ANONYMOUS AUTHENTICITY TO WORK WITH DATA OVER THE CLOUD

Gaurav[1], Jasmine Bedi Khurana[2]

[1,2]CSE, Galgotias College of Engineering and Technology, (India)

ABSTRACT

Clouds are proving to be game changer elements in this current era technology, each IT and Non-IT firm is moving toward clouds; to enhance their product marketing. People use these offers to get rid of carrying the data assets with them such as hard disks, compact disks and pen drives. But as this technology provides the attractive solutions, the only thing that strikes in a person's mind is that how much it is secure to store the information over the cloud. Is there a method to work with security breach? Is there any way to keep the identity of the user confidential? InThis papera method is being proposed that solve the above stated problems. Here encryption and decryption techniques are used.

Keywords: ABE, ABS, Cloud, Decryption, Encryption, KDC.

I. INTRODUCTION

Cloud computing gathers all the computing assets and copes with them automatically through software. In the process of data analysis, it integrates the history data and present data to make the collected information more accurate and provide more intelligent service for users and enterprises. The cloud is a space over the internet which provides the online storage of data, this helps in reducing the carriage for the pen drives, hard disks and other material.In this manner security and protection are imperative issues in distributed computing. In one hand, the client ought to confirm itself before starting any exchange, and then again, it must be guaranteed that the cloud does not mess around with the information that is out sourced. Client security is likewise obliged so that the cloud or different clients don't have the idea about the personality of the client. The proper searching method on encoded information is additionally an imperative concern in clouds. Here the clouds must not know the question asker but rather ought to have the capacity to give back the records that fulfill the inquiry. This is performed by method for searchable encryption systems.

Depending upon the use the clouds can be categorized into four categories, one is private cloud, second in public cloud, and third one is hybrid cloud and last but not least is community cloud. The private clouds are completely owned by an organization and that does not let the cloud space for rent. Public cloud is open for public means more than one organization can contribute over it. The hybrid cloud is maintained by an organization to let their services on use as per the rent basis. These days the hybrid clouds are being used mostly because these are becoming a good source for monetary funds and the security issues are growing in public as well as in hybrid clouds.Various types of services like SaaS(Software As A Service) which runs applications such as Google Apps, Microsoft online IaaS(Infrastructure As A Service) such as Amazon's EC2, Eucalyptus, Nimbus and etc, last but not least PaaS(Platform As A Service) such asAmazon's S3, Windows Azure and etc. different layers that are provided by the clouds to help the users.

This ubiquitous technology is helping the people with anytime and anywhere availability of the data. Just take a real time example of drop box,(a cloud service utility to store the data online) where a user used to store the data, this data can be sensitive some personal information, now what if somebody logged in your account and can use that data then this puts a direct question over the security of data which is stored over the clouds.

II. ISSUSES TO DEAL WITH

2.1 Confidential Users

The cloud can hold the customer records for the data over it, and in like way, to give advantages of ongoing utilization itself is capable. The authenticity of the customer who stores the data is furthermore affirmed. There is additionally a prerequisite for law execution divided from the particular responses for surety security and insurance.

2.2 Encryption in Cloud Computing

The cloud is likewise inclined to information change and server intriguing mangle. The opponent can barter storage servers in server intriguing attack, so that server can change information records despite the fact that the servers are inside consistent. The information necessities to be encoded to give secure information capacity. Nonetheless, the information is regularly encrypted;this property needs to be taken into care while working on the productive secure capacity strategies.

2.3 Cipher and Plain Text Conversions for Query Optimization

Customer's Authentication policy using public key cryptographic methods as a piece of appropriated registering. Various homomorphic encryption techniques have been optional to ensure that the cloud is not prepared to examine the data while performing operations on the data. By using this encryption plot, the cloud gets cipher data and performs operations on the cipher text and returns the encoded form of the data to customer then the customer has the limit decipher the result, regardless of the way that the cloud does not understand what data it has used away at. In such circumstances, it must be likely for the customer to affirm that the cloud returns right results.

