ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

Self-Destruction System for Protecting Data Privacy using Attribute Based Encryption

[1] Aboli Sarode, [2] Shruti Mohod, [3] Kavita shelke, [4] Shika Deshmukh, [5] Prof Shankar Gadhve,
[1][2][3][4]VIIth semester student, Department of Computer science and Engineering, Nagpur, Maharashtra, India,
[5] M.TECH student, Department of Computer science and Engineering, RCOEM Nagpur, Maharashtra, India
[1] srodeaboli29@gmail.com, [2]Shrutimohod115@gmail.com, [3]kavitashelke@gmail.com,
[4]shikadeshmukh02@gmail.com [5]Shankar_gadhve@yahoo.com

***Abstract:* — In Cloud Storage we store confidential data of particular organization or Software Company. Important information for developing software, and other such information that can be abuse by hackers or unauthorized person. Self-destruction System mainly aims at securing the user confidential data's privacy. In previous paper there is possibility to leak data to prevent previous sequence. In exiting system system used different technique to encrypt data, but In this paper, we present a system that provide more security for user valuable data and use different algorithm for encrypt data. We implemented automatic deletion performing system through the different methods and different security properties evaluations of this system. In addition to this the data privacy can be given to the system by encode the data. All the data and their copies become unreadable after auserspecifiedtime, without any user intermediates. In addition, the decryption key is destructed after the user-specified time.**

***Keyword:* -- Triggering parameter, Cloud data privacy, specific protocols for uploading the data**

***Domain:* -- Cloud computing, KGC, DSC**

I. INTRODUCTION

As storage framework and provides services which are becoming more and most important among people's life. People are requested to submit some personal information to the storage system. With development of Cloud computing and popularization of Internet, Cloud services are becoming more and more useful and important for people life .People are more or less requested to submit some cofidentional private information to the Cloud by the Internet. When people do this, they particular hope service providers will provide security to protect their data from leaking, so other people will not for any their privacy.

As people depend more and more on the Internet and Cloud technology, protect of their privacy take more and more hazards. On the one and, when data is being processed, transformed and stored by their computer system or network, systems or network must cache, clone or archive it. These copies are necessary for systems and the network. However, people having or about these copies and cannot control them, so these copies may leak their private data. On the other user, their privacy also can be leaked via Cloud Service Providers (CSPs') negligence, hackers some legal actions. These problems present form challenges to protect people privacy.

A pioneering study of Vanish supplies idea for sharing and protecting secure data [2]. In the Vanish system, a secret key is separated and stored in a point 2 point system with distributed hash tables (DHTs). With combining and entering of the point to point node, the system can maintain private keys. According to property of point to point, after about eight hours the DHT will renew very node.

II. LITERATURE REVIEW

A pioneering study of Vanish is the system that provides the basic idea of automatic deleting data [2]. In the Vanish method, a secure key is individual and stored in a point to point system with categorize hash tables. With joining and entering of the point to point method, the system can save the secure keys. According to parameter of point to point, the categorize hash tables will refresh every node after every eight hours. With using Shamir Secret Sharing Algorithm [5], when we will not accept limited parts of a key, it will not decrypt user data or data archives with this public key, which emphasis the public key is discard and the data cannot be recovered. Some special rush to characteristics of point to point are challenges of deleting, uncontrolled in how long the key can survive. Vanish is a system used for generate text messages that automatic performing deletion operation after a specific period of time. It contains cryptographic techniques with global scale; point to point categorize

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

hash tables. Categorised hash tables have the property to delete data older than certain time duration. In this the key is permanently vanish, and the encoded data key is permanently deleted after data terminates time. In Vanish system each message is encoded with a random key and storing share of the public key in a large.

III. OBJECTIVES

Objectives of Proposed System to implement a automatic deletion performing system and data privacy are as follows:-

The self destructive systems explain some modules [1], a self-destruct method and time to live property. In this case, System could meet the requirements of self-destructing system with triggering parameter people can use this protect system as a general active system.

Our objectives are briefly explained as follows.

1) We accent on the AES core algorithm, which is used as the main algorithm to implement users. We use these methods to apply a safety destruct with set of rules.

2) Based on active storage framework, we use an object-based storage interface to store and handle the equally separate key.

3) Through functionality and protecting properties evaluation of this prototype, the results established that System is practical to use and meets all the security goals.

4) System supports protected files and random AES encryption keys stored in a active storage framework or solid state drive, respectively.

5) Through functionality and privacy properties value of this method, the results demonstrate. System is more responsible to use and accept all the private goals. The method of the system can impose reasonable low runtime overhead.

6) System supports privacy deleting files from storage framework within specified protocols.

7) Advance encryption standard provide the data security.

8) Set of rules provides the information to be uploaded on active storage framework.

IV. PROPOSED METHODOLOGY

The self destructive system based on self-des defines new modules, a automatic deletion module that is associated with Set of protocols. In this paper, self destructive system can meet with the need of automatic deleting system with manageable protocols while users can used this system as a general active Storage system [4].

A) Active Storage Object

An active storage system creates from a user system and has a TTL value property. The triggering is used to delete the self-destruct method [1]. The time to-live *value* of a user object has the infinite value so that the user object will not be deleted until the user discard manually.

The triggering parameter is nothing but the TTL parameter which is used to activate the automatic deletion operation. The user decided by triggering parameter for how long time duration user wants the data on cloud storage and after the survival time period the data which is uploaded on cloud that will be deleted automatically once the survival time period is will over.

