Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.525 – 528

SELF-DESTRUCTION OF CIPHERTEXT IN CLOUD

Ms. Rekha S N[1], Ms. Guru Priya M[2]

[1]M.Tech Student, Department of Computer Science and Engineering, New Horizon College of Engineering, Bangalore, India

[2]Associate Professor, Department of Computer Science and Engineering, New Horizon College of Engineering, Bangalore, India

[1] rekhasnreddy@yahoo.in; [2] priyamano89@gmail.com

Abstract— In this growing age, it is very important to secure data and one of the best way to secure data is cloud computing. It is widely used by many corporate companies to store their data safely. But it is very difficult to provide full protection to cloud and also a challenge to control the bulk users accessing data in cloud. So we propose a key-policy attribute based encryption with time defined attribute. By this approach the cypher text will be self-destructed after a specified expiration time. Here cypher text is tagged with time interval in which file up loader can set the time duration while uploading the file. The cypher text will be decrypted if time instance at both the ends are matched. Also provides a fine grained access control by supporting user defined authentication period.

Keywords— Cloud computing, Security, Self-destruction, data privacy, time interval, AES algorithm.

I. INTRODUCTION

Cloud Computing is one of the most emerging technology from a decade it has changed the way the organizations using technologies, making them to easily available for the users anywhere any time with reduced costs. The user's sensitive information which is stored in cloud is secured (e.g., secret, important information). Since pay per usage facility is provided which attracts the business and IT sector people to us the cloud. As the cloud is adaptable to any working environment the cloud is more prone to attacks which will cause damage to the stored data in the servers. The unknown parties in the middle will hack the data which is great loss to the user.

To tackle such a problem a system is required which is reliable, redundant as well as secure. Now a days the main concentration only on the front end with some attributes, user ids, passwords and keys generated. But there are more chances for malicious hackers to gets access to the front end by knowing the passwords will get into the cloud and access the important information which is stored. So we need to secure both the front end as well as middle end which provide more security for the system.

So we are proposing the system which focuses on the middle end security more. The methods used here are time stamp, KP_TASBE Self-Destruction and AES algorithm for encryption and decryption. Self-destruction is introduced by encrypting the data with AES key and

Self-destruction is implemented by encrypting the data with a key and collecting the decryption key with the users. The KP_TSABE will solve some of the important security problems by providing user defined authorization and secured access control during this period.
The secured information will be self-destructed after a user specified time expires. Since the data is destructed the malicious users will not get the information as it is self-destructed and moved to other locations. And even if they get accessed the data will be of no use since it is decrypted with AES key. The hackers can perform all the activities in a time interval, if not they have to start from the beginning as the session will not exists.

II. RELATED WORK

N S Jeyakarthikka et al [1] the personal information which is stored in the cloud will be 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. Ranjith K, et al [2] concluded that the self-destruction system automatically deletes all the information which is no more required to the user. When 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.
Jinbo Xiong et al. [3] proposed that the data stored in the cloud will be destructed if an unauthorized access is detected. This detection is based on the time interval and the attributes associated with cipher text. Kishore K et al. approach provides the latest functionalities and the system also feasible to use in a cloud environment. 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 period of time. First encrypt the data into cipher text using AES encryption and the provide decryption key and cipher text to the user.

III. EXISTING SYSTEM

To protect the privacy of the data in a cloud is a very big challenge especially in cross cloud and big data environment since the ownership of the data is divided by the administration the cloud servers may migrate the user data into other cloud. To meet this challenge, design a solution which supports the user-defined authorization and provide a fine-grained access control to the users. The data which is shared is to be destroyed after the user specified time expires. Encrypted form is one of the method to store the data in the cloud but this format cannot be shared at the access level. Whenever the user want to share the information, he must know exactly to whom the data is to be shared.
The disadvantage of the system is that the hacker will get into the system at access level and misuses the secured data. The data owner should know the other whom he wanted to share the data. Key policy based time encryption is proposed which has many advantages where multiple users can download the information at a specified time.

IV. PROPOSED SYSTEM

The gradual increase in the business and the IT sectors, the cloud services has a vast demand. As the cloud services grows, a lot of new challenges has emerged. One of the very basic problem is security. How to secure the sensitive data on servers safely?
So in this paper we propose a concept KP-TABE method which is able to solve some of the problems of the cloud storage environment. The time interval is specified while uploading the information to the cloud by the user. Also a flexible access control is provided during the authorization period. The user specifies the time, once this time expires the data which is stored will be destroyed automatically so that the data can be secured from the unauthorized agents. The AES algorithm used for encryption and decryption.

