Time Based Self-Destruction System for Secure Data Sharing in Cloud

[1] Harikrishnan G.R., [2] Sreeja V., [3] Pavithra T.P., [4] Sithara A.P.

[1] Asst. Professor, Department of Computer Science, MES College of Engineering,
Kuttippuram, Kerala, India

[2,3,4] Student, Department of Computer Science, MES College of Engineering,
Kuttippuram, Kerala, India

Abstract - Cloud computing is often touted as the future of business and enterprise technology where people are subjected to post their personal information like passwords, account number and different vital data. The shared data in a dynamic environment remains in cloud for indefinite period of time and the sensitive information stored may be misused by a miscreant or even by service providers. As a result sensitive and confidential data is at risk from outsider and insider attacks. Thus security and privacy becomes a major issue. In our proposed system, a self-destructing module can be used to automatically clear the data and their copies after a user-specified time. After time expiration, the multicloud feature enables the user to retain the shared data from the user cloud while it is deleted from the shared cloud. By using AES-256 and triple DES algorithm such a system can be developed and hence it reduces the time taken to upload and download file as compared to the native system.

Keywords - **Cloud Computing, Cryptography, Self Destruction, Data Privacy.**

1. Introduction

Cloud computing is a term used to describe a new class of network based computing that takes place over the internet. These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing a very simple graphical interface. In many cases, there occurs a need where people need to submit or post some personal information to the cloud by the web and also share their data among some users. Earlier cloud systems were traditional single owner system, where data sharing couldn’t reach to all relevant users due to reduced cloud utilization and manageability. As a solution multi-owner cloud system was introduced which offers maximum cloud utilization, improved reach ability of shared files etc. Such a group includes several group members and a single group manager. Each group members are data owner of his/her data files and free to store and share any information in the group. Group manager is responsible for management and monitoring of the entire group. As people rely more in cloud they are free to upload and share more files than usual. Moreover, shared files remains in cloud for indefinite period of time which increased possibilities of data misuse by cloud group members as well as cloud service providers. Also this system consumes more space unnecessarily because of the presence of stored and shared files in the cloud. Hence, periodical removal of shared files is the only solution to tackle such a situation.

Since cloud group consists of large number of files, manual removal is not practical in real world. So, automatic removal of shared files is needed. A self-destruction can be used to solve this problem which automatically removes unwanted files. But, still it experience problem in removing files. Because, some files may need for a long time sharing whereas few may not. Therefore automatic removal of files is not applicable here, as it can’t differentiate which file is needed and which is not.

So, we proposed a self-destruction system based on time. In this, each data owner has to specify a time limit up to which the files are available for sharing in the cloud while uploading the files to the cloud. When the time expires, the files will be automatically self destructed from the cloud. If the user wants to retain the deleted files, we have also proposed a multi-cloud feature in which the files will be deleted only from the shared cloud while it is kept as such in the data cloud .So the user can again upload the file if needed. Security and privacy issues still remain as challenges. For ensuring more security, multiple encryption techniques(AES-256 and 3DES) are used. The users can encrypt their files using any of these techniques thus making the task of a hacker more complicated or he/she cannot decrypt the files more easily.

2. Literature Survey

Anuja Palande et al. [2] introduces self-destructing data system using Shamir Secret Sharing algorithm. The user information like bank account numbers, passwords and other personal data can be stored, copied and hacked by cloud service providers (CSPs) without user's permission. So in self-destruction all the information and its copies and decryption key get destructed after user specified time. In Shamir Secret Sharing Algorithm, when one cannot get enough parts of a key, he cannot decrypt the encrypted data using this key, i.e. the key is damaged. Shamir Secret Sharing Algorithm is a form of secret sharing, where a secret key divided into parts, giving each participant its own part. Divide data D into D_1, $D_{2,}$ ....,$D_n$making D easily computable. Idea of Shamir's threshold scheme is it takes k points to define a polynomial of degree (k-1). Suppose (k, n) threshold scheme is to share secret s assumed to be an element in finite field F of size: $0<k<n<p$ where p is prime. Choose random coefficients a_1, a_2,…,$a_{(k-1)}$in F and a_0=s. Build the polynomial $f(x)=a_0,a_1x+a_2x^2+\ldots\ldots+a_{(k-1)} x^{(k-1)}$.

