Decentralized Way to Manage with Secret Validation of Information Stored in Clouds

M.Nanda Kishore
MCA., M.Tech
Assistant Professor,
Department of MCA,
Sri Venkateswara College of Engineering and Technology,
Chittoor

V.Mounika
PG Scholar,
Department of MCA,
Sri Venkateswara College of Engineering and Technology
Chittoor

V.Divya Bharathi
PG Scholar,
Department of MCA,
Sri Venkateswara College of Engineering and Technology,
Chittoor

ABSTRACT

We offer a replacement redistributed thanks to manage theme for secure information storage in clouds that supports secret validation. Within the planned theme, the cloud verifies the validity of the series while not knowing the user's identity before storing information. Our theme additionally has the added feature of contact rule that solely valid users are able to decipher the keep info. The theme prevents replay attacks and supports creation, modification, and reading information keep within the cloud. We tend to additionally address user revocation. Also, our verification and access management theme is redistributed and robust, in contrast to alternative access management schemes designed for clouds that are centralized. The communication, computation, and storage overheads are appreciate centralized approaches.

General Terms

Access control, Authentication, Attribute-based signatures, Attribute-based.

1. INTRODUCTION

Research in cloud computing is receiving many attention from every academe and industrial worlds. In cloud computing, users can supply their computation and storage to servers (also observed as clouds) victimization internet. This frees users from the hassles of maintaining resources on-site. Clouds can offer several variety of services like applications. bumper of the information hold on in clouds is very sensitive. Security and privacy are thus, very important issues in cloud computing. In one hand, the user got to attest itself before initiating any dealing, and on the other hand, it ought to be ensured that the cloud doesn't tamper with the information that's outsourced. User privacy is in addition required that the cloud or completely different users don't acknowledge the identity of the user. The cloud can hold the user up to speed of the information it outsources, and likewise, the cloud is itself up to speed of the services it provides. The validity of the user World Health Organization stores the information is in addition verified.

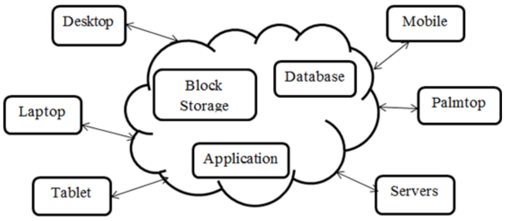


Fig1: Cloud Storage

1.1. Overall System Diagram:

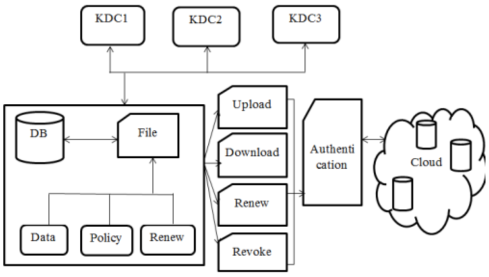


Fig 2 . Overall system

First the client was authenticated with the username and password, which is provided by the user. Then the user was asked to answer two security levels with his/her choice. Each security level consists of 5 user selectable questions. The user may choose any one question from two security levels. The private key to encrypt the file was generated by the combination of username, password and the answers to the security level questions. After generating the private key to the client will request to the key manager for the public key.

The key manager will verify the policy associated with the file. If the policy matches with the file name then the same public key will be generated. Otherwise a new public key will be generated. With the public key and private key the file will be encrypted and uploaded into the cloud. If a user wants to download the file he/she would be authenticated. If the authentication succeeded, the file will be downloaded by the user. Still the user can't able to read the file contents. The user should request the public key to the key manager. In this scheme for authentication, the key manager will produce the public key to the user. Then the user may decrypt the file using the login capability given by the user and the public key provided by the key manager. The client can revoke the policy and renew the policy due to the necessity.

2. SYSTEM ARCHITECTURE

The design of projected system pictured in Fig.2.1.There are 3 users, a creator, a reader, and writer. Creator Alice receives a token nine from the trustee, WHO is assumed to be honest. A trustee are often somebody just like the national WHO manages social welfare numbers etc. On presenting her id (like health/social insurance number), the trustee provides her a token nine. There are multiple KDCs (here 2), which might be scattered. for instance, these are often servers in several elements of the planet. A creator on presenting the token to at least one or a lot of KDCs receives keys for encryption/decryption and language. In the Fig.2.1, SKs are secret keys given for secret writing, Kx are keys for language. The message flavoring is encrypted below the access policy X. The access policy decides WHO will access the information keep within the cloud. The creator decides on a claim policy Y, to prove her credibleness and signs the message below this claim. The cipher text C with signature is c, and is distributed to the cloud. The cloud verifies the signature and stores the cipher text C. once a scanner desires to read, the cloud Sends C. If the user has attributes matching with access policy, it will decode and acquire back original message.