2.4 Data Access Policies

Access control is fundamental when unauthorized clients try to access the information from the capacity, so that just approved clients can get to the information. It is additionally huge to check that the data originates from a dependable source. We have to tackle the issues of access control, verification, and security insurance by applying suitable encryption systems given in [1] [2] [3].There are three sorts of right to use controlling policies such as : user-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC).In UBAC, the entrance control list contains the rundown of clients why should approved access information. This is unrealistic with various clients over the cloud.

In RBAC users are categorized based on their own roles. Data should be accessed by the users who satisfy the role matching constraint. There exist various roles that are used by the system such as for e.g., just employees and senior secretaries may have entry to information however not the lower secretaries.

ABAC is more reached out in extension, in which clients are given properties, and the information has joined access approach. Just clients with legitimate arrangement of traits and fulfilling the accessing approach, can get to the information. Just when the clients have coordinating arrangement of properties, they have decoding the data

put away in the cloud. The merits and demerits of RBAC and ABAC are discussed and compared in [4]. There has been some related work on ABAC in clouds for authentication (for example, [5], [6], [7], [8]).

This is not only just confined up to the storing of the data it has wide range where the user who want to upload some sensitive data over the cloud without being acknowledge his identity. This anonymous action can be done via keeping cloud untouched about the identity of the user but the user should be validated so the key must be generated by another trusted third party just like online banking system where the transactions done through a third party that is called as the merchant site. Complete process is handled by this merchant or one can say the trusted third party (TTP).

III. LITERATURE SURVEY.

Wang et al. addressed secure and dependable cloud storage**.**In this paper clarifies the information encryption method to store the information in cloud. So that the security is high when contrasted with alternate plans included. To moderate the danger, distributed computing partners ought to put vigorously in risk appraisal to guarantee that the framework scrambles to ensure information, makes trusted establishment to secure the stage and foundation, and incorporates higher confirmation with evaluating to fortify consistence. Security concerns must be tended to keep up trust in distributed computing innovation [6].

D. R. Kuhn, E. J. Coyne, and T. R. Weil proposed adding attributes to role-based access controlby working onaccess control mechanisms that collaborates attributes to the role based access control mechanism(ACM).This paper puts emphasis on Access Control by which a system grants or revokes the right to access data, or perform some action. Normally, a user must first Login via some Authentication system. Next, the ACM controls the operations that user may or may not make by comparing the User ID to an Access Control database[7].

Zhao et al. gives protection protecting verified access control in cloud, the current deal with access control in cloud is centralized in nature. Except, and all different plans utilizes a symmetric key approach and does not support verification. And likewise a few schemes don't support confirmation. The current framework has one limit that is the cloud knows the access policy for every record put away in the cloud [8].

R.Ranjith and D.Kayathri Devi portrays the idea of Secure Cloud Storage utilizing Decentralized Access Control with Anonymous Authentication.They executed secure distributed storage by giving access to the documents with the strategy based document access utilizing Attribute Based Encryption (ABE) plan with RSA key public private key blend. Private Key is the mix of the client's traits, so that high security will be accomplished. Time based record Revocation plan is utilized for document guaranteed deletion. At the point when the time furthest reaches of the document terminated, the record will be naturally denied and can't be open to anybody in future. Manual Revocation additionally upheld. Policy based record renewal is proposed. The Renewal could be possible by giving the new key to the current record, will remains the document until the new time limit comes to an end[9].

S DivyaBharathy and T Ramesh presented the idea of security safeguarding access control scheme for information storage, which support anonymous confirmation and performs decentralized key administration in Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control. In the proposed scheme, the cloud embraces an access control strategy and traits concealing method to upgrade security. This new plan backings secure and proficient element operation on information pieces, including: information upgrade, creation, adjustment and reading information put away in the cloud. Also, their verification and access

control plan is decentralized and vigorous, dissimilar to different access control plans intended for clouds which are centralized [10].

