INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 4, Issue 2 JULY 2015

USER ABBROGATION TO PREVENT REPLAY ATTACKS USING DISTRIBUTED ACCESS CONTROL TECHNIQUE

[1] N. DIVYA, [2] B. DHANA LAKSHMI
[1]PG Scholar, Department of CS.

nagoludivya503@gmail.com

[2] Asst Professor, Department of CS.

dhanaspecial@gmail.com

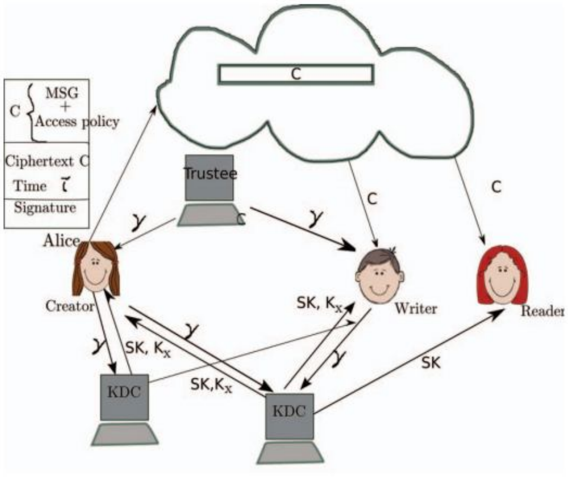
ABSTRACT— Cloud computing could be a rising computing normal during which assets of the computing framework area unit given as a service over the web. As guaranteeing because it is also, this normal additionally delivers plenty of individuals new challenges for information security and access management once shoppers outsource sensitive information for providing on cloud servers, that aren't within identical trusty dominion as data possessors. In any case, in finishing therefore, these results inescapably gift a considerable processing overhead on the information person for key distribution and information administration once finegrained data access management is in demand, and later do not scale well. the difficulty of at identical time accomplishing fine-grainedness, measurability, and information confidentiality of access management extremely still remains uncertain. This paper addresses this open issue by, on one hand, characterizing and implementing access policies supported information qualities, and, then again, allowing the information owner to representative the bulk of the calculation undertakings enclosed in fine-grained information access management to un-trusted cloud servers without unveiling the underlying information substance. we tend to accomplish this goal by exploiting and mixing techniques of localized key policy Attribute based mostly secret writing (KP-ABE) . in depth investigation shows that the planned approach is very economical and secure.

I. INTRODUCTION

Now a days cloud computing could be a rationally developed technology to store information from quite one consumer. Cloud computing is associate degree setting that permits users to remotely store their information. Remote backup system is that the advanced concept that reduces the price for implementing a lot of memory in a corporation. It helps enterprises and government agencies scale back their monetary overhead of information management. they will archive their information backups remotely to 3rd party cloud storage suppliers instead of maintain information centers on their own. a private or a corporation might not require buying the required storage devices. Instead they will store their information backups to the cloud and archive their data to avoid any info loss just in case of hardware / software package failures. abundant of the info hold on in clouds is very sensitive, as an example, medical records and social networks. Even cloud storage is a lot of versatile, however the protection and privacy square measure accessible for the outsourced information becomes a significant concern. In one hand, the user ought to attest itself before initiating any dealing, and on the opposite hand, it should be ensured that the cloud doesn't tamper with the info that is outsourced. User privacy is additionally needed so the cloud or alternative users don't recognize the identity of the user. The cloud will hold the user in charge of the info it outsources, and likewise, the cloud is itself in charge of the services it provides. The validity of the user UN agency stores the info is additionally verified. except the technical solutions to ensure security and privacy, there's conjointly a desire for enforcement. Access management in clouds is gaining attention because it's necessary that solely licensed users have access to valid service. a large quantity of data is being stored within the cloud, and far of this can be sensitive info. Care ought to be taken to make sure access management of this sensitive info which may typically be associated with health, necessary documents (as in Google Docs or Dropbox) or even personal info (as in social networking). it\'s simply not enough to store the contents firmly within the cloud however it might even be necessary to make sure namelessness of the user. as an example, a user would really like to store some sensitive information however doesn't wish to be recognized. The user may wish to post a inquire into a commentary, however doesn\'t want his/her identity to be disclosed. However, the user ought to be ready to influence the opposite users that he/ she could be a valid user UN agency hold on the knowledge while not revealing the identity. There square measure science protocols like ring signatures , mesh signatures, cluster signatures , which may be employed in these things. Ring signature isn\'t a possible option for clouds wherever there square measure an oversized range of users. cluster signatures assume the being of a gaggle that might not be doable in clouds. when scrutiny the drawbacks of all the science protocols mentioned higher than, a new protocol called attribute-based signature (ABS) has been projected during this paper. ABS was projected by author Maji. In ABS, users have a claim predicate related to a message. The claim predicate helps to spot the user as a licensed one, while not revealing its identity. alternative users or the cloud will verify the user and also the validity of the message hold on. ABS is combined with ABE to realize documented access management while not revealing the identity of the user to the cloud.

