**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**

*IJCSMC, Vol. 4, Issue. 3, March 2015, pg.604 – 606*

**REVIEW ARTICLE**

# Review on Self-Destructive System for Data Privacy on Web Services

**Ganesh Z Bhade[1], Vikrant Chole[2]**

[1]Department of Computer Science and Engg

[1]G.H. Raisoni Academy of Engineering and Technology, Nagpur, India

[2]Department of Computer Science and Engg

[2]G.H. Raisoni Academy of Engineering and Technology, Nagpur, India

***Abstract:*** ***Now a days more and more services and applications are emerging in the Internet, exposing sensitive electronic data in the internet has become easier. Web services causes personal data to be cached, copied, and archived by third parties, often without our knowledge or control. We propose a secure self-destructing scheme for data, which can protect a user's sensitive data by making the sensitive and important data automatically destructed after particular period of time. Specifically, we first encrypt the data into a cipher text. Then, we associate the cipher text, and extract a part of the cipher text to make it incomplete. There will be one time passwords to decrypt the data. In addition, a time-to-live (TTL) is integrated into the executable to provide an additional layer of security so that the data is only accessible within a defined time period.***

***Keywords: Data privacy, self-destruction, time to leave (TTL), web services.***

## I. INTRODUCTION

With development of web services and popularization of Internet, web services are becoming more and more important for people's life. People requested to post their private and personal data on internet. People rely on internet service provider their privacy and security takes more risks. When data is being processed, transformed, stored by computer system or network, one of them copy or archive the data. This data is essential for system or network. The copy of data is stored in the system or at the network may leak the privacy of user. Internet service provider can use this data without user knowledge and may misuse this data.

Self-destructive data scheme will self-destruct the data which get stored at client side in the form of cookies. Additional to this data which is to be stored at server side will be stored in encrypted form. To decrypt the

 

data one key will be generated which is valid for only one time. In addition Time to live (TTL) is provided which will increase security so that data is only accessible within a defined time period.

In this paper, Self Destruction (SeDas) present a solution to implement a self destructing data system, Which consist of two main parts: 1) secret key part-generate a pair of keys through RC4 algorithm. 2) survival time part-specify time limit to each keys. Through this it can meet the following advantages: 1) No explicit delete action by any third party. 2) The keys can be self destructed after user specified time and also reduces the communication overhead as well as network delay. 3)Increase processing speed and it will meet all the privacy preserving goals.

## II. LITERATURE SURVEY

1. Lingfang Zeng , Shibin Chen , Qingsong Wei , and Dan Feng SEDAS: "A self-destructing data system based on active storage framework" - This paper proposes a distributed object-based storage system with self-destructing knowledge operate. we tend to use SeDas system with the assistance of Shamir's algorithmic program for secure fund dealings. methodology} combines a proactive approach within the object storage techniques and method object, victimization processing capabilities of OSD to attain knowledge self-destruction. User will specify the key survival time of distribution key and use the settings of swollen interface to export the life cycle of a key, permitting the user to manage the subjective life-cycle of personal knowledge. Vanish may be a system for making messages that mechanically destroy once a amount of your time. The secret is for good lost, and also the encrypted knowledge is for good unclear once knowledge expiration. Vanish is a motivating approach to a very important privacy downside, but, in its current kind, it's insecure. Vanish is that the previous approach of the Sedas System, it additionally supported key generation algorithmic program however at a time it generate just one key thus rather than that Sedas generate multiple keys with the assistance of shamirs algorithmic program thus its higher for security purpose. Also, we tend to bestowed Associate in Nursing improved approach against sniffing attacks by means of victimization the general public key cryptosystem to stop from sniffing operations.

2. Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "FADE: Secure overlay cloud storage with file assured deletion," FADE, was proposed by tang et al provides a contribution for the self destructing data by integrating cryptographic techniques. The data will be encrypted before sending it. This system will delete the files and makes them unrecoverable by revoking the file access permissions. Another system called File System Design with assured delete proposes three types of file delete. First is the expiration known at the time of file creation, second is on demand deletion of individual files and third is the usage of custom keys for classes of data.
As given above, many systems have been proposed to implement a self destructing system among which only some provide promising results. The system doesn't have a user controllable data expiration time. They rather have a fixed time for file expiration which is not an efficient approach for the self destructing scenario.

