Public Auditing for Data Stored on Cloud with Decentralize Access Control

Rachana Jadhav[1], Shital Gavahane[2], Pratima Kumari[3], Aparna Bharate[4], A. J. Jadhav[5]

[1234]Student, Dept. of Information Technology, RSCOE, Pune, India
[5]Professor, Dept. of Information Technology, RSCOE, Pune, India

---***---

Abstract — *Cloud computing is a vital area which permits user to remotely store their information into the clouds and can get to when required. So here, security and privacy are extremely essential things. The user should to validate him/her before beginning any transaction and user privacy is likewise vital so that the cloud or different users in cloud don't know the identity of the client who stores the information. This is an entrance control system for information put away in clouds that gives anonymous verification. In this scheme, the cloud validates the users without knowing the users identity before using so as to put away information in the cloud ABS (Attribute-Based Signature). This scheme has the feature of access control in which just legitimate users can decrypt the put away data by utilizing ABE (Attribute-Based Encryption). The scheme helps to restrict attacks and permits uploading, modification, downloading of information stored in cloud. Quite a bit of information stored in cloud is sensitive so this framework is effective. The System also provides integrity checking of data with the help of TPA. The system can be utilized for different applications, for example, storing health care data, in online social networking, where users store their own data and share with chose groups of clients or communities them relative in with. It likewise handles user revocation.*

Key Words: Authentication, Attribute Based Signatures (ABE), Cloud Storage, Attribute Based Access Control, Authentication, Attribute Based Encryption (ABS), Third Party Auditor (TPA).

1. INTRODUCTION

Today because of the advances in networking technology and an expansion in the requirement for computing resources have provoked numerous organizations to outsource their storage and computing necessities. This novel economic and computing model is usually referred to as cloud computing and incorporates different types of services, for example, infrastructure as a service (IaaS), where a client makes utilization of an service suppliers computing, storage or networking infrastructure; platform as a services (PaaS), where a client influences the suppliers resources to run custom applications; lastly software as an service (SaaS), where clients use software that is keep running on the suppliers infrastructure.

It is vital thing to save the security of information and privacy of users. Cloud should to guarantee that the users attempting to get to information and services are approved users. Validation of users can be accomplished utilizing public key cryptographic methods. Users should to guarantee that the cloud is not tampering with their information and computational results. It may likewise be vital to hide the user's identity for privacy reasons. For instance, while storing medical records, the cloud should not have the capacity to get to records of a specific patient, given the specific identity. Users should likewise guarantee that the cloud can perform calculations on the information, without knowing the information values. One approach to hide the information from the clouds, however bear on calculation on the information, is by the utilization of homomorphic encryption systems [10]. User sends homomorphic encrypted messages, while the cloud without knowing the genuine information performs calculations on these encrypted messages and returns the outcomes to the user.

Consider now the accompanying circumstance. Patients store their medical records in the cloud. Distinctive users can get to various information fields. Here the same information fields may be gotten by a specific group of peoples which is approved set. For instance the patient's medical history and drug administration can be gotten by doctors and nurses, yet not by hospital administration staff.