IV. PROPOSED SYSTEM

Access control fits in with identity administration by it's extremely nature. It is obliged to safeguard the integrity, confidentiality and accessibility of information over cloud. Access control is executed based upon the strategies UBAC, RBAC and ABAC that manage the flow of information and staff who are authorized to work with the information. There are a couple of things that must be considered when granting ACM into frameworks, such as,

- System's Threats.
- Weak point of system towards threats.
- The hazard that may be emerged by the danger

In the Future, access control must be actualized as a strong establishment at different collaborating layers. At the center of the identity administration for getting to information is the entrance control, wherein arrangements are characterized that portray which gadgets and clients are permitted to get to information on the system and what assignment output be achieved by the client. Clients/clients can set up administrations and deal with their equipment through the cloud access control. The risks originating from systems, for example, spoofing information ought to be shielded by utilizing access control method

Access control services and schemes (predefined rules and strategies set by data and application owners) are called by the applications and related stored data to decide upon authentication and provisioning of services to requested users who satisfy/dissatisfy the specified strategies.

An idea has been proposed wherein, during the phase when a request to access data on the cloud is sent to the cloud via a device that has the user attributes captured in it, an additional level of user privacy and security is provided where the user is given the flexibility to manage the exposure of his attributes to the cloud. For example, this user privacy establishes its importance in situationswhere certain social networking sites and email service providers try to accesspersonal information in order to customize advertisements and contents forthe appropriate users, which might be offensive for a few users who value their privacyThedata put away in cloud takes after Distributed access control strategy so that just approved clients with substantial characteristics can get to the information. Confirmation of clients performs store and adjustment of the information in the cloud. Amid verification the identity of the client is shielded from the cloud. The cloud architecture is decentralized, which implies that there can be a few KDCs for key administration.

V. PROPOSED METHODOLOGY

The proposed system works with two authentication protocols one is Attribute Based Encryption (ABE) and the second is Attribute Based Signature (ABS). In this method the creator is the user who put the file over the clouds, but there is another party involved that gives authentication to put the file on which the cloud owner trusts blindly. While performing these operations the policies that are implied by the cloud owner must be followed, such as revoke policy, grant policy, key renewal policy and many more.

The architecture of proposed framework portrayed in Fig.1. The message is encrypted and decrypted by using ABS and ABE protocols. The whole scenario is studied to keep the user identification confidential and the tampering with data can be stopped.