Construct n points, for instance i=1,2,….,n to retrieve (i, f(i)). Every participant gives a pair of input to the polynomial and output. We can find coefficient of the polynomial using interpolation and the secret is the constant term a0 by the given subset of k of these pairs.

Lingfang Zeng et al. [2] introduces Safe Vanish. The vanishing system is a system used for creating messages that automatically self-destruct after a certain period of time. It integrates cryptographic techniques. Distributed Hash Table (DHT) is used to discard the data older than a certain age. The vanishing system is vulnerable to hopping attack and sniffer attack. Out of two versions, Vanish version 0.1 works for encrypting each message with a random key and storing the shares of a key in large, public DHT. The public DHTs like VuzeDHT cannot provide strong security. Vanish version 0.2 stores Vanish key on both.

VuzeDHT and OpenDHT are required to recover the key. A new scheme called Safe Vanish was proposed to prevent the hopping attack by extending the length range of the key share to increase the attack cost substantially and do some improvement on the Shamir Secret Sharing algorithm and also the public key cryptosystem prevent from the sniffing operation. Vanish encrypt data using a randomly generated key and uses the Shamir Secret Sharing to break the key into n shares where k of them are needed to reconstruct the key. The encrypted data object together with the list of random indices comprises the vanishing data object (VDO).

S. Christina Suganthi Monica and M. Subasini [4] introduces time constrained data destruction in cloud. Inorder to overcome the disadvantage in vanish they introduce time constrained data destruction in cloud. There is a meta server and time constrained data system which creates the active storage object. This system provides a specific timeout for the data to be available. Their contribution to be summarized as follows:

1) It focus on the related key distribution algorithm that is, Shamir Secret Sharing Algorithm for purpose of dividing the key equally and storing in object storage system.
2) Based on active storage framework, the object based system can manage and store the equally divided key.
3) Time constrained concept supports security erasing files and random encryption keys in hard disk drive or solid state drive.
4) Through functionality and security properties evaluation of time constrained data destruction prototype. The prototype system imposes reasonably low run-time overhead.

Shankar Gadhve, Prof Deveshree Naidu [5] introduces self destruction system for protecting data privacy in cloud storage. When people put their personal information to the cloud, they hope service providers will secure their information from leaking. The existing system include VANISH and FADE. Vanish is a system used for creating text messages that automatic self destruct after a specific period of time. Each message is encrypted with a random key and storing share of public key in a public key DHTs. In Fade, data will be encrypted before sending it. The system will delete the files and makes them unrecoverableby revoking the file access permission. Proposed system include a self destruct module in which user specifies the survival time and data will be deleted from the cloud environment once the survival time is over. AES core algorithm is used as the core algorithm to implement client. Which provide data privacy.

Lalitha K, Sasi Devi J [6] introduces SEDAS: A Self Destructing for protecting Data Privacy in Cloud Storage as a device model. Effective sharing of resources is not only share by multiple users but also dynamically reallocating as per demand. Self destruction method is protecting the user data privacy through Shamir Secret Sharing Algorithm, which can generate a pair of keys. Self destruction method is associated with time to live (TTL) properly to specify the life time of the keys. User can decrypt after timeout either user give correct keys or Shamir algorithm generates new keys. Self destructing data system consists of two main parts:

1) Secret key part which generate a pair of keys through Shamir secret sharing algorithm.
2) Survival time part which specify time limit of each keys.

Advantages of the self destruction are as follows:

1) No explicit delete action by any third party.
2) Keys can be self destructed after user specified time and reduces the communication overhead as well as network delay.
3) Increasing processing speed.