In online social networking , for the most part proprietors are members from the networking website, they keep their own details, pictures, music videos in the cloud and different members can see them relying on their entrance rights. A member can post a message or transfer a photo whenever, which will be noticeable just to the friends and certain selected groups that she has a place with yet it is not accessible to the rest. It is essential to likewise privacy of this information from the cloud. Giving access rights to some approved users and keeping different users from getting to the information, is called access control. One approach to accomplish this is to join a list of every legitimate user to the information called as user based access control. In cloud computing, such records can be much long and frequently progressive, which will make taking care of such records to a great degree troublesome. Every time the list must be verified whether the user is authenticated or not. This outcome in huge storage costs. Another approach to encrypted information is by utilizing public keys of authenticated users, so that just they can decrypt information utilizing their secret keys. However the same information then should be encoded a few times exclusively for every user, which might bring about enormous storage costs. Subsequently here it is valuable to utilize the cryptographic procedure called Attribute Based Encryption (ABE) [4] to accomplish access control in clouds. Utilizing ABE, proprietors encrypt information with qualities that they have and store the data in the cloud. The cloud is not ready to get store information. Users are given properties and secret keys by a key appropriation focus i.e. KDC. Those with coordinating set of attributes can decrypt the data. For instance, in public health records repository [5], the medical records contain history of the patients and may be gotten to either by medical experts (doctors and nurses), researchers and academicians or administration authorities, for example, insurance agencies and government policy creators. Various peoples are permitted to get to various records. Every user is given properties, for example, the association (hospital names), designation (occupation and specialization) etc. For instance, just a psychiatrist or neurologist in Hospital P or Q will have the capacity to get the record, the medical history of a bipolar person. Some other user, for instance a hospital staff of hospital P or Q, or a neurologist from Hospital R, won't have the capacity to get to the record.

The system uses Third Party Auditor, which performs the integrity of data stored in the cloud on behalf of user request. So here, we are having public audit ability for cloud storage that users will resort to a third-party auditor (TPA) to ascertain the integrity of information. Here, this paper provides the varied problems associated with privacy whereas storing the user's knowledge to the cloud storage throughout the TPA auditing.

The paper is organized as; section 2 contains information about related work. Section 3 contains implementation details which includes system architecture, systems overview, mathematical model, algorithms and experimental setup. The section 4 contains results and discussion of the proposed work done so far. The last section 5 contains the conclusion of research work done. At the end various references are mentioned which are used in this paper.

2. RELATED WORK

Here first think of some as existing plans. Fluffy IBE [9] offers rise to two fascinating new applications. The first is an Identity-Based Encryption framework that uses biometric identities. That is one can see a user's biometric, for instance an iris scan, as that users character depicted by a few attributes and after that encode to the user utilizing their biometric personality. Following biometric estimations are uproarious; it is bad to utilize existing IBE frameworks. Nonetheless, the mistake resistance property of Fuzzy-IBE takes into consideration a private key which is gotten from an estimation of a biometric to unscramble a ciphertext scrambled with a somewhat diverse estimation of the same biometric. Furthermore, Fuzzy IBE can be utilized for an application that can be called “attribute based encryption”. In this application a party will wish to scramble or encrypt a record to all users that have a specific arrangement of characteristics. For instance, in a software engineering office, the executive might need to encode a report to all frameworks staff on a procuring board of trustees. For this situation it would scramble to the personality “employing committee”, “faculty”, “systems”. Any user who has an identity that contains these properties could decrypt the report. The point of interest to utilizing Fuzzy IBE is that the report can be put away on a straightforward untrusted storage server as opposed to depending on trusted server to perform verification checks before conveying a record. ABE was proposed by Sahai and Waters [9]. In ABE, a client has an arrangement of ascribes notwithstanding its unique ID. There are two classes of ABEs. In key-strategy ABE or KP-ABE [4], the sender has an access policy to encrypt data. An author whose characteristics and keys have been renounced can't compose back stale data. The receiver gets attributes and secret keys from the attribute and authority and can decode data in the event that it has matching attributes. In Cipher text-policy, CP-ABE, the receiver has the entrance approach as a tree, with characteristics as leaves and monotonic access structure with AND, OR and other threshold gates.

