CIPHERTEXT DESTRUCTION IN CLOUD STORAGE

Ms. Rekha S N [1],
[1] PG Scholar, Department of Computer Science and Engineering,
New Horizon College of Engineering, Bangalore, Karnataka, India
[1] rekhasnreddy@yahoo.in;

Ms. Guru Priya M [2],
[2] Associate Professor, Department of Computer Science and Engineering,
New Horizon College of Engineering, Bangalore, Karnataka, India
[2] priyamano89@gmail.com

Abstract

In cloud services, users will frequently be required to reveal their personal sensitive information which could be stored in the cloud which is used for different purposes. However, in a cloud storage network, the servers are easily prone to strong attacks and also commonly experience software/hardware faults. As such, the private information could be under risk in an untrusted environment. Given that the personal sensitive information is usually out of user's control in most cloud-based services, ensuring data security and privacy protection with respect to untrusted storage network has become a formidable challenge in research. To address these challenges, in this paper we propose a self-destruction system, named Cloud Sky, which is able to enforce the security of user privacy over the untrusted cloud in a controllable way. Cloud Sky exploits a key control mechanism based on the attribute-based encryption (ABE) and takes advantage of active storage networks to allow the user to control the subjective life-cycle and the access control polices of the private data whose integrity is ensured by using HMAC to cope with untrusted environments. The feasibility of the system by its performance and scalability is demonstrated by experiments on a large-scale storage network.

Keywords: Cloud Sky, Security, Self-destruction, data privacy, time interval, AES algorithm, cipher text.

1. Introduction

Cloud storage and retrieval have gained increasing popularity in recent years to support different cloud services. To efficiently accomplish the provisioned services, cloud systems usually optimize the service processing by caching, copying and/or archiving a large amount of user data in its storage network.

Although these optimizations can improve the overall performance, they also leave a great risk to disclose the user data to the public since the cloud-wide storage networks are usually not secure in the sense that they are easily under strong attacks and commonly experience software/hardware faults. Given that these data always contain user's privacy, the risk is more serious for the cloud service provider (CSPs) to ensure the data security and privacy protection.

2. Related Work

Ranjith K, et al [1] concluded that the self-destruction system automatically destructs all the information which is no more required. User specifies the time while uploading the information to the cloud, we strongly believe the old data which is no more needed will be deleted and the data complexities will be reduced also cloud will have large space. N S Jeyakarthikka et al [2] the personal information stored in the cloud can have account numbers, sensitive codes, and other necessary details can be misused. This information may be cashed, copied by the service providers without the knowledge of the user and can be misused.

Jinbo Xiong et al. [3] proposed that the data in the cloud will be destructed, if an unauthorized access is detected. This detection is based on the time interval and attributes set. Kishore K et al.[4] approach provides the latest functionalities and the system also flexible for the users in a cloud sky. Further we include AES algorithm for the encryption and decryption process which secures the data in the cloud.

We propose a self-destructing which mainly focus on protecting data by automatically destructing the data after a certain time expires. First encrypt the data into cipher text using AES encryption and provide decryption key and cipher text to the user.

3. Problem statement

The cloud-wide storage networks are usually not secure in the sense that they are easily under strong attacks and commonly experience software/hardware faults.

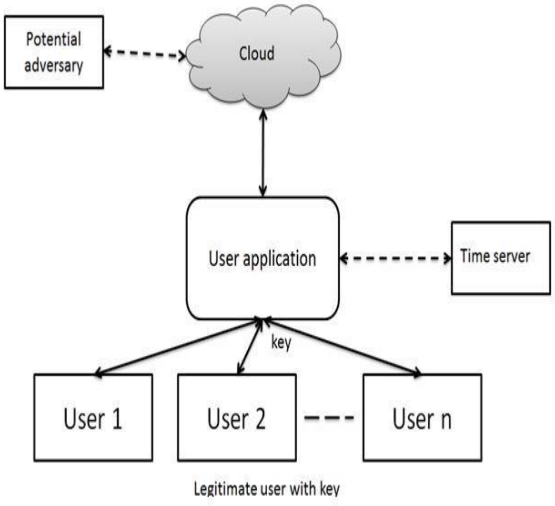
3.1 Proposed System

The IT sectors and the business has grown very vast in a decade and there is a lot of demand for cloud. The cloud services has a vast demand. As the growth of the cloud services increases there exists a lot of new challenges. Our basis problem is whether the stored data is secure or not?