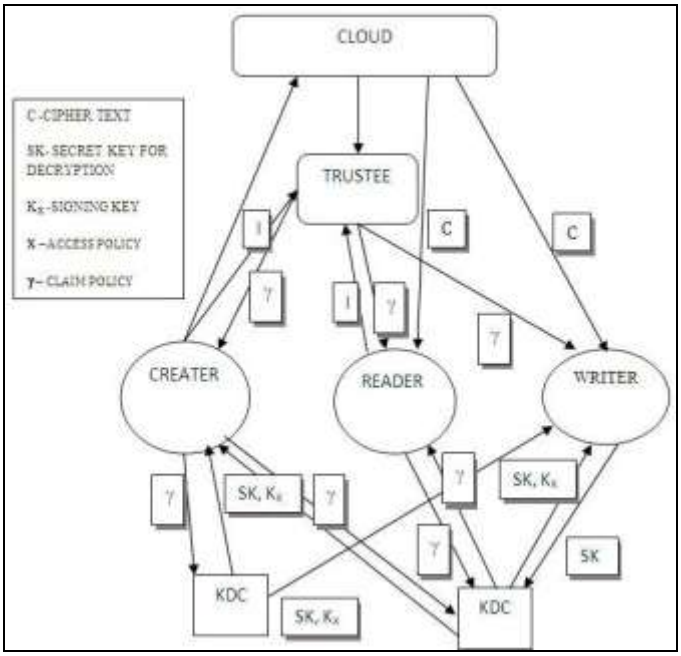

Fig.1 Data Storage on Clouds

Fig.2 depicts how the user one is regular user that uploads and downloads the file on the clouds on daily basis and the other one who just need to download the data that is the user who want to keep the identity confidential, so to help those type of users the cloud must answer the query without knowing the users identity added a third party that will issue some token and that will be considered as a hall ticket to enter in the cloud data. In Fig1and Fig2 it can be seen there are more than one key distribution centers that generates new key all the time by using RSA algorithm and that of 128bits that enhances the complexity of the system, which in turn provides more security.

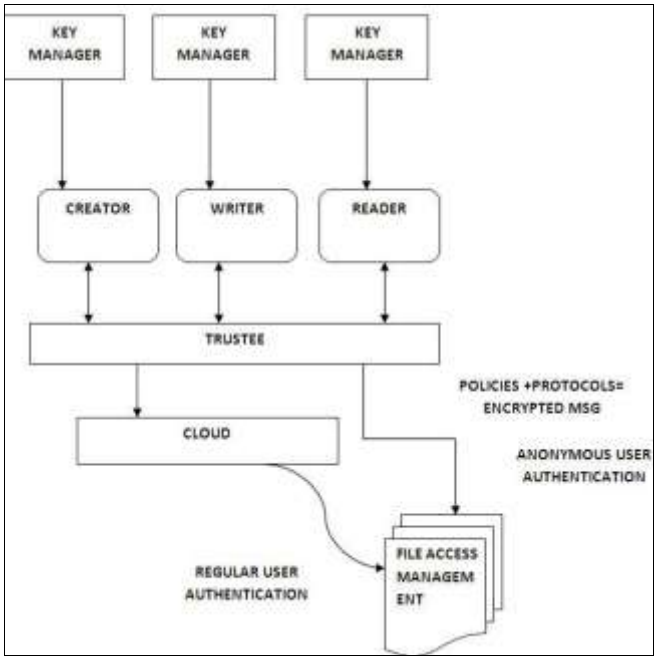

Fig.2 File Accessing by Different Users

5.1 Controlling File Access

5.1.1 Attribute Based Signatures

Each user gives their identity to the trustee which is an honest element in the whole system, based on which the token is generated with respect to each user's identity.

KDC only generate the public key [PK[i]] and secret key [SK[i]], they are used for encryption and decryption; and also it generates the ASK[i] andAPK[i], they are used for sign verification. Then user creates an access policy X to access the files using a Boolean function. This policy also contains the attributes of the user then the whole message is complied by using Extended Paillier algorithm.

C= Extended Paillier.Encrypt (Message, X)

Timestamp T is used to defend the repaly attacks.

In this scheme a writer whose rights have been cancelled cannot create a freshmark with new time stamp and thus it is not possible to write back stale information.

Signing the message and calculating the message signature as

σ = Paillier.Sign(PK_T, PK_K, T_K, SI_K, MSG, γ).

$PK_{T:}$ - Public Key of Trustee,

$PK_{K:}$ - Public Key of KDCs,

$T_{K:}$ - Token,

MSG: - Message,

$SI_{K:}$ - Signing Key,

γ :– Access Claim .

Once the user's information is stored over the server's database, the reply of the token is generated and received from the trustee, which is considered as an honest entity in the system.

5.1.2 File Upload

The customer made appeal to the key administrator for public key, which will be created by policy connected with the record. Diverse strategies for documents, public key likewise varies. At the same time for same public key for same policy will be created. At that point the customer produces a private key by joining the username, password and security certifications. At that point the record is scrambled with public key and private key and sent to the cloud.

5.1.3 File Download

The customer can download the document after completion of the confirmation process Fig2. As public key kept up by the key supervisor, the customer demands the key chief for public key. The validated customer can get the public key. At that point the customer can decode the record with the public key and the private key. The client's accreditations were put away in the customer itself. Amid download the document the cloud will confirm the client whether the client is substantial to download the record. Yet the cloud doesn't have any properties or the subtle elements of the client.