2.1 Key-Policy Attribute-based Encryption (KP-ABE)

KP-ABE [4] is a crypto framework for fine grained sharing of encrypted information. In KP-ABE cipher text are mark with attributes and private key are connected with access structures that control which encrypted message a use can decrypt. It is utilized for securing sensitive data put away by outsiders on the web. In this framework each ciphertext is marked by the encrypt or with an arrangement of descriptive attributes. Every private key is connected with an access structure that indicates which kind of ciphertexts the key can decrypt. Note this setting is reminiscent of secret sharing schemes. Utilizing known strategies one can fabricate a secret sharing schemes that determines that an arrangement of gatherings must coordinate so as to remake a secret. For instance, one can indicate a tree access structure where the inside nodes comprise of AND as well as OR gates and the leaves comprise of various groups. Any arrangement of group that fulfill the tree can reproduce the secret. In this development every user's key is connected with a tree-access structure where the leaves are connected with attributes. A client can decode a ciphertext if the properties connected with a ciphertext fulfill the key's entrance structure. The essential contrast between this setting and secret sharing schemes is that while secret sharing schemes take into consideration collaboration between various groups, in this setting, this is explicitly prohibited. For example, if Alice has the key connected with the entrance structure "X AND Y", and Bob has the key connected with the entrance structure "Y AND Z", framework would not need them to have the capacity to unscramble a ciphertext whose just property is Y by intriguing To do this, this framework adjusts and generalize the procedures to manage more mind boggling settings. This cryptosystem gives a capable apparatus for encryption with fine-grained access control for applications, for example, sharing review log data.

2.2 Cipher text Policy Attribute based Encryption (CPABE):

CP-ABE [3] is a strategy to secure complex control on encrypted information. This procedure is utilized to keep encrypted information private. In this framework, a user's private key is related with a discretionary number of properties communicated as strings. Then again, when a gathering encrypts a message in this framework, they indicate a related access structure over attributes. A client just can decrypt a ciphertext if that client's attributes go through the ciphertexts entrance structure. At a mathematical level, access structures in this framework are portrayed by a monotonic "access tree", where nodes of the access structure are made out of threshold gates and the leaves depict attributes. There AND gates can be built as n of n threshold gates as well as OR gates as 1 of n threshold gates. Besides, this plan can deal with more mind boggling access controls, for example, numeric extents by changing over them to small access tress.

2.3 Multi-Authority Attribute-Based Encryption (MA-ABE):

Mama ABE [8] strategy permits any polynomial number of autonomous authorities to monitor attributes and distribute secret keys. An encryptor can pick, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can just decrypt on the off chance that he has at any rate dk of the given properties from every authority k. hases scheme [8] is equipped for taking care of disjoint sets of attribute that are circulated among various authorities. In this plan, a encrypting party determines an arrangement of characteristics AC with the traits in AC being controlled by a few authorities. Give Ak a chance to be the set of attributes controlled by authority k. At that point the ciphertext C connected with the property set AC must be decrypted by those users u with an set of attributes Au for which the cardinality of the intersection Au Ak AC surpasses the individual threshold dk, for every authority k. one of the principle challenges in actualizing such a multi-power quality based encryption plan is the avoidance of arrangement assaults among clients that get mystery key segments from various powers. In addition, it is attractive that there is no correspondence between the individual authorities. To defeat these difficulties, Chase's plan depends on a trusted focal authority. The subsequent plan is equipped for capable of tolerating multiple corrupted authorities, yet the trustworthiness of the central authority remains stays of essential significance since, by the choking from [4], the trusted power has the capacity of decrypting every ciphertext.

3. IMPLEMENTATION DETAILS

Following Fig. 1 shows the proposed system architecture.

3.1 System Overview

The system architecture is decentralized, meaning that there are several KDCs are used for key management. Creator, reader and writer be the different users in system. User receives a token from the trustee. A trustee can be someone like the federal government who manages user ID's etc. A user after validating the token from one or multiple KDC's, receives key pairs for encryption / decryption. The message is encrypted under the access policy. The access policy decides who can access the data stored in the cloud. After encrypting the file user generate the hash of file using SHA1 algorithm and send the hash value of the file to Third party auditor.