B) Self-Destruct Method

A self-destruct method is used to deleting the data from the cloud storage as per the protocol defines [1]. User specifies the survival time and data will be discarding from the cloud storage once the survival time is over. Show the pseudo code for the entire process of algorithm. Pseudo code starts with the registration of the user and validates the user with user id and password. The next part of pseudo code is about the Data Process.

C) Data Process

To use the self destructive system, applications client should apply logic of data process and application client node. There are two different types of Operations: uploading and downloading.

i) Uploading : When user uploads a file on cloud. The file gets encrypted before uploaded on cloud. User must specify the file and TTL as arguments for the uploading

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

procedure. Once the files have uploaded on the cloud storage, the data will be on the cloud only for the time which specify in time-to-live property. Once the time will over as mentioned in time-to-live property the file will be self destructed from the cloud environment [3].

ii) Downloading: Any authenticated user who has proper permission can download data stored in the data storage framework. The file get decode before when it is downloaded from the cloud.

V. RELATED WORK

A. Data Owner:

It is a client who personal data, and wishes to upload it into the outer data storing centre for comfort of sharing or for cost saving. A data owner is accountable for defining extract policy, and enforcing it on its own data by encoding the data under the policy before categorize it. Data Owner to get key from key generator Encrypt the file. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized user.

B. Data Storing Centre:

It is an object that provides a data sharing service. It is in charge of controlling the accesses from external users to the storing data and providing similar contents services. The data storing centre is another key authority that create personalized user key with the Key generation centre, and issues and revokes attribute group keys for only valid users per each attribute, which are used to implement a user access control. Data storing centre store the data. Data Storage Centres provide the offsite data and tape storage, retrieval, delivery and destruction services.

C. User:

This is an entity who wants to extract the data. If a user possesses a set of attributes satisfying the access policy of the encrypt the data explain by the data owner, and is not abort in any of the attribute groups, then he will be able to decode the cipher text and obtain the data.

D. Key Generation Centre:

It is a key authority that creates public and secret parameters for CP-ABE. It is in charge of issuing, aborting, and updating attribute keys for users. It provide authority to access rights to individual users based on their attributes. Key create is the process of creating keys for cryptography. A key is used to encode and decode whatever data is being encrypted or decrypted. Node Structure of a Data Sharing System. The nodes involved are admin and clients which stands as UI for the system. The nodes are Key Generation Centre (KGC) is a key authority that generates public and secret parameters for CP-ABE. Data storing center is an object that provides a data sharing service. The data storing center is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a user access control. It is a client who personal data, and wishes to upload it into the external data storing center for comfort of sharing or for cost saving. A data owner is responsible for defining access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. User is an object who wants to access the data.

VI. PROPOSED PLAN OF WORK

1. Study of the Existing System as well as Proposed System:-

In this module we will do study of the existing system and also of the proposed system and whatever disadvantage that are in the existing system we have to remove it and have to see that it does not occur in the proposed system.

2. Development of Active Storage Framework:-

An active storage object that is derived from a user object and has the same set of rules for uploading the data on active storage system. The set of rules are used to trigger the self -destruct operation [1]. The values of a user object is infinite i.e. user object will not be deleted until a user deletes it manually. The time-to-live value of an active storage object is limited so an active object will be deleted when the value of the associated Policy object is true.

3. Development of login tracking of the user:--

To use the Self destructive system, user's applications should implement logic of data process and act as a client node. There are two different methods: uploading and downloading.

i) Uploading file process: When a user uploads a file to a active storage system and stores his key in this System, he should specify the file, the key as arguments for the uploading procedure. We assume data and key has been read from the file. The ENCRYPT procedure uses a AES encrypt algorithm or user-defined encrypt algorithm. After uploading data to storage server, key generated by

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

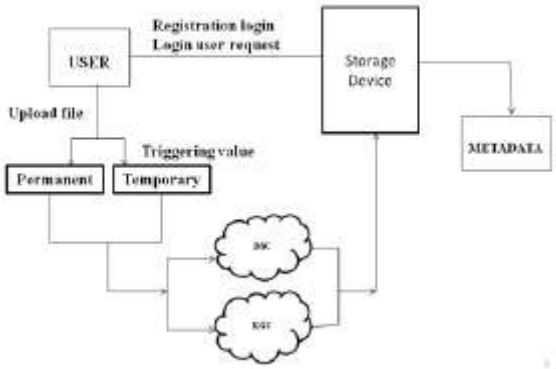
AES algorithm will be used to create framework storage object in storage node in the self destructive system.

***ii) Downloading process*:** Any user who has intended permission can download data stored in the framework storage system. The data must be decrypted before it is downloaded. The whole logic is implemented in code of user's application.

4. Development of deletion module in case user logs out:-

A self-destruction method is a active service method. It needs three arguments. The lug argument specifies the device; the pied argument specifies the partition and the object id argument specifies the object to be destructed.

Proposed Plan of Work



VII. CONCLUSIONS

Data security has become increasingly important in the Cloud storage. In this paper acquaint a new way for securing data secure from attackers who retroactively obtain, through legal or other means, a user's stored data and personal decoding keys. A novel aspect of our method is the leveraging of the essential properties of active storage framework.

REFERENCES

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

[2] 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.

[3] A. Shamir. Identity based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in Cryptology, pages 47–53. Springer Verlag New York, Inc., 1985.

[4] 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.

[5] A. Shamir, "How to Share a secret", Commun.ACM, vol.22, no.11, pp.612-613"Dec 2010.

[6] R.Perlman," File System design with assured delete, "in proc. Third IEEE Int. Security Storage Workshop (SISW), Dec 2009.

[7] S.W.Son, S.Lang, R.Ross, R.Thakur and B.Oziasikyilmaz and K.Liao,"Enabling Active storage On Parallel System" Jan 2012