ISSN 2395-1621

A Survey on Data Self-Destruction System for Cloud Storage Networks

[#1]Vaishali Hargude, [#2]Jyoti Ohol, [#3]Sonal Rahinj, [#4]Smita Wangale

[1]vaishalihargude95@gmail.com
[2]jyotiohol95@gmail.com
[3]rahinjsonal123@gmail.com
[4]smitawangle@gmail.com

[#1234]Department of Computer Engineering,

JSPM's,
Imperial College of Engineering and Research, Wagholi.

ABSTRACT

In Cloud Storage we store personal data which contain banking details such as account number, passwords, valuable notes, and other such information that can be misused by hackers. These data are copied and cached by Cloud Service Providers, often without users' authentication and control. Self-destruction system mainly aims at securing the user valuable data's privacy. All the information and their copies become destructed .In this paper, we study a system that meets this challenge through integration of active storage techniques. We implemented self destructive system through the different functionality and different security properties evaluations of this system. In addition to this the data privacy can be given to the system by encrypting the data

Keywords: **Private Data, Self-destruction of data, Cloud Computing, Encryption**

ARTICLE INFO

Article History

Received: 2nd December 2016

Received in revised form :

2nd December 2016

Accepted: 5th December 2016

Published online :

5th December 2016

I. INTRODUCTION

As Cloud computing and mobile Internet are getting popularized, Cloud provides services which are becoming more and most important among people's life. People are requested to submit or post some personal information to the Cloud by the web. When people put their data, they subjectively hope service providers will secure policy to secure their information from leaking, so others user will not retrieve their privacy of data. As people depend more and most on the Internet and Cloud environment, security of their data and privacy is on more threaten. On the another hand, when information is being accessed, transformed and stored by the computer system or network must make cache, copy or stored it. Because these copied information are essential important for systems and the network system. As users who have no information about these copies and could not control them, so these copies can leak their data. On the another hand, their privacy data also can be leaked through Cloud service Providers, hacker' intrusion or some unauthorized actions. These problems could occurs challenges to secure people's data privacy. Personal important data stored in the Cloud may contain banking information, passwords, important notes, and other important data that could be used and improper by a unauthorized person, a competitor, or different user. These information or data are cache, copy, and archived by Cloud Service Providers, without users' permission and manage. Self-destructing system generally aims at securing the user data's security.

II. LITERATURE SURVEY

Dr. Arockiam L et al has focused on issues related to cloud. paper mainly focuses on the issues related to Privacy in cloud computing. Privacy is defined as a fundamental human right related to the collection, use, disclosure, storage and destruction of personal data (Personally Identifiable Information-PII). The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Charted Accountants (CICA) define that it is the right and obligation of individuals and

organizations with respect to the collection, use, retention, and disclosure ofpersonal information. Privacy is the protection of appropriate use of personal information of cloud user. [1]

Keiko Hashizume et al has analysed security issues in cloud and as per analysis, Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.In Cloud computing Security is major factor for transferring the data one to another.This paper presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. In this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which al-lows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. [3]

P. Muralikrishna et al has proposed the system which involves a design of a pre-distribution algorithm using a deterministic approach. Deterministic approach is the process of determining the keys before placing them within the network. A key pre-distribution algorithm using number theory with high connectivity, high resilience and memory requirements is being designed by implementing a deterministic approach.[2]

N. Ramakalpana et al have presented an Asymmetric Cryptography in cloud computing i.e. encryption and decryption process.RSA algorithm is used for establishingsecurity in the internet. Its strength is its computational complexity. It is known for its security based on finding the prime factor of very large numbers. [4]

Kshama D. Bothra et al have implemented the SeDas system.Application client connect through metadata server. In metadata user management, server management, session management, key management.This paper creates multiple nodes for performing the sedas application. Users can perform operation like uploading, downloading or any activity in cloud server then privacy is must for transferring the data. So this paper implementing Shamir's Algorithm for performing encryption and decryption operation. [5]

III.PROPOSED SYSTEM

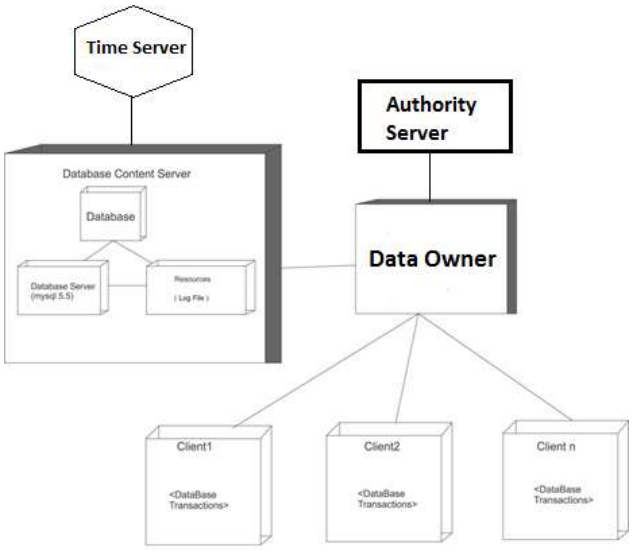

Fig 1. System Architecture

There are lot more security problems in cloud data access. In this paper it is considered how to resolve all the security problems which user faces. Also how user can specify expiration time for cloud data on which data gets self destructed with all its copies over cloud. It supports user defined authorization period in which fine-grained access control is provided over the period.