The creator decides on an access policy, to prove his/her authentication and signs the message using this claim. The cipher-text or Encrypted File is sent to cloud server while the hash of file is sent to TPA. TPA verifies the integrity of file on behalf of user request by proof generation and proof verify and result sent to the requested user. When a reader wants to read the file, then he/she request for file to cloud server, the cloud sends cipher-text or encrypted file. If the user has attributes matching with access policy, he/she can decrypt the ciphertext and get original message. Writing process is similar to file creation. When a reader wants to read data in the cloud, it tries to decrypt data in by using the secret keys which he receives from the KDCs. If user has sufficient attributes matching with the access policy, then he/she can decrypt the information stored in the cloud.

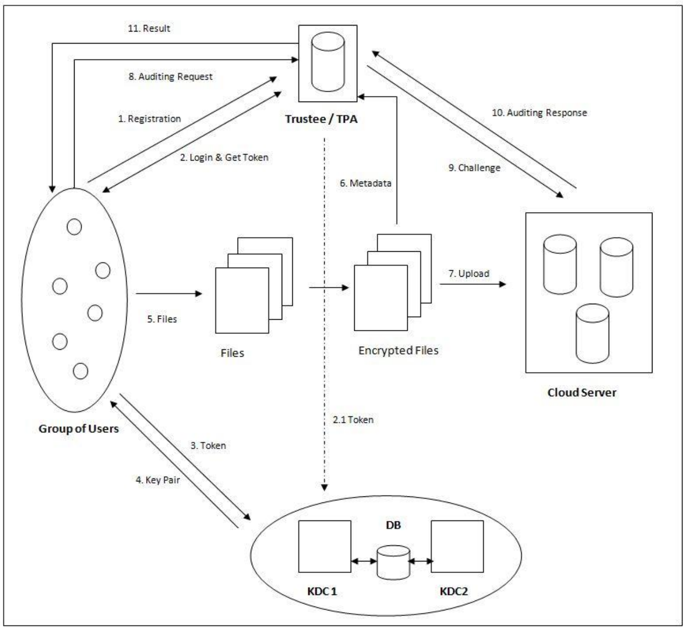

Fig -1: System Architecture

The main modules are:

1. Trustee: A trustee can be someone like the federal government who is responsible for managing social insurance numbers etc. On presenting unique id like health insurance or adhar card number, the trustee gives her/him a token.

2. KDC: The KDC is responsible fordistribute secrete key and writer key to all authentic users. Cloud has multiple KDCs in different locations around the globe. If there is single KDC then it is centralize approach and if multiple KDCs then decentralize approach. KDC is a key distribution center which generates keys and assign thekeys to the users, each organization or group of users have unique keys. KDC generates keys using key generation algorithm and random function. The proposed system uses decentralized access ofKDC which are at different locations in the world. If one KDC is get failed then it automatically switches to another available KDC.

3. Client:

a) Reader - Reader can perform only read operation on file. Reader reads the file online with help of secret key (SK).Reader perform the request to the KDC for the key. When the Reader enters the validkey only then the file is decrypted to the reader. The Decryption proceeds using algorithm ABE. Client is any user who wants to read or write or modify the files which are stored on the cloud server.

b) Writer - When the writer wants to modify file then he is first authenticated using ABE. If the writer key is valid then he/she can update the file. To write the already existing file, User send its request to Cloud server, then cloud will send the encrypted file and ask for key (SK,PK) If key matches, then user is authenticated and allow to write.

c) Creator - Authorized Creator can write the file and upload new files in the cloud. If any other user wants to read or modify the file of creator, he has to then send the request to the KDC to get access keys to the particular file. If KDC provide the key then only user is able to read, update or modify that file.

4. Cloud Server: Cloud server is used to storage of data where user can upload or stores the data. It also maintains the user database which is used for validating the user.

3.2 Algorithm

Algorithm 1: ABE (Attribute Based Encryption)

It works under the following stages.

Step1: Setup

This is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public

Parameters PK and a master key MK.

Step 2: Encryption

This is a randomized algorithm that takes as input a

Message m, a set of attributes, and the public parameters

PK. It outputs the ciphertext E.