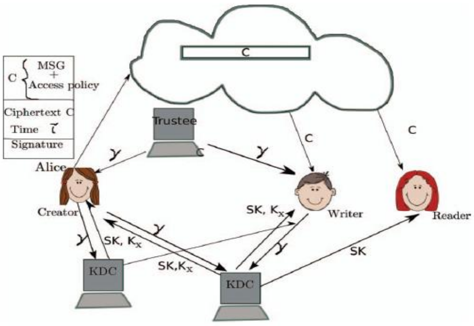


Figure : 2.1 Protected Cloud Storage Model

Advantages:

1. Our access control scheme is secure which means no outsider or cloud can decrypt cipher texts.
2. Collusion resistant
3. Authorized users only can access.
4. Resistant to replay attacks
5. Protects privacy of the user.
6. The cloud is honest-but-curious, such that the cloud administrators can be able to view user's content, but cannot modify data/information.
7. Users have rights like either read or write or both accesses to a file stored in the cloud.
8. The communications between users/clouds are secured by secure shell protocol, SSH.

2.2 Encryption / Decryption

We used RSA algorithm for encryption/Decryption. This algorithm is that the tested mechanism for secure dealings. Here we have a tendency to tend to are practice the RSA algorithm with key size of 2048 bits. The keys are cut up ways get a divorce|separate|split and detain four totally different places. If a user must access the file he/she might got to turn out the four set of data to produce the one personal key to manage encryption/decryption.

2.3 File Upload

The client created request to the key manager for the final public key, which may be generated keep with the policy associated with the file. utterly totally different policies for files, public key put together differs. aside from same public key for same policy square measure generated. Then the patron generates a private key by combining the username, secret and security credentials. Then the file is encrypted with the final public key and private key and forwarded to the cloud.

2.4 File Download

The client can transfer the file once completion of the authentication technique. as a result of the general public key maintained by the key manager, the patron request the key manager for public key. The attested client can get the final public key. Then the patron can decrypt the file with the final public key and conjointly the non-public key. The users credentials were keep inside the patron itself. throughout transfer the file the cloud will proof the user whether or not or not the user is valid to transfer the file.

2.5 Policy Revocation for File Assured Deletion

The policy of a file is additionally revoked below the request by the patron, once expiring the elemental live of the contract or totally move the files from one cloud to a special cloud atmosphere. once any of the on prime of criteria exists the policy square measure revoked and conjointly the key manager will totally removes the final public key of the associated file. thus no one recover the key of a revoked get in future. For this reason we tend to square measure ready to say the file is assuredly deleted. Automatic file revocation theme is in addition introduced to revoke the file from the cloud once the file reaches the termination and conjointly the patron didn't restore the files length.

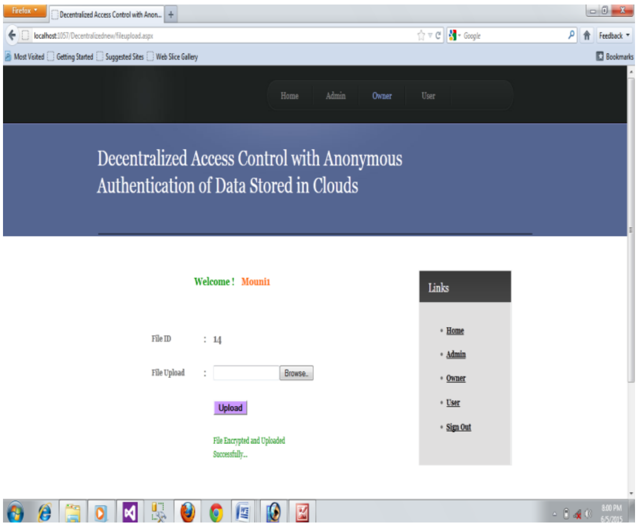
2.6 File Access Control

Ability to limit and management the access to host systems and applications via communication links. To achieve, access ought to be renowned or documented. once achieved the authentication technique the users ought to go at the side of correct policies with the files. To recover the file, the patron ought to request the key manager to induce the final public key. For that the patron ought to be documented. The attribute based secret writing commonplace is used for file access that's documented via associate attribute associated with the file. With file access management the file downloaded from the cloud square measure inside the format of browse exclusively or write supported. each user has associated with policies for each file. thus the proper user will access the proper file. for making file access the attribute based secret writing theme is employed.