II. RELATED WORK

Existing work on access management in cloud area schemes use ABE. The theme in uses a bilaterally symmetrical key approach and doesn't support authentication. The schemes don't support authentication additionally. Security and privacy protection in clouds area unit being explored by several researchers. In paper, Wang addressed storage security exploitation Reed-Solomon erasure-correcting codes. Authentication of users exploitation public key cryptographical techniques has been studied in . Many homomorphic cryptography techniques are recommended to confirm that the cloud isn't ready to browse the data whereas acting computations on them. exploitation homomorphic cryptography, the cloud receives ciphertext of the info and performs computations on the ciphertext and returns the encoded price of the result. The user is ready to decipher the result, however the cloud doesn't apprehend what information it\'s operated on. In such circumstances, it should be potential for the user to verify that the cloud returns correct results. Author Wang, in paper addressed secure and dependable cloud storage.



Our secure cloud storage model

Cloud servers vulnerable to Byzantine failure, wherever a storage server will fail in whimsical ways that . The cloud is also vulnerable to information modification and server colluding attacks. In server colluding attack, the individual will compromise storage servers, so it will modify information files as long as they're internally consistent. to produce secure information storage, the data has to be encrypted.

unit centralized in nature. Except and , all alternative

However, the info is commonly changed and this dynamic property has to be taken into account whereas coming up with economical secure storage techniques. In paper , Zhao provides privacy protective authenticated access management in cloud. However, the authors take a centralized approach wherever one key distribution center (KDC) distributes secret keys and attributes to any or all users. sadly, one KDC isn\'t solely one purpose of failure however tough to keep up due to the big variety of users that area unit supported during a cloud atmosphere. Thus, emphasis ought to incline on it clouds ought to take a decentralized approach whereas distributing secret keys and attributes to users. In paper, principle projected a decentralized approach, their technique doesn't evidence users, who need to stay anonymous whereas accessing the cloud. In associate degree another paper, Ruj projected a distributed access control mechanism in clouds. However, the theme failed to offer user authentication. the opposite downside was that a user will produce and store a file and alternative users will solely browse the file. Write access wasn\'t permissible to users apart from the creator. within the projected system, a decentralized design is projected which means that there is many KDCs for key management. the most aim of paper is to style a theme for distributed access management of knowledge keep in cloud so that solely licensed users with valid attributes will access them.

Following assumptions ar created within the projected system:

- Users will have either browse or write or each accesses to a file hold on within the cloud.
- All communications between users/clouds ar secured by secure shell protocol, SSH.
- The cloud is honest-but-curious, which suggests that the cloud directors is fascinated by viewing user ′ s content, however cannot modify it.

The projected privacy protective attested access management theme uses 2 protocols ABE and ABS. These protocols ar explained in Sections severally. within the projected theme a user will produce a file and store it securely within the cloud. the small print of the projected theme ar shown in Figure one. The careful description of model is as follows:

