ISSN 2395-1621

Self Destructing Data on Cloud Storage

[#1]Prof. Sandeep Kadam, [#2]Pratik Dhamale, [#3]Madhura Awachat,
[#4]Dhanashree Bhide, [#5]Harshada Birewar

[4]dhanashree.bhide3@gmail.com

[#1]HOD, Department Information Technology,
[#2345]Department Information Technology,

Zeal College Of Engineering And Research, Pune,
Maharashtra, India.

ABSTRACT

With the fast development of resourceful cloud services, it becomes receptive to use cloud services to share data in a friend circle in the cloud computing environment. As it is not practicable to execute full lifecycle of and privacy security, access control becomes a challenging task, especially when one shares sensitive data on cloud servers. In order to overcome this problem, we propose a Self Destructing System for Privacy, to secure data in cloud storage. The cipher text can only be decrypted if the attributes associated with the cipher text satisfy the key's access structure. The system is able to solve some important security problems by supporting user-defined authorization period and by providing fine-grained access. The sensitive data will be securely self-destructed after a user-defined expiration time.

ARTICLE INFO

Article History

Received: 10th March 2017

Received in revised form :

10th March 2017

Accepted: 13th March 2017

Published online :

18th May 2017

Keywords:- ACL (Access Control List), TTL (Time to Live), data-destruction.

I. INTRODUCTION

Cloud computing is that the promising utility computing, where applications and services area unit getting into the Web is referred to as cloud‖. The cloud users store their information onto the cloud servers and obtain the numbers of your time they use the cloud services. Several firms like Amazon, Google, SUN, and IBM have empowered in cloud computing and offers cloud based solutions.

The data storage in Cloud and in P2P networks is different from that of data stored on personal machines. Data stored in Cloud and in P2P networks is distributed over many servers and could be compromised at any time if it is not properly secured. Trusting the Cloud and P2P systems for securing confidential data is risky. Simple way or solution is to encrypt the data and store that encrypted data in a database to avoid archiving and caching. But, even after data encryption the data can be decrypted by the cloud service provider, because the service provider has access to all the data, and even to the keys and also data may have been cached. A simple encryption is not enough to keep the data secure. Data stored in cloud may contain account numbers, passwords and some confidential data. With popularity of cloud computing and internet, people have started relying more on services provided by both. People are requested to provide private and personal information to cloud through internet.

II. PROBLEM DEFINITION

Secure data storage and usage is one of the major issues in cloud computing environment. In regard of providing security for same few developers have proposed a KP-TSABE scheme which is a novel secure self-destructing scheme for data sharing in cloud computing. One of the most important problem is how to securely delete the outsourced data stored in the cloud server implementing time duration. So we proposed a system that will help data security by blocking the data after the 3 attempts and user will have to request the owner to resend the data and strengthen cloud computing security with federal identity management using cryptographic key exchange methodology and to secure data access in cloud computing.

III. GOALS AND OBJECTIVES

Objectives of the Proposed System to implement a self destructing system for data privacy are:-
The self destructive system defines some modules, a self destruct method and triggering parameter. In such case, System may meet the requirements of self-destructing system with time to live property people can use this secure system as a general active system.
We use these methods to implement safety destruction of data with set of rules.

1) Based on the active storage framework, system use an object based storage interface to store and manage the equally divided key.
2) Through functionality and security properties analysis of this Framework, the results demonstrate that system is practical to use and meets all the privacy goals.
3) System supports security files stored in a cloud storage.
4) Through security and functionality properties evaluation of this method, the results demonstrate that system is more reliable for use and accepts all the security goals. The framework of the system can impose a reasonable low runtime overhead.
5) System supports security deleting files from cloud within a specific rule.
6) The Set of rules provide the information to be uploaded on cloud.

IV. PROPOSED SYSTEM

The proposed project is based on a destruction of data that gives the user a method of Securing its valuable information over a cloud environment.

- It reduces the issue of misuse and the risk that is occurred due to the data leakage.
- Hence, the system offers a methodology of securing the data of a user by providing the specified Time and using an encryption technique.
- The proposed system will help in protecting the data against external as well as internal attackers.
- This will hide the data from other users of the same cloud service.
- It will help in securing the computation between the untrusting parties.
- This system creates a ACL (Access Control List) in which only authorized individuals are listed out.
- It uses concept called key distribution, where original key is divided into sub keys. These sub keys are distributed among individuals present is ACL.
- Encryption takes place at the time of uploading data on cloud with the help of Cryptographic Server. This server also performs key management functionality.

V. PRINCIPLES

Data in transit protection:
Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.
Separation between user Personal securities:
Separation should exist between different consumers of the service to prevent one malicious or compromise consumer from affecting the service or data of another.
Personnel security:
Service provider staff should be subject to personal security. Personal security screening and security education for their role.
Identity and Authentication:
Access to all service interfaces for users and data owners should be constrained to authenticated and authorized individuals.

VI. RISK MANAGEMENT

While some organizations have successfully moved part or all of their information assets into some form of cloud computing infrastructure the large majority still haven't done much with this choice. The extent to which an organization should move its information asset to the cloud and take advantage of the tremendous benefits by doing so is determined by the application of the risk assessment framework .Mapping the virtual machines to the physical machines has to be carried out securely. Data security involves data encryption as well as ensuring that appropriate schemes are enforced for data sharing In addition, resource allocation and memory management algorithms have to be secure. Service providers are now providing self-encrypting drives that implement trusted storage standards of the trusted computing group. Also system provides security of authorization limit so if the password given to system is incorrect then the data will not be retrieved. Although software encryption can also be used for protecting data, since it may be possible for an adversary to steal the encryption key from the machine without being detected. Encryption is the best option for securing data in transit. In addition, authentication and integrity protection mechanisms ensure that data only goes where the users wants it to go and it is not modified in transit.