3. R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," Vanish is the system that provides the basic idea of self destructing data. The system developed is a prototype which is implemented using Distributed Hash Table (DHT). It used bittorrents Vuze DHT that can support eight hours timeout or Planet Lab hosted Open DHT that can support one week timeout. This system provides a plug-in for Firefox browser that creates a message which automatically disappears after a specified period of time. Here the expiry time for the data is controlled by the DHT and not by the user. Later many extensions are been implemented on the Vanish system

4. J.A.Chandy, M.John and T.Ramani "An Active Storage System for High Performance Computing", Traditional active memory device execute custom application code on large amount of knowledge by utilizing the unused process power of the storage nodes for computation intensive application, the performance could be quite low thanks to insufficient process power of storage nodes.

 

5. H.Chai, D.Feng, C.Li and K.Zhou "Implementing and Evaluating Security Control for Object Based Storage System" The development of high performance computing has based on storage capacity and I/O performance, storage system has entered the peta byte era. The storage system scale of high performance computing is very large, the amount of storage nodes is very huge.

6. Carns, P.Choudhary, S.Lang, B.Ozisikyilmaz and S.W.Son "Enabling Active Storage on Parallel I/O Software Stacks" As data sizes continue to increase the concept of active storage is well fitted for many data analysis kernals. The sedas system propose and
evaluate an active storage system that allow data analysis, mining and statistical operations to be executed from with in a parallel I/O interface.

7. Disha Handa, Bhanu Kapoor PARC4: "High Performance Implementation of RC4 Cryptographic Algorithm using Parallelism" India RC4 is ideal for storing information that is highly sensitive and highly important. A RC4 method can secure a secret over multiple servers and remain recoverable despite multiple server failure. The dealer may act as several district participants, distributing the shares among the participants. Each share may be stored on a different server, but the dealer can recover the secret even if several servers break down as long as they can recover. The algorithm divides a message into fix sized large blocks and encrypts these blocks concurrently on multi core machine.

## Conclusion

Authenticated user, the RC4 generate a pair of keys also the user specify the lifetime of each keys. After user specified time the keys can be self destructed without user intervention. During the download process the RC4 check the validity of the keys. If the keys are expired, The RC4 generate new pair of keys to the user through this only the sedas system meet all the privacy preserving goals. The future work of the sedas system further to increase the key length to provide user data privacy in web infrastructure

## References

[1] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "FADE: Secure overlay cloud storage with file assured deletion," in Proc. Secure Comm, 2010.
[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," in Proc. IEEE INFOCOM, 2010.
[3] 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.
[4] P.Carns, A.Choudhary, S.Ozisikyilmaz and S.W.Son "Enabling Acyive Storage on Parallel I/O Software Stacks" Mar.2010
[5] H.Chai, D.Feng, C.Li, w.Yingping and K.Zhou "24th IEEE Conf.Mass Storage System and Technologies(MSST), QOS Provisioning Framework for an OSD based Storage System" Jan 2011.
[6] D.Feng, Y.Kang, K.K.Muniswamy Reddy, Z.Tan and Y.Xie "Design and evaluation of oasis: An Active storage based on T10 OSD standard" Dec 2011
[7] Disha Handa, Bhanu Kapoor PARC4: High Performance Implementation of RC4 Cryptographic Algorithm using ParallelismICROIT 2014, India.
[8] Y.Kang, E.Miller and J.Yang "Object Based Storage Class Memories:An effient interface for SCM" in Proc.27th IEEE symp. Massive Storage System and Technology in April 2009.
[9] A.Shamir, "How to Share a secret", Commun.ACM, vol.22, no.11, pp.612-613"Dec 2010.
[10] R.Perlman," File System design with assured delete,"in proc. Third IEEE Int. Security Storage Workshop(SISW), Dec 2009.
[11] S.W.Son, S.Lang, R.Ross, R.Thakur and B.Oziasikyilmaz and K.Liao, "Enabling Active storage On Parallel System" Jan 2012.
[12] Y.Tang, P.P.C.Pee, J.C.Lui and R.Perlman, "FADE: Secure Overlay cloud storage with file assured deletion," in proc.Secure Comm, Mar 2010.
[13] H.Chai, Z.Niu, W.Xiao and K.Zhou "Implementing and Evaluating Security in cluster storage system" Feb 2011.
[14] A.Devulapalli, T.Murugandi, D.Xu and P.Wyckoff, "design of an Intelligent Storage Devices "April-2012.

 