3. Existing System

VANISH

Vanish provides a new idea for sharing and protecting privacy in cloud. In the vanish system, a secret key is divided and stored in a point to point system with distributed hash tables (DHTs). With the joining and exiting of point to point method, the system can maintain secure keys. According to characteristics of point to point, after eight hours the DHT will refresh every node. Vanish uses Shamir secret key algorithm. When one cannot get full parts of a key, he will not decrypt data encrypted with this key, which means the key is destroyed.

Vanish is a system for creating messages that automatically self-destruct after a period of time. DHTs discard data older than a certain age. The key is permanently lost, and encrypted data is permanently unreadable after data expiration. Vanish works by encrypting each message with a random key and storing shares of the key in a large, public distributed hash table.

Vanish version 0.2 was report two main countermeasures. The first is to store vanish keys on both VuzeDHT and OpenDHT. The data from both DHTs are needed to recover the key. The second is to modify the Vuze to disable the push-on-join behavior and use less aggressive data replication.

FADE

Another system called FADE, provide contribution for the self destructing data by integrating cryptographic techniques. The data will be encrypted before sending it. The system will delete the files and makes them unrecoverable by revoking the file access permission. FADE which is built upon standard cryptographic techniques and assuredly deletes files to make them unrecoverable to anyone upon revocations of file access policies. The public key based homomorphism authenticator with random mask technique are used to achieve a privacy-preserving public auditing system for cloud data storage security. It present three types of assured delete: expiration time known at file creation, on-demand deletion of individual files, and custom keys for classes of data.

4. Proposed System

4.1 Overview

Cloud and its services play an important role in day-to-day life. Cloud users finds it easier to store and share huge number of files in the cloud. But most of them never think about those files after sharing. The shared files remain in cloud for longer period of time and may be misused by miscreant or even service providers. Also dumping of huge number of files in cloud consumes more storage space and reduces search efficiency of the system. Our proposed system finds a solution for these problems. Following session describes design and implementation details of our system in detail.

4.2 System Description

User Registration

User registers with the system by providing the necessary details. After successful registration user can login to the system by providing user name and password.

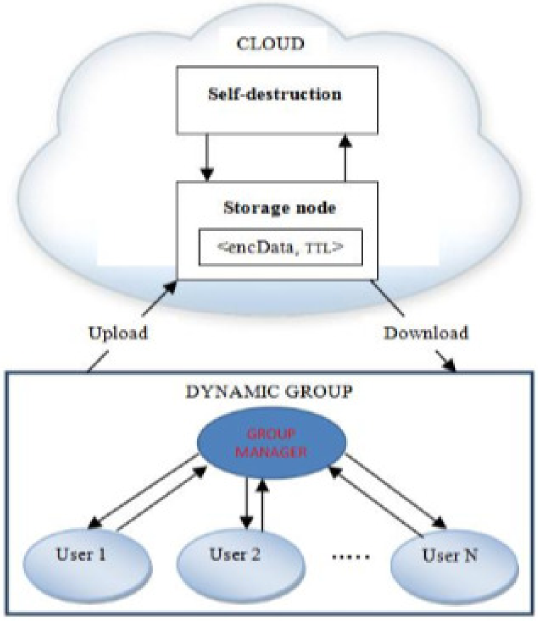

Fig.1 System architecture

File Uploading

File uploading is the process of storing specified data files into the cloud for sharing in the group. When a user uploads a file, it gets uploaded both in data cloud and share cloud. A hash value will be generated for the original file by Secure Hash Algorithm (SHA). The files are encrypted using either AES-256 or 3DES during uploading and the user can choose the type of encryption. User must specify the file and the encryption type as the arguments for the uploading procedure. Once the file are uploaded on the cloud storage the data will be on the cloud only for the specified time limit. Once the time limit expires the file will be automatically deleted from the share cloud.

Share File

When uploading a file the user can select to whom the files have to be shared. The selected users can then access the shared file within the specified time limit.

