International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 12, December 2016)

Attribute Based Encryption with Privacy Preserving in Clouds

MEGAVATH SRINU
Asst.Professor
Department Of CSE
Scient Institute of Technology, Khanapur, Ibrahimpatnam

Abstract: **- Security and assurance are crucial issues in appropriated registering. In existing structure get the opportunity to control in fogs are united in nature. The arrangement uses a symmetric key approach and does not support affirmation. Symmetric key computation uses same key for both encryption and disentangling. The makers receive a united technique where a single key movement center (KDC) scatters riddle keys and attributes to all customers. Another decentralized access control plot for secure data amassing in fogs that support secretive approval. The authenticity of the customer who stores the data is furthermore checked. The proposed plot is solid to replay strikes. In this arrangement using Secure Hash count for check reason, SHA is the one of a couple of cryptographic hash limits, routinely used to affirm that a record has been unaltered. The Paillier crypto structure is a probabilistic unbalanced figuring for open key cryptography. Pailier figuring use for Creation of access methodology, record getting to and archive restoring process.**

Keywords: **KDC, User, Security, Privacy, Password**

I. INTRODUCTION

The mainstay of this is to propose another decentralized access control scheme for secure data amassing in fogs that support obscure confirmation. The proposed plot is solid to replay ambushes. A creator whose qualities and keys have been repudiated can't form back stale information. Passed on get the chance to control of data set away in cloud so simply endorsed customers with authentic attributes can get to them. Confirmation of customers who store and modify their' data on the cloud. The character of the customer is protected from the cloud in the midst of approval. The building is decentralized, suggesting that there can be a couple of KDCs for key organization. The passage control and approval are both interest safe, inferring that no two customers can plan and get to data or affirm themselves, in case they are independently not endorsed. Denied customers can't get to data after they have been disavowed. The proposed plot is solid to replay attacks. A writer whose qualities and keys have been disavowed can't make back stale information. The tradition reinforces different read and makes on the data set away in the cloud. The costs are like the current brought together procedures, and the exorbitant operations are generally done by the cloud. Proposing insurance sparing affirmed get to control scheme. According to our arrangement a customer can make a record and store it securely in the cloud. This arrangement includes use of the two traditions ABE and ABS. The cloud checks the authenticity of the customer without knowing the customer's character before securing data. The arrangement moreover has the extra part of access control in which simply significant customers can unscramble the set away information. The arrangement neutralizes replay ambushes and sponsorships creation, alteration, and examining data set away in the cloud.

II. RELATEDWORK

ABE was proposed by Sahai and Waters In ABE, a client has an arrangement of credits notwithstanding its one of a kind ID. There are two classes of ABEs. In Key approach ABE or KP-ABE (Goyal et al. the sender has an entrance approach to scramble information. An essayist whose properties and keys have been denied can't compose back stale data. The recipient gets qualities and mystery keys from the characteristic specialist and can unscramble data in the event that it has coordinating properties. In Cipher content arrangement, CP-AB the beneficiary has the entrance .

strategy as a tree, with traits as leaves and monotonic access structure with AND, OR and other limit entryways. All the methodologies adopt a unified strategy and permit just a single KDC, which is a solitary purpose of disappointment. Pursue proposed a multiauthority ABE, in which there are a few KDC specialists (composed by a confided in expert) which disperse credits and mystery keys to clients. Multiauthority ABE convention was considered in, which required no trusted expert which requires each client to have traits from at all the KDCs. As of late, Lewko and Waters proposed a completely decentralized ABE where clients could have at least zero traits from every expert and did not require a confided in server. In every one of these cases, unscrambling at client's end is calculation escalated. Along these lines, this system may be wasteful when clients get to utilizing their cell phones. To get over this issue, Green et al. proposed to outsource the unscrambling undertaking to an intermediary server, so the client can contend with least assets (for instance, hand held gadgets). Be that as it may, the nearness of one intermediary and one key dispersion focus makes it less powerful than decentralized methodologies. Both these methodologies had no real way to validate clients, secretly. Yang et al introduced a change of, verify clients, who need to stay mysterious while getting to the cloud. To guarantee mysterious client validation Attribute Based Signatures were presented by Maji et al this was additionally a brought together approach. A current plan

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 12, December 2016)

by similar creators adopts a decentralized strategy and gives confirmation without uncovering the personality of the clients. In any case, as said prior in the past area it is inclined to replay assault.

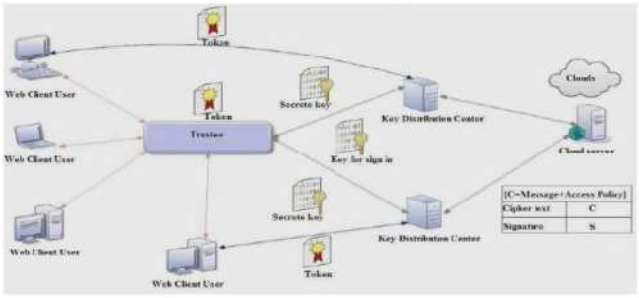


Fig 1: Secure Cloud storage model

Authentication of users who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDC's for key management. There are three users, a creator, a reader and writer. Creator Alice receives a token γ from the trustee, who is assumed to be honest.