VII. BENEFITS OF THE SYSTEM

Flexibility:
Users can scale services to fit their need, customize application and access cloud services from anywhere with an internet connection.

Efficiency:
Enterprise users can get application to market quickly without worrying about underlying infrastructure costs or maintaince.

Strategic Value:
Cloud services give enterprises a competitive advantage by providing the most innovative technology available.

Scalability:
Cloud infrastructure scales on demand to support fluctuating workloads.

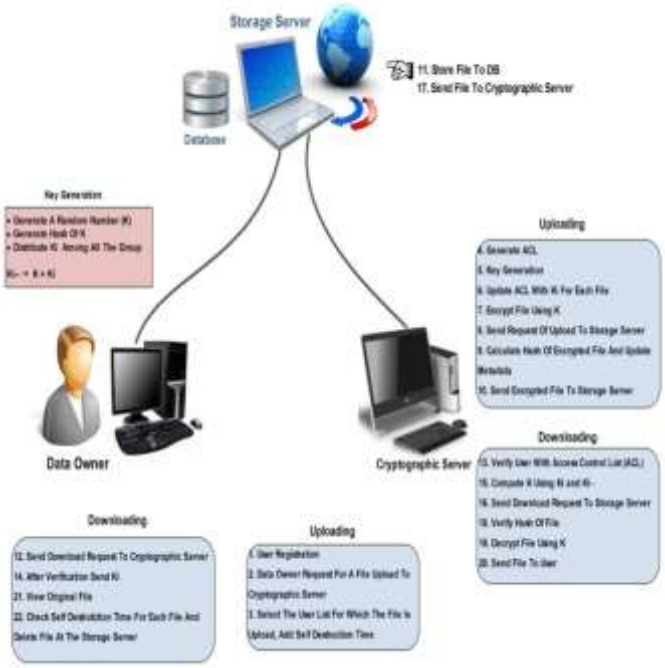
Storage options:
Users can choose public, private or hybrid offerings depending on security needs and other considerations.

Accessibility:
Cloud based applications and data are accessible from virtually any internet-connected device.

Data Security:
Hardware failures do not result in data loss because of networked backups.

Collaboration:
World wide access means teams can collaborate from widespread locations.

VIII. SYSTEM ARCHITECTURE AND REQUIREMENT ANALYSIS



8.1 Architecture System

The self destructive system based on self des defines new modules, a self-destruct module that is associated with Set of rules. In this paper, self destructive system can meet with the need of security and privacy with manageable rules while users can use this system as a general active storage system.

A) Active Storage Object

An active storage system gene rates from a user system and has a triggering parameter value property. The TTL (Time to Live) value is used to delete the self-destruct function. The TTL value of a user object has the value infinite so that the user object will not be deleted until the user deletes it manually. The triggering parameter is nothing but the TTL parameter which is used to activate the self destruction operation. The triggering parameter is decided by the user for how long the user wants the data on cloud environment and after the specified time the data which is uploaded on cloud that will be deleted automatically once the survival time will over

B) Self-Destruct Method

It is used to vanish the data from the cloud storage as per the given rules. User specifies the survival time and data will be deleted from the cloud environment once the survival time is over. System Process begins with the registration of the user and validates them with user id and password.

C) Data Process

To use the self destructive system, applications client should implement logic of data process and act as a node. There are two such different Operations: uploading and downloading.

I) Uploading

When a user upload a file. The file gets encrypted before uploaded on cloud. Data owner creates a ACL (Access Control List) in which the details of authorized users are specified User must specify the file and triggering parameter (survival time) as arguments for the uploading procedure.
the files have uploaded on the cloud storage, the data will be on the cloud in encrypted format and survival time. Once the time will over as mentioned time in triggering parameter, the file will be erased automatically from the cloud environment.

II) Downloading

Owner will request for data download to server. After verification, owner will send key to server. After key verification, data owner can able to perform altering, deleting operation on data.
Authorized user can download the file by sending request to server, server than check user authority by using ACL, than by using key which is on user side, server will compare original key and public key of user. If match found, user is able to download the data. The data gets decrypted before downloading.

IX. CONCLUSION

Data privacy is one of the main aspects in cloud environment. Different approaches are used to protect privacy of data. Self-destruction is a mechanism to protect data from the user who retroactively obtain another user's stored data and key. SQL is used to store data in different nodes. SQL allows storing huge amount of data, and processing it in much more efficient manner and faster manner. File is encrypted and stored in different nodes in SQL. To decrypt file user will not only require key but also all the encrypted parts of a file. Authentic user will be able to download file.

REFERENCES

[1] IEEE2015, Author-Lingfang zeng, Yang Wang, Dan Feng, "Cloudsky: A Controllable Data Self-Destructing System For Untrusted cloud Storage Networks"
[2] IEEE2014, Author-Jinbo Xiong, Ximeng Liu,Zhiqiang Yao, Jiangeng Ma, Qi Li, Kui Geng and Patrick S.Chen
[3] IJISET2015,Author-Shankar Gadhave,Prof. Devashree Naidu Title" Self destruction system for protecting data privacy in cloud storage"
[4] IJERT2014 Author : Prabhavati, Geeta.N , Jyoti Title " Privacy Preserving by Self-Destructing Data Using Time Factor in Cloud"
[5] IJCSMC 2015 Author : Ganesh Bhade and Vikrant Chole Title"Review on Self Destructive System for data privacy on Web services"
[7] IJIRSET 2014 Author : Lalitha K, Sasi Devi Title : SEDAS: a Self Destruction for Protecting Data Privacy in Cloud Storage as a Service Model