- Author can provide fine-grained access to the entire authorized user having cloud access.
- Author gives access to user for a specific time period. After that time no user (authorized as well as unauthorized) can access data which is shared by the user.
- Data is shared over cloud for particular time period which is specified by the author. This shared data is in encrypted form so that no one can read the data without decrypting it.
- When user specified time expires, shared data gets self-destructed. While deleting data, this system not only delete original data but also all the copies of data which are resided over cloud.

MODULE:

1) Data Owner: This is user who shares data or files, containing private information with other data users. Data owner stores his/her data over cloud so that other data users can access data from cloud.

2) Authority: Task of authority is to generate, provide and manage private key of users. Authority is an entity which is trusted by all the other users present in the system.

3) Time Server: This server has responsibility regarding time specification. It does not interact with any other entity in the system.

4) Data Users: These are the users who have passed through authentication and access the data which is shared by the data owner. All the data users are able to access shared data by authentication and within authorization period only.

5) Cloud Servers: There are the servers where data owner shares his/her data. Cloud servers have almost unlimited storage space. Cloud servers store and manage stored data so that it can be easily available to users who are accessing cloud.

IV. MATHEMATICAL MODEL

System Description:
Input:
Upload file ()
U : Upload file on cloud.
E : Encryption File.
S : file for security.
D : Decrypt value for each file.

Output:
Check Encryption file on cloud storage

Input:
Function Recovery (id, request, file)
ID : unique id for each file.
Request : User request for recovery of file.
File : Check file on cloud.

Output:
File will recover to data owner.

Success Conditions: Encryption will done for input file

Failure Conditions: Our system fails when no any security policy apply to the input file.

V. CONCLUSION

In this paper, we study a self-destruction system for dynamic group data sharing in cloud systems. Since shared data items in dynamic groups remains long time in the system will considerably reduce the security and privacy of system with increased complexity in managing data files.

REFERENCES

[1] Dr. Arockiam L, Parthasarathy G and Monikandan S,"Privacy in Cloud Computing : A Survey", Natarajan Meghanathan, et al. (Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 321–330, 2012.

[2] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An Analysis Of Security Issues For Cloud Computing",Hashizume et al. Journal of Internet Services and Applications 2013.

[3] P.Muralikrishna, S. Srinivasan, N.Chandramowlis-waran, "Secure Schemes for Secret Sharing and Key Distribution Using Pell's Equation", International Journal of Pure and Applied Mathematics, Volume 85 No. 5 2013.

[4] N. RamaKalpana, R. Santhosh, "SeDas Self - Destruction Data System for Distributed Object Based Active Storage Framework ", International Journal of Software and Web Sciences, 7(1), December 2013-February 2014, pp. 94-100.

[5] Kshama Bothra, Sudipta Giri, "Enhancing Security in Cloud by Self-Destruction", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 9, September 2015.

[6] IEEE paper on " A Self-Destructing system Based on Active Storage Framework" by: Lingfang Zeng, Shibin Chen, Qingsong Wei , and Dan Feng IEEE TRANSACTIONS ON MAGNETICS, VOL. 49, NO. 6, JUNE 2013.

[7] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self- destructing data," in Proc. USENIX Security Symp., Montreal, Canada, Aug. 2009, pp. 299–315.

[8] Y. Xie, K.-K. Muniswamy-Reddy, D. Feng, D. D. E. Long, Y. Kang, Z. Niu, and Z. Tan, "Design and evaluation of oasis: An active storage framework based on t10 osd standard," in Proc. 27th IEEE Symp. Massive Storage Systems and Technologies (MSST), 2011.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," in Proc. IEEE INFOCOM, 2010

[10] Y. Zhang and D. Feng, "An active storage system for high performance computing," in Proc. 22nd Int. Conf. Advanced Information Networking and Applications (AINA), 2008, pp. 644-651.

[11] T. M. John, A. T. Ramani, and J. A. Chandy, "Active storage using object-based devices," in Proc. IEEE Int. Conf. Cluster Computing, 2008, pp. 472-478.