III. PROPOSED WORK

The main contributions of this paper are the following: Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. The identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management. The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized. Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. The protocol supports multiple read and writes on the data stored in the cloud. The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud. Manages social insurance numbers etc. On presenting her id the trustee gives her a token γ.. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 1, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The cipher text C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the cipher text C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message. Write proceeds in the same way as file creation. By designating the verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

1. Creation of KDC

Different numbers of KDC's are created and to register a user details. KDC name, KDC id and KDC password are given as input to create KDC. Inputs will save in a database and to register a user details given a input as username and user id.

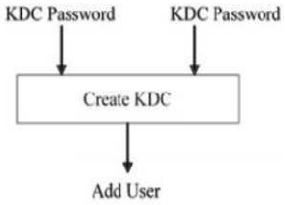


Fig 2: Creation of KDC

2. KDC Authentication

After KDC given a user id to a user, the user will enroll the personal details to KDC's given a input as user name, user id, password etc. The KDC will be verify the user details and it will insert it in a Database.

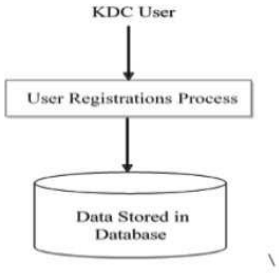


Fig 3: KDC Authentication

3. Trustee and User Accessibility

Users can get the token from trustee for the file upload. After trustee was issuing a token, trustee can view the logs. User can login with their credentials and request the token from trustee for the file upload using the user id. After the user id received by the trustee, trustee will be create token using user id, key and user signature (SHA).

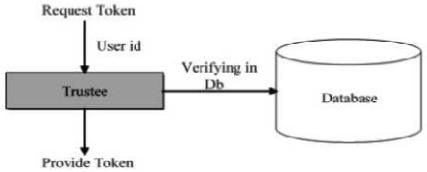


Fig 4: User Accessibility

4.Creation of access policy

After the key was received by the User, the message MSG is encrypted under the access policies. The access policies decide

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 12, December 2016)

who can access the data stored in the cloud. The cipher text C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the cipher text C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message and user can upload the file after user get key from the KDC.

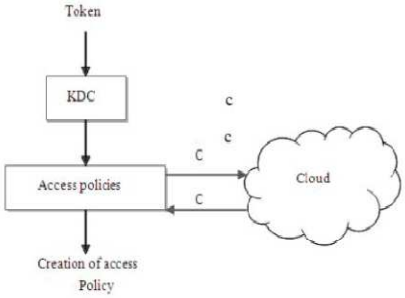


Fig 5: Creation of access policy

5. File accessing

Using their access policies the users can download their files by the help of kdc's to issue the private keys for the particular users. After trustee token issuance for the users, the users produce the token to the KDC then the token verify by the KDC if it is valid then KDC will provide the public and Private key to the user. After users received the keys the files are encrypt with the public keys and set their Access policies (privileges).

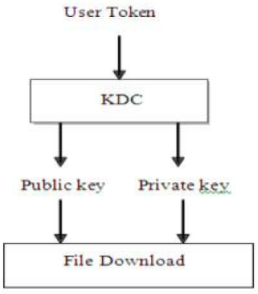


Fig 6: File accessing

6.File Restoration

Files stored in cloud can be corrupted. So for this issue, using the file recovery technique to recover the corrupted file successfully and to hide the access policy and the user attributes.

Fig 7: File Restoration

7. Secure Hash Algorithm Definition:

SHA-1 is one of several cryptographic hash functions, most often used to verify that a file has been unaltered. SHA is short for Secure Hash Algorithm. File verification using SHA-1 is accomplished by comparing the checksums created after running the algorithm on the two files you want to compare. SHA- 1 is the second iteration of this cryptographic hash function, replacing the previous SHA-0. An SHA-2 cryptographic hash function is also available and SHA-3 is being developed. One iteration within the SHA-1 compression function. A, B, C, D and E are 32bit words of the state. *F* is a nonlinear function that varies. *n* denotes a left bit rotation by *n* places. *n* varies for each operation. Wt is the expanded message word of round t. Kt is the round constant of round t. denotes addition modulo 232.

Paillier Algorithm

The Paillier cryptosystem, named after and invented by Pascal Paillier is a probabilistic asymmetric algorithm for public key cryptography. *Key generation* Choose two large prime number *p* and *q* randomly and independently of each other such that gcd (pq,(p-1)(q- 1))=1. This property is assured if both primes are of equivalent length, i.e p,q {0,1 }s-1 for security parameter S . Compute n=pq and λ=lcm(p-1,q-1). Select random integer g where gZ*n 2. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse .μ= (L(gλ mod n2))-1mod n, where function L is defind as the public (encryption) key is (n,g).. The private (decryption) key is (λ,μ).

