ISSN 2395-1621

A Survey Paper on Advance Security in Cloud by Cypher Deletion using Self-Destruction

[#1]Swapnil Jumale, [#2]Darshan Kuyate, [#3]Pranav Bansod, [#4]Kanhaiya Ufade,

[#5]Prof. Vaishali Bhorde

[1]srjumale@gmail.com
[2]ddotkuyate@gmail.com
[3]pranavbansod2010@gmail.com
[4]kanhaiyaufade2012@gmail.com

[#1234]Department of Computer Engineering
[#5]Prof. Department of computer Engineering
JSPM's
Imperial College of Engineering and Research
Wagholi, Pune
.

ABSTRACT

In this growing age of computing, it is very important to use cloud for sharing data. On preliminary basis it is very essential to secure data on cloud. It is very difficult to give full privacy centered security to cloud and also accessing the data by bulk of different users results controlling becomes the challenging task, so to tackle this problem, [1] we are using a proposed approach of key-policy attribute based encryption with time defined attribute (KP-TSABE).In this scheme the sensitive cypher text of data will be securely self-destructed after a user specified expiration time. In this scheme cipher text is tag with time interval, while private key is associated with time instant. The cipher text will get automatically decrypted if time instant of both the end gets matched. It also supports access control during the period by supporting user defined authentication period. With this kp-tsabe for enhancing security [2] cypher text of data will get destructed not only to the single cloud with the augmentation of security we also provide an enhancement of based applications for providing a better cloud data storage decision, taking into consideration the user budget as well as providing the best quality of service for the user. This scheme is proposed by us to satisfactorily provide the privacy based security scheme in cloud data storage.

ARTICLE INFO

Article History

Received :18th October 2015

Received in revised form :

18th October 2015

Accepted : 22th October , 2015

Published online :

23th October 2015

Keywords: **Cloud computing, Data privacy, self-destructing data, cloud security**

I. INTRODUCTION

Cloud computing the most developing technology of the decade has changed the way organizations using IT technologies, enabling them to become more easily available anywhere any time and with reduced costs. Cloud storage covers mainly user's sensitive information (e.g., Secret, Important information etc.). As the cloud computing is attracting the business and IT sectors because of its Pay per usage term. As being more used the cloud are more to prone attacks which may cause harming the stored data in cloud servers. To overcome such a problem there is required a system which will be reliable as well as more secure and redundant. But As per todays scenarios the main focus is only on securing the front end with some passwords, keys, otp's, etc. But what if the malicious (Hacker) user gets the access to the front end then he will be able to get into the system and access the data. So what if the front as well as the middle ends is secure. This will give more security to the system.

So here we are proposing the system which will have more concentration the Middle level security. The methodologies used in our system will be the Time stamp, [1] KP-TSABE Self-destruction. As the user login there will be duration for the session. [2][7][9] If found the user is malicious then Self-destructing systems is designed to address these concerns. The aim is to destroy cypher text of data after a specified timeout. Self-destruction is implemented by encrypting the data with a key and then escrowing the info needed to recollect the decryption key with one or more third parties. The KP-TSABE is able to solve some important security problems by supporting user defined

authorization period and by providing secure access control during this period. The sensitive data will be securely self-destructed after a user-specified expiration time. I) First of all the malicious user will not get the access to the data as it is self-destroyed and moved to random locations, II) And even if he gets access to one of the location then the data will be of no use as the data is encrypted, III) the malicious user will have to perform all this activities in a given time stamp, if not the he will have to start from the beginning as the session will no longer exist.

II. LITERATURE SURVEY

Jinbo Xiong et al. [1] had proposed the system the data stored on cloud would be self-destructed if an unauthorized/adversary is detected. The detection of unauthorized/adversary agent is based on the time instant is in the allocated time interval and the attributes associated with the cipher text fulfill the key access structure. N.S.Jeyakarthikka et al. [2] stated that first encrypt the data into cipher text and then distribute both the decryption key and the cipher text into a distributed hash table. To recover the plain text, both the decryption key and the cipher text should be obtained from the DHT before the pre-configured period of time. Ranjith.K, et al. [8] concluded that self-destruction system all files are removed automatically if those are no more needed. Also, the time period for sharing can be explicitly fixed by data owners while uploading the files itself. We strongly believe that the system will reduce complexities in managing old data files and thereby increasing possibilities in reducing security and privacy issues. Kishore K et.al [7] this approach provides the latest functionalities in its scope. The system is also feasible to use in a standard cloud environment. The experiment will serve as a base for the future researchers in the scope of self-destructing data. Future work will include the integration of additional algorithms for encrypting video files and other formats. N.S.Jeyakarthikka et.al [3] Personal data stored in the cloud may contain account numbers, secret codes and other necessary details that could be used and misused. These data can be cashed, copied by cloud service provider without user's control. We propose a self-destructing data which mainly aims at protecting the user data's privacy by making the sensitive data automatically destructed after a period of time. First encrypt the data into cipher text and then distribute both the decryption key and the cipher text into a distributed hash table.