So in this paper i propose a concept ABE method which solves many problems in the cloud environment. The specified time expires which is set by the user. The uploader sets thee time interval in which the user should download the file within the time.

The system architecture includes two clouds in which the user will store the data in first cloud with the time interval. Once time expires the data is deleted and moved to second cloud. So that a request for recovery of data can be executed.

Fig. 2: System architecture

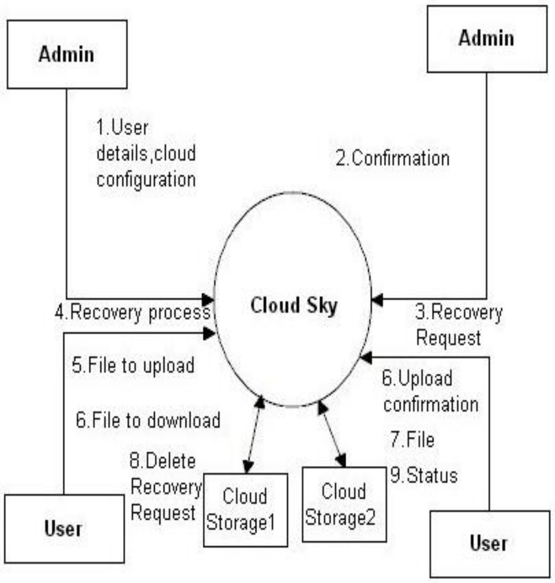


3.2 Methodology

The method proposed here solves many problems which determines the security issues and provides security for the cloud. The cloud user here in this case uploads the data with the time interval set and automatically destructs after the time expires. The user who wants to download the data should download with in the time interval. Once time expires and user requests the data which can be uploaded again. The data should be recovered from the second cloud the first cloud so that request can be granted.

The data stored automatically destructed in the cloud once the specified time expires. The data can be recovered from the second cloud and decrypted by user key and moved to first cloud by encrypting using master key. So here we require two clouds for the recovering of data.

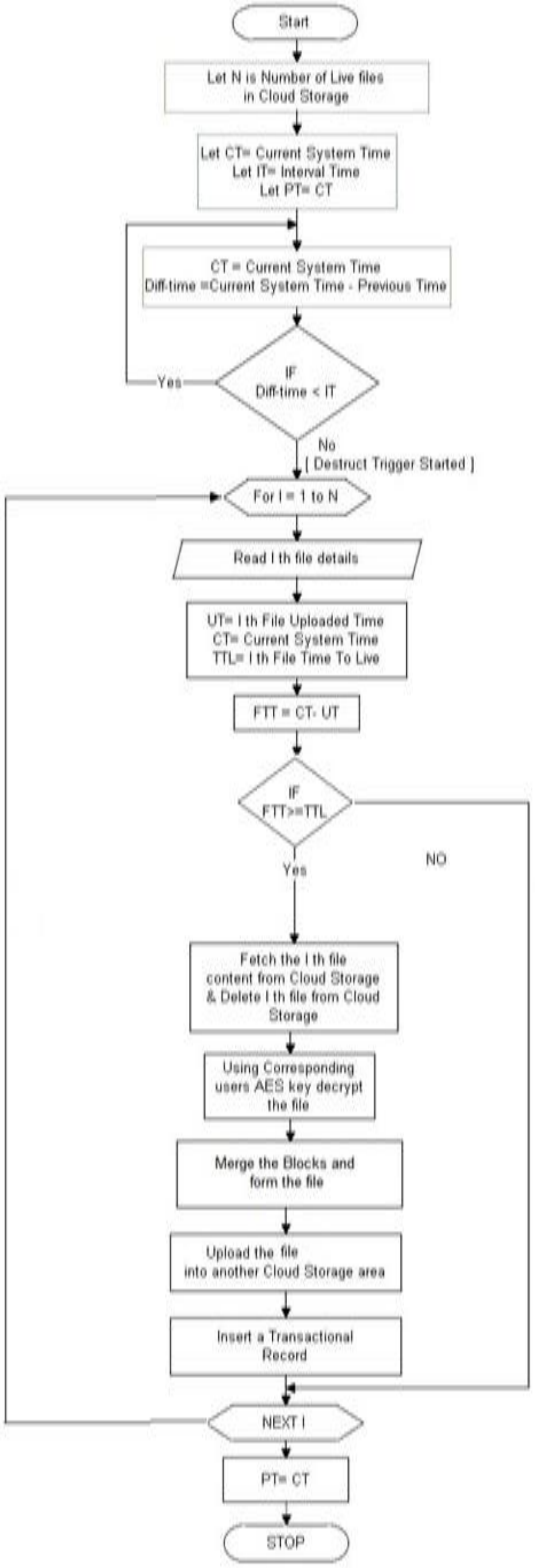
Fig. 2 Context Diagram of Proposed System