Encryption

Let m be a message to be encrypted where m Zn. Select random r where r Z*n. Compute cipher text as:

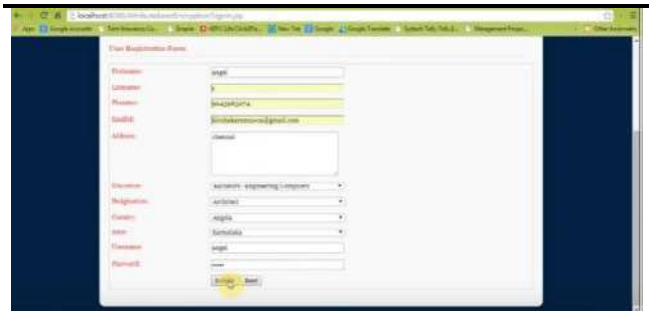
c= gm .rn mod n2 *Decryption* Cipher text: cZ*n2.Compute message: m =L(cλ mod n2). M mod n

IV. EXPECTED OUT PUT RESULTS

Home Page:

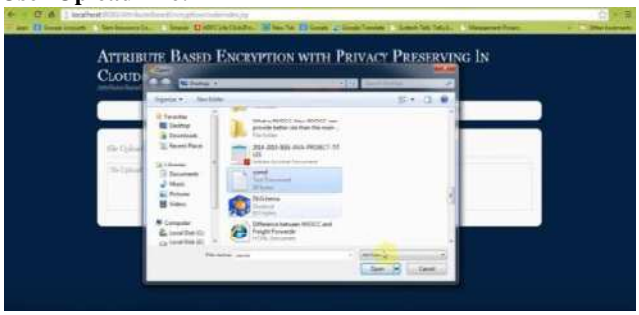
User Registration:

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 12, December 2016)



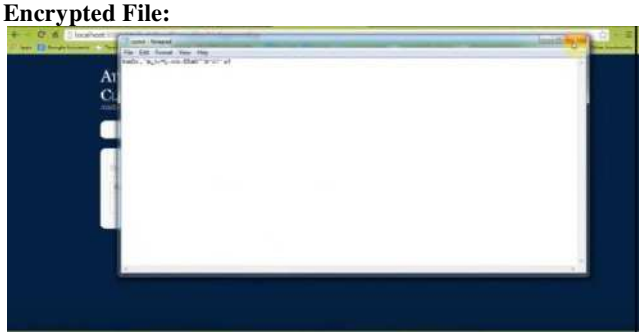
User Login:

User Upload File:



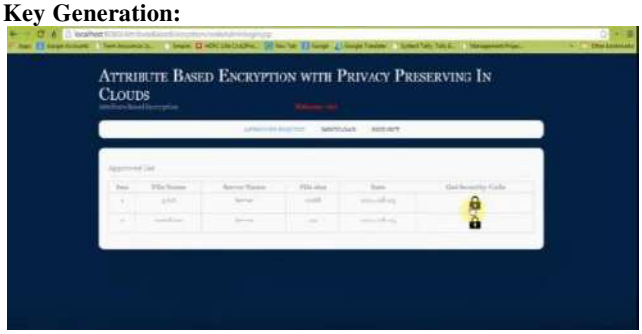
User Operation:

Encrypted File:



Cloud Page:

Key Generation:



V. CONCULSION

A decentralized access control strategy with secretive confirmation, which gives customer repudiation and expects replay strikes, is expert. The cloud does not know the character of the customer who stores information, yet just affirms the customer's accreditations. Enter scattering is done decentralized and moreover cover the qualities and access game plan of a customer. One hindrance is that the cloud knows the passageway plan for each record set away in the cloud. In future, using SQL inquiries for cover the properties and access approach of a customer. Records set away in cloud can be undermined. So for this issue using the report recovery framework to recover the corrupted record viably and to cover the passageway procedure and the customer qualities.

REFERENCES

[1]. S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", *IEEE/ACM International Symposium on 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 T. Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.

[3]. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *IEEE INFOCOM.* , pp. 441–445, 2010.

[4]. S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography Workshops*, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

[5]. H. Li, Y. Dai, L. Tian, and H. Yang, "Identitybased authentication for cloud computing," in *CloudCom*, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

[6]. C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.

[7]. A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," in *TRUST*, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429, 2010.
[8]. R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trust cloud: A framework for accountability and trust in cloud computing
[9]. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," in *ACM ASIACCS*, pp. 282–292, 2010.
[10]. D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in *15th National Computer Security Conference*, 1992.
[11]. 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.

About the author

MEGAVATH SRINU has completed B.Tech in Sri Indu College Of Engineering & Technology 2013, Hyderabad, Telangana, INDIA. And M.Tech in Scient Institute Of Technology 2016, Hyderabad, Telangana, INDIA. Present working in Scient Institute Of Technology, Hyderabad, Telangana, INDIA. As a assistant Professor and his interest area are Cloud Computing, Data Mining.