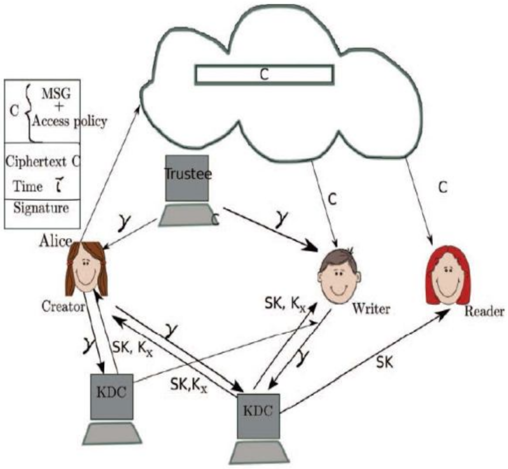
- There ar 3 users, a creator, a reader, and writer.
- Creator Alice receives a token γ from the trustee, WHO is assumed to be honest. A trustee is somebody like
- the centralized WHO manages social welfare numbers etc. On presenting her id (like health/social
- insurance number), the trustee provides her a token γ .
- There ar multiple KDCs (here 2), which might be scattered. for instance, these is servers in numerous components of the world.

A creator on presenting the token to 1 or additional KDCs receives keys for encryption/decryption and signing. within the Figure one, SKs ar secret keys given for cryptography, Kx ar keys for language.

III. FRAME WORK

message flavourer is encrypted below the access policy χ.

- The access policy decides WHO will access the information hold on within the cloud. The creator decides on a claim
- policy y, to prove her legitimacy and signs the message below this claim. The ciphertext C with mark is c, and is sent to the cloud.
- The cloud checks the mark and stores the ciphertext C. At the point when a peruser needs to peruse, the cloud sends C. In the event that the client has properties coordinating with access approach, it can unscramble and get back unique message. Compose continues in the same route as record creation.
- By assigning the check procedure to the cloud, it calms the individual clients from prolonged checks.
- When a peruser needs to peruse some information put away in the cloud, it tries to decode it utilizing the mystery keys it gets from the KDCs. In the event that it has enough traits coordinating with the entrance arrangement, then it decodes the data put away .



Cloud Storage Model

Cloud Server Phase

The cloud server will store the record made and transferred by maker. The cloud permits the client to The strategy and it is checked by cloud if the client is confirmed then keep in touch with existing document is permitted. There is a protected correspondence in the middle of clients and cloud.

Client Phase

Creator,Reader,Writer are distinctive clients here. Inventor will make a record and transfer it to cloud. The maker will scramble the information with access strategy and to demonstrate the genuineness inventor uses claim strategy y and signs the message utilizing this claim approach.

The mark c and ciphertext C is sent to the cloud. Trait Based Encryption is utilized for Encryption what's more, unscrambling of information in cloud .Writer will keep in touch with existing document in the cloud. Peruser will download the document decode it utilizing keys to get unique message.

Trustee Phase

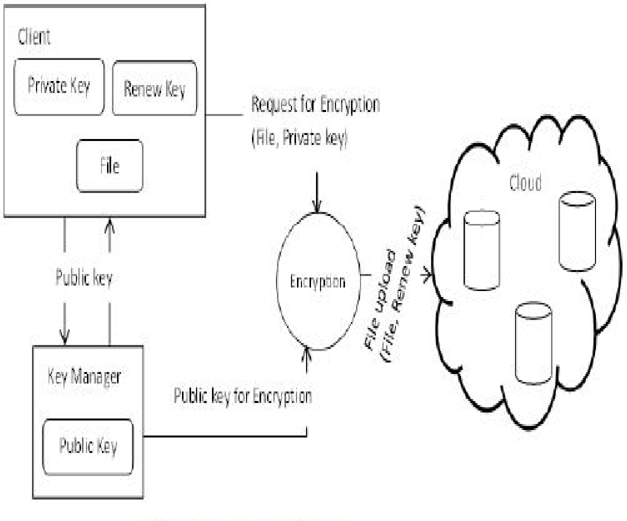
Trustee is framework or server that will confirm that substance maker is a legitimate client. This framework gets id from inventor what's more, makes token and sends it to maker.

KDC Phase

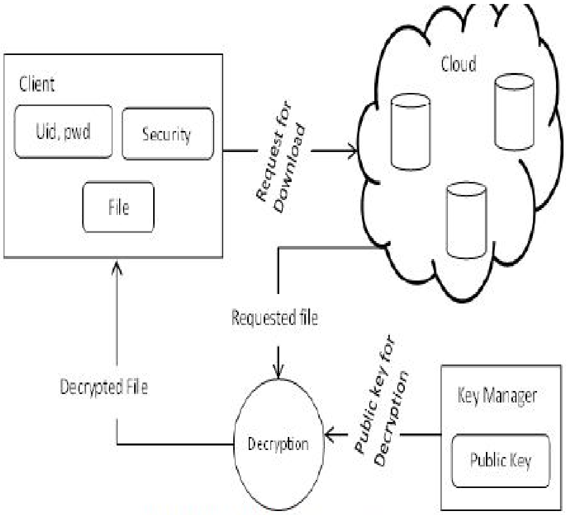
There are various KDCs and they are situated in diverse districts and it produces encryption and unscrambling keys and keys for marking. Maker on displaying token to KDC it will give mystery keys and keys to marking.

