could link multiple signatures as being from the same signer).

RSA:RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of an integer is hard (the factoring problem). RSA stands for Ron

Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

V. CONCLUSION

In order to protect the data stored in the cloud we use authentication and access control algorithms. It also performs multiple read and write operations and prevent replay attack.The scheme prevents replay attacks and supports creation, modification and reading data stored in the cloud. It also addresses user revocation.Our project can be successfully implemented in a variety of domains including ERP, Banking, hospital, etc.,

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-
563, 2012.

[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. 220-232, Apr.-
June 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy
Keyword Search Over Encrypted Data in Cloud Computing,”
Proc. IEEE INFOCOM, pp. 441-445, 2010.

[4] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc.
14th Int’l Conf. Financial Cryptography and Data Security, pp. 136-
149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication
for Cloud Computing,” Proc. First Int’l Conf. Cloud Computing
(CloudCom), pp. 157-166, 2009.

[6] C. Gentry, “A Fully Homomorphic Encryption Scheme,” PhD
dissertation, Stanford Univ.,
http://www.crypto.stanford.edu/
craig, 2009.