The context diagram will works as, the user details should be registered, cloud to be configured. The user will upload the file and can be downloaded with in the time interval. Deleted files can be recovered from the second cloud and can be encrypted to first cloud for the user to download the data again which becomes a live file in the cloud.

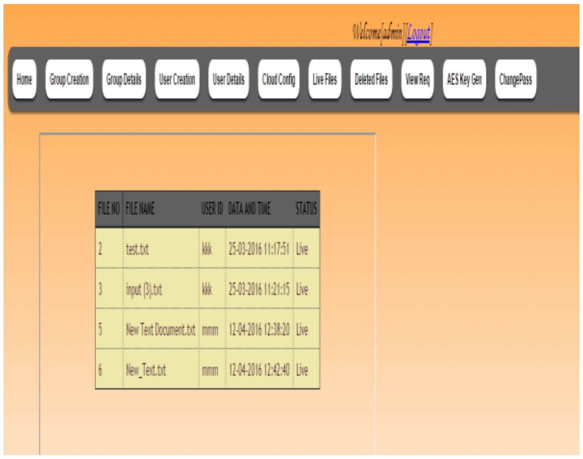
The flow chart contains the number of live files, time interval and the current time in which the difference time is calculated for the data to download with in it. File to be stored is divided into number of blocks and stored in cloud. The user can download the blocks with logical block addressing and can merge the blocks, with the user key the data is decrypted.

Fig. 3 Flow Chart of the Proposed Data


Start
Let N is Number of Live files in Cloud Storage
Let CT= Current System Time
Let IT= Interval Time
Let PT= CT
CT = Current System Time
Diff-time =Current System Time - Previous Time
IF Diff-time < IT
Yes
No
[Destruct Trigger Started]
For I = 1 to N
Read I th file details
UT= I th File Uploaded Time
CT= Current System Time
TTL= I th File Time To Live
FTT = CT- UT
IF FTT>=TTL
Yes
NO
Fetch the I th file content from Cloud Storage & Delete I th file from Cloud Storage
Using Corresponding users AES key decrypt the file
Merge the Blocks and form the file
Upload the file into another Cloud Storage area
Insert a Transactional Record
NEXT I
PT= CT
STOP

3.3 Snap Shots

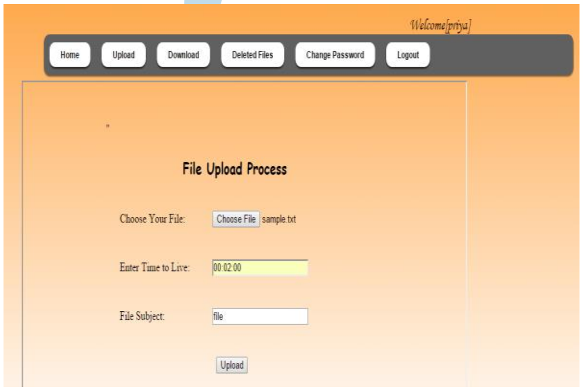
Fig. 4: User details of the cloud



FILE NO	FILE NAME	USER ID	DATA AND TIME	STATUS
2	test.txt	kkk	25-03-2016 11:17:51	Live
3	input (3).txt	kkk	25-03-2016 11:21:15	Live
5	New Text Document.txt	mmm	12-04-2016 12:38:20	Live
6	New_Text.txt	mmm	12-04-2016 12:42:40	Live

The admin will login to the system where a group of users can be created with unique names and registered. We can see the list of groups as well as the users registered successfully. Also includes the configuration settings of the cloud, live files in the cloud, view request, and an AES master key generation.