The cloud takes decentralized approach in dispersing mystery keys and credits to client.

peruse or compose access to record put away in cloud. The client must send the message and claim



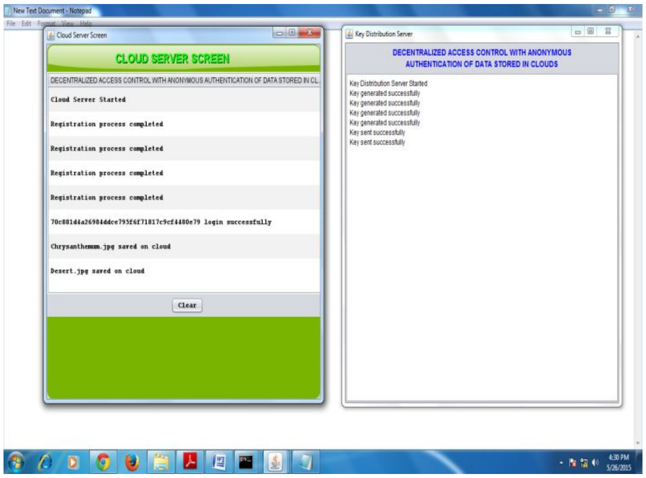
File uploading process



File downloading process

I. EXPECTED RESULT

When we upload some data in to cloud server the message will be shown and the keys for data will be generated for the data which is uploaded.that information was shown in below figure.



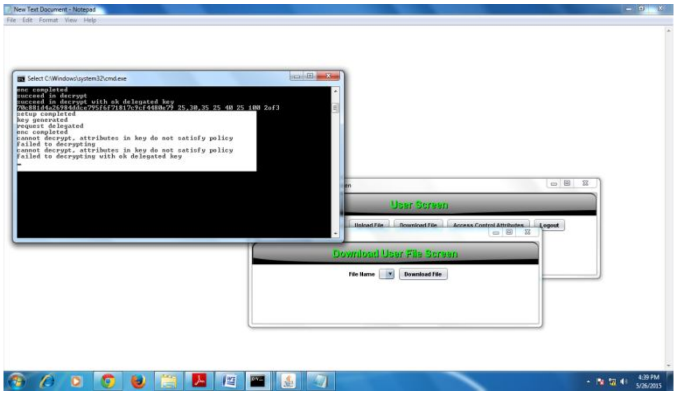
DECENTRALIZED ACCESS CONTROL WITH ANONYMOUS AUTHENTICATION OF DATA STORED IN CL

```
Cloud Server Started
Registration process completed
Registration process completed
Registration process completed
Registration process completed
70c881d4a26984ddce795f6f71817c9cf4480e79 login successfully
Chrysanthemum.jpg saved on cloud
Desert.jpg saved on cloud
```

DECENTRALIZED ACCESS CONTROL WITH ANONYMOUS AUTHENTICATION OF DATA STORED IN CLOUDS

```
Key Distribution Server Started
Key generated successfully
Key generated successfully
Key generated successfully
Key generated successfully
Key sent successfully
Key sent successfully
```

After downloading the data also we will get the messages.those messages was shown below.