5.1.4 File Access Control

The power to control the entrance into host frameworks and applications through correspondence points is achieved by ABE &ABS. To accomplish documents access,user must be distinguished or validated. After accomplishing the validation handle the clients must take up with right approaches with the documents. To recoup the record, the customer must demand the key admin to produce public key, so that the customer must be confirmed. The ABE standard is utilized for document access which is confirmed by means of a policy and

attribute connected with the record. With document access control the record downloaded from the cloud will be in the configuration of read just or compose bolstered. Every client has connected with policies for every record. So the right client will get the document while using ABE and ABS protocols.

The whole work is implemented in the Net beans which gives the GUI to the work that upload and download the file from and to the server respectively. Fig.3 the trusted third party (TTP) interface which calls for the authentication steps and also do work in collaboration with KDCs, Signature Policy, Claim Policy and cipher text.The token is being requested by the user to work with the data on the cloud server. This TTP enables the system to hide the user details so that the user can work anonymously keeping his/her details confidential. Since the key and the token are two important steps in the whole procedure and the encryption with the RSA makes the system more complex and that disables the tampering with the stored data.

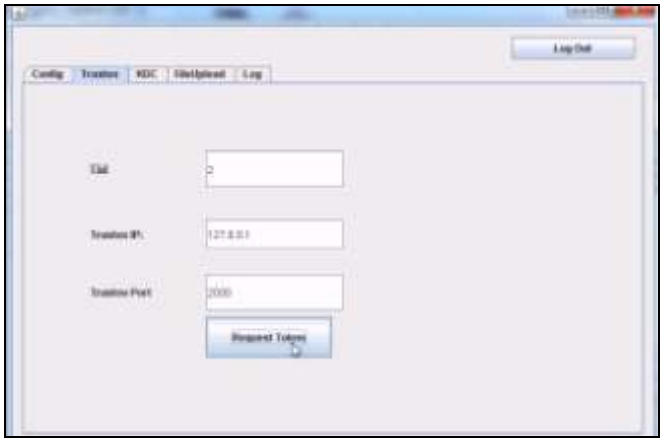

Fig. 3 Trusted Third Party Interface

VI. CONCLUSION

When working with clouds the thing that matters most for a user is the security of the information which he/she uploads over the cloud. Since the clouds are becoming the part of daily use document storage so any tampering with data is not bearable in any case, here the secured way of working with cloud is proposed in which the security of the user is primary concern for which ABE and ABS protocols are used to encrypt the message and more than one KDC are used which will produce different key for different operation but the key will remain same for the same policy and along with this anonymous user can also upload /download the data without being let his/her identity revealed. This system has its own merits and demerits because the data with which one is working can be very sensitive here a third party interface is used and which is considered as most honest element of the system, if this trustee got tampered by some mischievous elements then this will turn into a curse rather than a blessing.

REFERENCES

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

[2] M. Green, S. Hohenberger, and B. Waters, “Outsourcing the Decryption of ABECiphertexts,” Proc. USENIX Security Symp., 2011

[3] H.K. Maji, M. Prabhakaran, and M. Rosulek, “Attribute-Based Signatures: Achieving Attribute-Privacy and CollusionResistance,” IACR Cryptology ePrint Archive, 2008.

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

[5] Sushmita Ruj, Milos Stojmenovic, And Amiya Nayak," Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds" IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

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

[7] 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.

[8] 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

[9] R.Ranjith, D.Kayathri Devi," Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication," Proc. IJARCCE, Vol. 2, Issue 11, November 2013

[10] S Divya Bharathy,T Ramesh,"Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control," Proc. IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1069 – 1074.

[11] V.R.Mani Megalai, R.Mekala M.E. , "A Literature Survey On Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds Using KDC" ,IJARECE, Vol 3, Issue-12, Dec 2014