Fig. 5: File upload process with time interval by user



File Upload Process

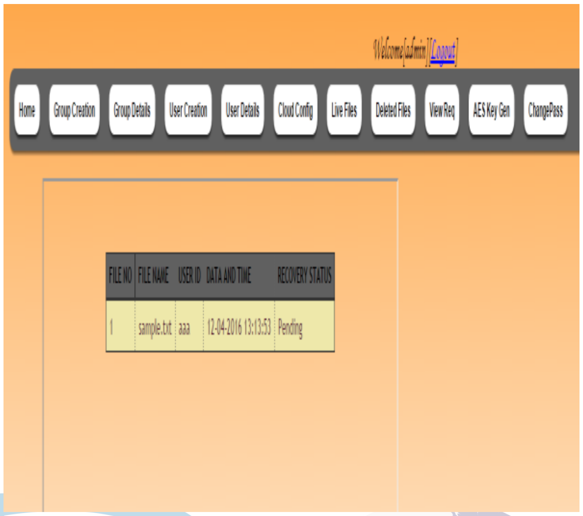
Choose Your File: sample.txt

Enter Time to Live: 00:02:00

File Subject: file

The user will login to the system, the file or data to be uploaded will be chosen from the list of files. After the file selection the time interval for the download of the file is set by the user who uploads the file. Once the time is set enter the subject name and upload the file. After uploading the file conform whether the file exists in cloud under the particular group. Once it is uploaded the user can download the file successfully.

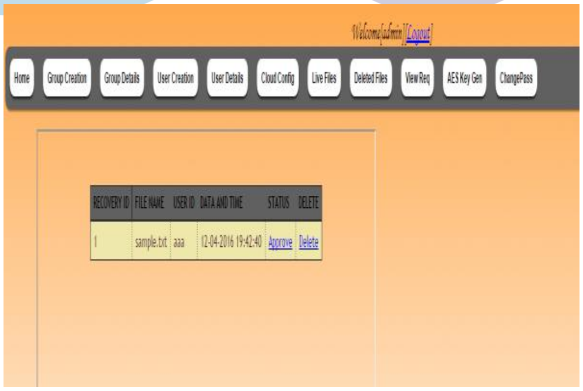
Fig. 6: Deleted files form the cloud to be recovered



FILE NO	FILE NAME	USER ID	DATA AND TIME	RECOVERY STATUS
1	sample.txt	aaa	12-04-2016 13:13:53	Pending

Once the file downloaded successfully the file is automatically destructed after the certain period of time. If the user failed to download the file on time, they can request the system for recovery of the file from cloud.

Fig. 7 Request viewed to approve



RECOVERY ID	FILE NAME	USER ID	DATA AND TIME	STATUS	DELETE
1	sample.txt	aaa	12-04-2016 19:42:40	Approve	Delete

After the user request for the recovery of data from the cloud, admin has the approve the request so that the file from second cloud will be decrypted and copied to first cloud by encrypting with the master key. Later on the file can be available for download, and the file will become a live file.

4. Conclusions

Cloud computing has a wide range of applications in which user stores their sensitive data in the cloud. Cloud provides a storage for users but the data in cloud may not be secure. The hackers may get into system and misuse the information available in cloud. So to avoid the third party agents the system proposed here gives a solution and solves many problems. So to use the cloud services efficiently, the cloud should be secure enough and provide protection for data.

REFERENCES

[1] S Bhaggiaraj N S Jeyakarthikka, A Abuthaheer - Self-destruction of data system based on session keys INTERNATIONAL JOURNAL OF SCIENCE AND TECHNOLOGY RESEARCH FEBRUARY 2014.

[2] Ranjith k, P G Kathiravan - A self-destruction system for dynamic group data sharing in cloud, IJRET.

[3] Jinbo Xiong, Ximeng liu, Zhiqiang Yao, et al. –A secure data self-destruction scheme in cloud computing. IEEE TRANSACTIONS ON CLOUD COMPUTING 2014.

[4] Ramachand V, Kishore K, "A novel technique for enhancing cloud security with self-destruction, April 2014.

[5] "Self-destruction data system for distributed object based active storage framework", by N Ramakalpana, R Santhosh, IASIR.

[6] J Xiong, Z YAO, J Ma, X. Liu, Q. Li, "Priam: Privacy preserving identity and access management scheme in cloud, ITTS, 2015.