V. METHODOLOGY

The method which we proposed here solves some problems so that the data stored in the cloud can be secured. Here the time interval is required. While the user uploading the information he will set the time. Within the time interval the user should download the information from the cloud. Before the time expires the user can have access to get thee data. Once the time expires then the data in cloud automatically destroyed so that the data is secured. Also unauthorized agents will not be able to get the data.
While user uploading the file, it will be stored in cloud in the encrypted format by AES encryption key, the stored data will be different blocks depends on the size of the data uploaded. User can download the data by decryption key before the time expires as it gets destroyed automatically. Once self-destroyed the user should recover data from the cloud.

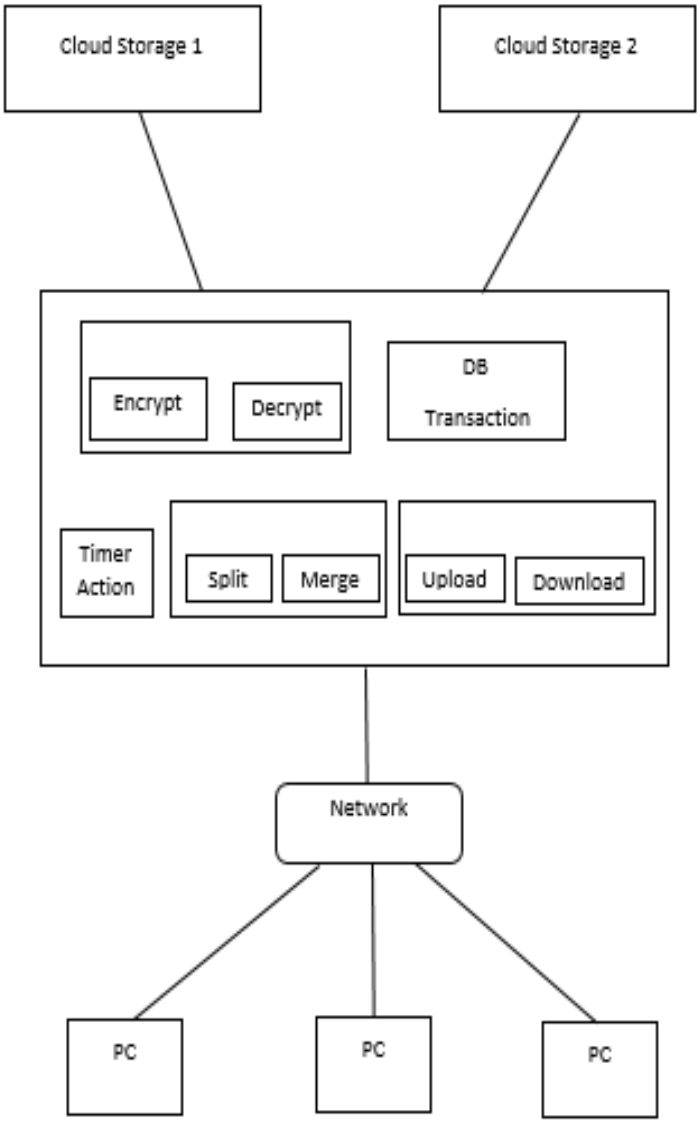

Fig. 1 Architecture of Proposed System

The above figure shows the architecture of the scheme used to self-destruct the cipher text after a specified time expires. After the data is self-destructed and if the user wants the data, he should send request to the uploader so that the uploader recovers data from other cloud and uploads again. Once the data is requested it should get approved by the admin.

There are many advantages in this proposed system which provides security to front end as well as the middle end of the system. Also provides a self-destruction method which reduces the complexities in the cloud and secures the data as well. The possibility of data being theft also reduced.

VI. CONCLUSION

Cloud computing has the wide range of users, increasing the data privacy became very essential in the storage environment. The data should be protected from the hackers which may include personal, legal and sensitive information. If hackers gets the data, there is a chances of misuse. So to avoid the risk factors, the approach introduced here provides a solution for data privacy. Here our system will help to improve the security by deleting the data in the cloud keeping a backup of the data. This provides a convenient way to secure the data in the cloud.

REFERENCES

[1] N S Jeyakarthikka, S Bhaggiaraj, 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.