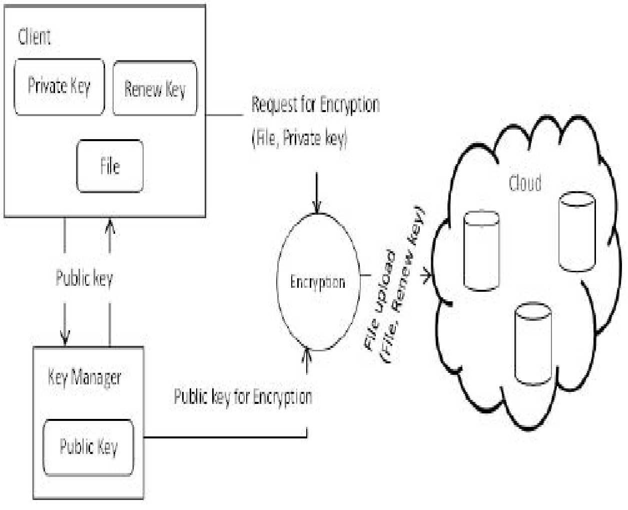

New Text Document - Notepad
File Edit Format View Help
Select C:\Windows\system32\cmd.exe
User Screen
Upload File
Download File
Access Control Attributes
Logout
Download User File Screen
File Name
Download File
4:39 PM
5/26/2015

```
enc completed
succeed in decrypt
succeed in decrypt with ok delegated key
70c881d4a26984ddce795f6f71817c9cf4480e79 25,30,35 25 40 25 100 2of3
setup completed
key generated
request delegated
enc completed
cannot decrypt, attributes in key do not satisfy policy
failed to decrypting
cannot decrypt, attributes in key do not satisfy policy
failed to decrypting with ok delegated key
_
```

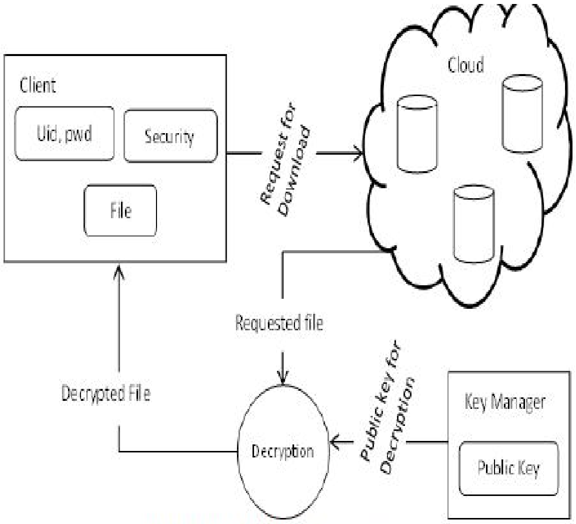
I. Conclusion

In this paper, a decentralized access control framework with strange acceptance is proposed, which gives customer disavowal and thwarts replay attacks. The records are joined with record access courses of action, that used to get to the records set on the cloud.

More security is ensured when exchanging and downloading of a record to a cloud is performed with standard Encryption/Decryption methods. The cloud does not know the character of the customer who stores information, regardless, just checks the customer's capabilities. Key appointment is done in a decentralized way. One farthest point is that the cloud knows the passage game plan for each ought to be conceivable to disguise the qualities and access method of a customer.



File uploading process



File downloading process

IV. EXPECTED RESULT

When we upload some data in to cloud server the message will be shown and the keys for data will be record set away in the cloud. In future, the work

generated for the data which is uploaded.that information was shown in below figure.

REFERENCES

[1] Perlman, “File System Design with Assured Delete,” *Proc.Network and Distributed SystemSecurity Symp. ISOC (NDSS), 2007.*

[2] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed access control in clouds,” in *IEEE TrustCom, 2011*.

[3] Kan Yang, Xiaohua Jia and Kui Ren, “ DAC-MACS: Effective Data Access Control for MultiAuthority Cloud Storage Systems”, *IACR Cryptology ePrint Archive*, 419, 2012.

[4] M. Chase and S. S. M. Chow, “Improving privacy and security in multi authority attribute-based encryption,” in *ACM Conference on Computer and Communications Security, pp. 121–130, 2009.*

[5] W. Wang, Z. Li, R. Owens, and B. Bhargava, “Secure and efficient access to outsourced data,” in *ACM Cloud Computing Security Workshop (CCSW)*, 2009.

[6] 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.*

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

[8] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in *ACM ASIACCS, pp. 261–270, 2010.*

[9] personal M. Li, S. Yu, K. Ren, and W. Lou, “Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings,” in *SecureComm, pp. 89–106, 2010.*

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

[11] 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.*

[12] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A View of Cloud Computing. *Comm. of the ACM, 53(4):50–58, Apr 2010.*