File Downloading

Before downloading the time has to be checked to determine whether it is in the range of user specified time. If it is so then download is possible. Then it compares the current and stored hash value to determine whether any change is occurred. If it is equal then data will be decrypted and accessed by the user. A log table is maintained which keeps the details of the user who access the file. User can access the data cloud and the shared people can access the shared cloud.

Self-Destruct Method

A self-destruct method is used to delete the data from the cloud storage as per the rules defines. User specifies the survival time and data will be deleted from the cloud environment once the survival time is over.

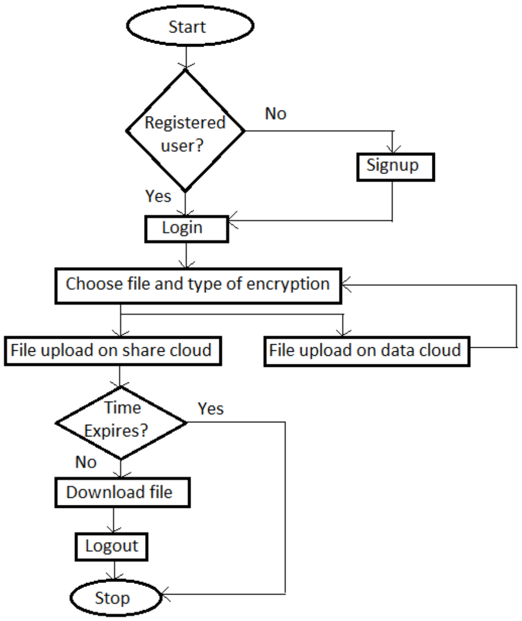
Start
Registered user?
No
Signup
Yes
Login
Choose file and type of encryption
File upload on share cloud
File upload on data cloud
Time Expires?
Yes
No
Download file
Logout
Stop

Fig.2 flowchart of the proposed system

The above figure shows the flowchart of the proposed system.

5. Conclusion and Future Work

In this paper, we proposed a secure self destruction system in cloud computing. Data privacy has become increasingly important in the cloud environment. Thus for ensuring more security multiple encryption techniques were used. We also included a multi cloud feature for the recovery of the destructed file if it is further needed. Hence in this self destruction system all the file are removed automatically as the time expires. We strongly believe that the system will reduce complexity in managing old data files and thereby increasing possibilities in reducing security and privacy issues. This system may be adapted for dealing with Big Data analysis with slight modification.

References

[1] Jinbo Xiong, Ximeng Liu, Zhiqiang Yao, Jianfeng Ma, Qi Li, Kui Geng and Patrick S. Chen, "A Secure Data Self-Destructing Scheme in Cloud Computing", IEEE Transactions on Cloud Computing, VOL:PP NO:99 YEAR 2014.

[2] Anuja Palande, Chaitali Rao, Pooja Redi, Vrunda Bhusari, "Self-Destructing Data System Using Shamir Secret Sharing Algorithm", IJAIEM Volume 4, Issue 1, January 2015.

[3] Lingfang Zeng, Zhan Shi, Shengjie Xu, Dan Feng, "Safe Vanish: An Improved Data Self-Destruction for

Protecting Data Privacy", in second IEEE International Conference on Cloud Computing Technology and Science, January 2010.

[4] S. Christina Suganthi Moricca, M. Suhasini, "Time Constrained Data Destruction in Cloud", International Journal of Innovative Research in Computer and Communication Engineering, Volume 2, Special Issue 1, March 2014.

[5] Shankar Gadhve, Prof. Deveshree Naidu, "Self Destruction System for Protecting Data Privacy in Cloud Storage" , International Journal of Innovative Research in Computer and Communication Engineering, Volume 2, Issue 4, April 2015.

[6] Lalitha K, Sasi Devi J, "SEDAS: A Self-Destruction for Protecting Data Privacy in Cloud Storage As A service Model", International Journal of Innovative Research in Computer and Communication Engineering, Volume 3, Special Issue 1, February 2014.