Step 3: Key Generation

This is a randomized algorithm that takes as input anaccess structure A, the master key MK and the publicparameters PK. It outputs a decryption key D.

Step 4: Decryption

This algorithm takes as input the ciphertext E that wasencrypted under the set of attributes, the decryption key Dfor access control structure A and the public parametersPK. It outputs the message M if 2 A.

Algorithm 2: ECC Encryption

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

3.2.1 Key Generation:

Key generation is an important part where Alice have to generate both public key and private key. The sender will be encrypting the message with Bob's public key and the Bob will decrypt using its private key. Now, Alice have to select a number d within the range of 'n'. Using the following equation we can generate the public key.

$Q = d * P$

d = random number that we have selected within the range of (1 to n-1). P is the point on the curve. 'Q' is the public key and d is the private key.

3.2.2 Encryption:

Let 'm' be the message that Alice is sending. Alice have to represent this message on the curve. This has in-depth implementation details. Consider 'm' has the point 'M' on the curve 'E'.

Randomly select 'k' from [1 - (n-1)].
Two cipher texts will be generated let it be C1 and C2.
$C1 = k*P$
$C2 = M + k*Q$
C1 and C2 will be send to Bob.

3.2.3 Decryption:

Bob wants the original message 'm' that is send to Alice,
$M = C2 - d * C1$
M is the original message that Bob wants to view.
How does we get back the message?

M = C2 - d * C1
'M' can be represented as 'C2 - d * C1'
C2 - d * C1 = (M + k * Q) - d *(k*P)(C2 = M + k * Q and C1 = k *P)
= M + k * d * P - d * k * P (canceling out k * d *P)
= M (Original Message)

3.3 Experimental Setup

The system is built using Java framework (version jdk 1.8) on Windows platform. The Net beans (version 8.0) is used asa development tool. The system doesn't require any specifichardware to run; any standard machine is capable of running the application.

4. RESULTS AND DISCUSSION

Table -1: Comparison Table

Ref papers	Architecture	Write/Read Access	Types of Access Control	Privacy Preserving Authentication	Integrity Check
[5]	centralized	1-W-M-R	ABE	No Authentication	No
[6]	Decentralized	1-W-M-R	ABE	No Authentication	No
[7]	centralized	M-W-M-R	ABE	Authentication	No
This Scheme	Decentralized	M-W-M-R	ABE, ABS	Authentication	Yes

5. CONCLUSION

In this paper, a secure cloud storage model is faced. This framework is decentralized in nature with unknown validation. Utilizing this framework uploading and downloading of a file to a cloud with Encryption / Decryption is more secure. The cloud does not know the identity of the user who stores the data. Key distribution is done in decentralized way utilizing different KDC structure. Also integrating checking is performed by Third Party Auditor on behalf of user request. One limitation is that the cloud knows the access policy for each record stored in the cloud.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure andDependable Storage Services in Cloud Computing," IEEE Trans. ServicesComputing, vol. 5, no. 2, pp. 220-232, Apr, June 2012.

[2] S. Ruj, M. Stojmenovic, A. Nayaks "Decentralized Access Control withAnonymous Authentication of Data Stored in Clouds," IEEE transactionson parallel and distributed systems, pp. 384-394, f 2014.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext Policy AttributeBased Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute Based Encryptionfor Fine Grained Access Control of Encrypted Data," Proc. ACMConf. Computer and Comm. Security, pp. 89-98, 2006.

[5] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records inCloud Computing: Patient Centric and Fine-Grained Data Access Controlin Multi Owner Settings," Proc. Sixth Int'l ICST Conf. Security andPrivacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

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

[7] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained andFlexible Access Control to Outsourced Data with Attribute Based Cryptosystems,"Proc. Seventh Int'l Conf. Information Security Practice andExperience (ISPEC), pp. 83-97, 2011.

[8] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. FourthConf. Theory of Cryptography (TCC), pp. 515-534, 2007.

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

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