2.7. Policy Renewal

Policy renewal might be a tedious technique to handle the renewal of the policy of a file stick with it the cloud. Here we tend to tend to implement one additional key referred to as as renew key, that's utilized to renew the policy of the file stick with it the cloud. The renew secret is keep inside the patron itself.

3. RESULTS & DISCUSSIONS



Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds

Welcome ! Mouni1

File ID : 14

File Upload :

File Encrypted and Uploaded Successfully...

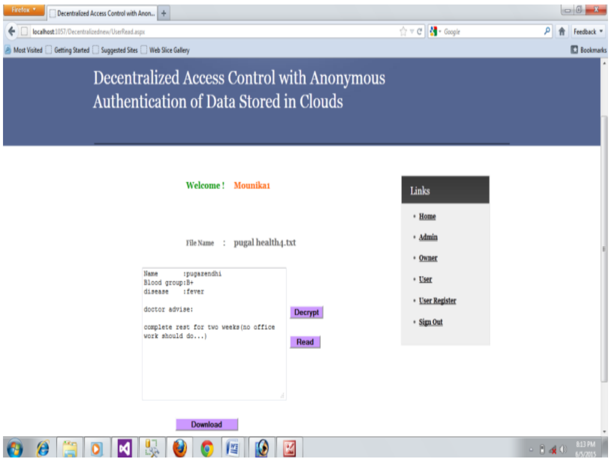
Figure: 3.2 Owner Encrypt File.

The owner can upload the files to the users in the encryption format.

Owner Section

File verification: The public verifier is able to properly check the truth of shared data. The public verifier can check the integrity of shared data without retrieve the entire data from the cloud, if some blocks in shared data have been resign by the cloud**.**

File view: In this unit public auditor view the all details of upload, download, re-upload**.**



Decentralized Access Control with Anonymous
Authentication of Data Stored in Clouds

Welcome ! Mounika1

File Name : pugal health4.txt

```
Name       :pugazendhi
Blood group:B+
disease    :fever

doctor advise:

complete rest for two weeks(no office
work should do...)
```

Figure: 3.1 User Decrypt File

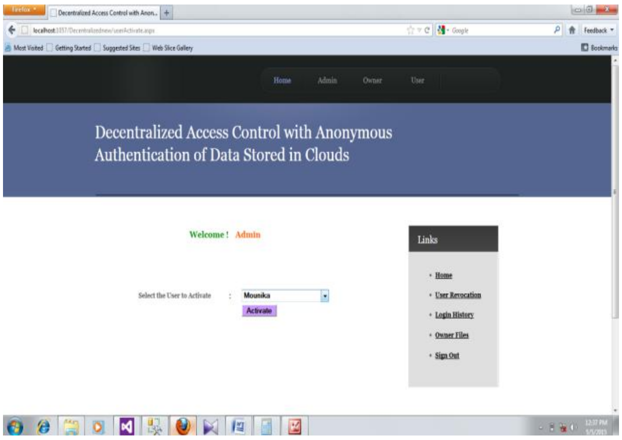
The owner has upload the files in encryption format, the user can read the data in decryption format then only the user will download the uploaded files.

User Section

Registration: In this unit each user register his user information for using files. only user can capable to login in cloud server.

File upload: In this unit user upload a block of files in the cloud with encryption. This ensure the files to be protected from illegal user.

Download: This unit allows the user to download the file using his top secret key to decrypt the downloaded data of blocked user and verify the data and re-upload the block of file into cloud server with encryption**.**



Decentralized Access Control with Anonymous
Authentication of Data Stored in Clouds

Welcome ! Admin

Select the User to Activate : Mounika

Figure: 3.3 Admin Activator

The admin can activate the key permissions for the user and owner.

Admin Section

View file: In this unit public auditor view the all information of upload, download, blocked user, re-upload.

4. CONCLUSION

We have given a localized access management technique with anonymous authentication, that has user revocation and prevents replay attacks. The cloud does not apprehend the identity of the user international organization agency stores knowledge, however entirely verifies the user's credentials. Key distribution is finished throughout a localized suggests that. One limitation is that the cloud is attentive to the access policy for each record keep among the cloud. In future, we'd would like to cover the attributes and access policy of a user.

5. ACKNOWLEDGEMENTS

First and foremost I offer my sincerest gratitude to my college, SVCET and my department of Computer Science and Engineering which has provided the support and equipment I have needed to complete my work. I extend my heartfelt gratitude to my guide, Mr Nanda Kishore and department of Computer Science, who has supported me throughout our research with their patience and knowledge

6. REFERENCES

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

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

[7] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.

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

[9] Sushmita Ruj, Member, Ieee, Milos Stojmenovic, Member, Ieee, 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.

[10] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.