III. EXISTING SYSTEM

As the ownership of the data is divided from the administration of them, the cloud servers may migrate user data to other cloud servers. Therefore, it becomes a big challenge to protect the privacy of those data shared in cloud, especially in cross-cloud and big data environment. In order to meet this challenge, it is necessary to design a wide-ranging solution to support user-defined authorization period and to provide fine-grained access control during this period. The shared data should be self-destroyed after the user-defined expiration time. [4] One of the methods to ease the problems is to store data as a common encrypted form. The drawback of encrypting data is that the user cannot share encrypted data at a fine-grained level. When a data owner wants to share someone his/her information, the use must know exactly the use must know exactly the one he/she wants to share with In many applications, the data owner wants to share information with several users with reference to the security policy based on the users' authorizations. Attribute based encryption (ABE) has significant advantages based on the tradition public key encryption instead of 1-to-1 encryption because it achieves flexible one-to-many encryption. ABE scheme provides a dominant method to achieve both data security and fine-grained access control. In the KP-ABE scheme to be elaborated in this paper, the cipher text is labeled with set of descriptive attributes. [1]Only when the set of attributes satisfies the access structure in the key, the user can get the plaintext.

IV. PROPOSED SYSTEM

With the rapid development of different cloud services, a lot of new challenges have emerged. One of the most important problems is how to secure the data stored on severs. In this paper, we proposed a novel concept as KP-TSABE scheme which is able to achieve the time-specified cipher text with the use of in order to solve these problems by implementing flexible fine-grained access control during the authorization period and time-controllable self-destruction after expiration to the shared and outsourced data in cloud computing. We also gave a system model and a security model for the KPTSABE scheme. Furthermore, we proved that KPTSABE is secure under the standard model with the decision l-Expanded BDHI assumption. The Comprehensive analysis indicates that the proposed KP-TSABE scheme is higher to other existing schemes.

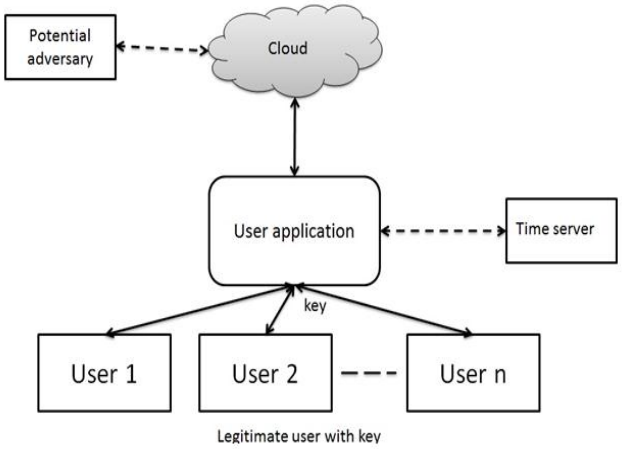

Fig 1. System Architecture

Advantages of proposed system:

- Safer front end as well as mid end of the system.
- Use of the self-destruction in cloud environment will lower the possibility of data being theft, misuse.

- Attribute based encryption (ABE) has major advantages based on the traditional public key encryption instead of one-to-one encryption because it achieves flexible advantages.
- [1]With regard to security and fine-grained access control compared to other secure self-destructing schemes.
- [1]Supporting user-defined time-defined permission, fine-grained access control and data self-destruction.

V. CONCLUSION

As the fade of cloud computing is increasing the data privacy has become the essential part in the Cloud environment. So the introduced approach is for protecting the data privacy from hackers. As data stored on the cloud may contain personal, legal, financial and other necessary details that can be used and misused. So our system will help to improve the data security providing a convenient way by deleting not actually the data but the cypher text of the data which is stored on the cloud taking the data security on the higher altitudes.

REFERENCE

[1] Jinbo Xiong, Student Member, IEEE, Ximeng Liu, Student Member, IEEE,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] Self-Destructing Data System Based On Session Keys-N.S.Jeyakarthikka, S.Bhaggiaraj, A.Abuthaheer INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 3, ISSUE 2, FEBRUARY 2014.

[3]B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014.

[4] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme incloud," KSII Transactions on Internet and Information Systems(TIIS), vol. 8, no. 1, pp. 282–304, 2014.

[5]M. Armbrust, A. Fox, R. Grifth, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A Berkeley view of cloud computing. Technical re-port, University of California at Berkeley, February 2009.

[6]R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. Cloud computing and emerging it platforms: Vision, Future Generation Computer Systems, 25(6):599–616, 2009.

[7] Kishore K, Ramchand V "SDD: A Novel Technique for Enhancing Cloud Security with Self Destructing DataInternational Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 4, April 2014.

[8] Ranjith.K, P.G.Kathiravan" A SELF-DESTRUCTION SYSTEM FOR DYNAMIC GROUP DATA SHARING IN CLOUD" IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[9] N. RamaKalpana, R. Santhosh" SeDas: SELF - DESTRUCTION DATA SYSTEM FOR DISTRIBUTED OBJECT BASED ACTIVE STORAGE FRAMEWORK" International Association of Scientific Innovation and Research (IASIR) ISSN (Online): 2279-0071.

