IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Performance Evaluation of Trigger Driven Zero Remnance Proof Based Data handling for Digital Forensic

Pooja Bhavsar[1], Rakesh kumar Lodhi[2]

PG Scholar, Computer Science and Engineering, P.C.S.T., Bhopal, India[1]

Assistant Professor, Computer Science and Engineering, P.C.S.T., Bhopal, India[2]

Abstract: In today's world web based system security scenario and storage services is getting popularity among individual users and the associations. It involves open medium information exchanges over insecure channels. To present better security against the open vulnerabilities we should be assured about the security offered by those systems. To make the system more secure and strong against the attacks, effective confidentiality and integrity techniques have to be implemented concurrently with designing the new communication system. This work proposed a novel trigger driven zero remnance proof (TD-ZRP) approach for improving the data security. It makes deletion/removal complete following the forensic properties embedded with the data lifecycle events. The approach is using the active object phenomenon which uses attach metadata for activating the events consequently. This paper also presents the result evaluation of proposed approach in comparison with some of the well known existing methods.

Keywords: Information Exchanges, Security, Self Data Removal (SDR), Lifecycle.

I. INTRODUCTION

Data lifecycle management is one of the major activities performed to effectively analyze the period for which the data is used and includes its complete phase transitions. One should always focuses on the lifecycle of the data means when the overall of living period of data is over then it needs to be removed completely with all its local and permanent copies [1]. Most of the organizations have the several policies for this data destructions based on the fixed time interval. But as of now the copies or replicas of data is getting multiplicatively increased so deleting all in a single go is very difficult. Also the deletion is not complete and some residues metadata remains at the location of the files from which the recreation of data can be performed. Data destruction is the process of deleting the data and its overall components and copies when the lifecycle of its operations is finished [2]. The deletion should be in such a way that its reconstruction cannot be performed but many organizations are unable to achieve such behavior and hence left a vacant space for attackers to regenerates the copies of original and forged some other services by the same [3].

The removal of data is quite a complicated task before which the total number of copies which is generated has to be identified. Whenever a file is replicated some information needs to be attached there in its replica about its previous file location and total number of replications applied by which all the same existing copies is located and deleted. Most of the organizations are unable to perform such forensic deletion or destruction of data from the storage and always have vulnerability of data regeneration attacks [4]. Thus this work gives a brief study of such issues and provides a solution to overcome the existing data destruction issues.

Self-destructing data systems are designed to address these concerns. Their goal is to destroy data after a pre-specified timeout, regardless of where the data is stored or archived and despite technology that may make such deletion challenging.

As a result, such systems prevent the exposure of "old" data that is past its useful life. Self destruction is implemented by encrypting data with a key and then escrowing the information needed to reconstruct the decryption key with one or more third parties [5]. Assuming that the key reconstruction information disappears from the escrowing third parties at the intended time, encrypted data will become permanently unreadable in following situations:

(1) When an attacker have a encrypted data copy [6]
(2) When the users forgot to remove the temporary files from the system
(3) Can't be able to modify any of the stored or retrieved content of users authorized data
(4) Even if the user is not having any reliable hardware of access locations

Once the key-reconstruction information disappears, data owners can be confident that their data will remain inaccessible to powerful attacks, whether from hackers who obtain copies of backup archives and passphrases or through legal means. Control over data lifetime will become increasingly important as more public and private activities are captured in digital form, whether in the Distributed or on personal devices [7].

Self-destructing data systems can help users preserve some control, by ensuring that data becomes permanently unavailable after a pre-specified timeout. We now describe

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

key properties of our threat model for self-destructing data systems and review how Vanish addressed these properties as background for understanding our current work.

II. MOTIVATION

Self data removal or destruction is the configured policy of the system which enables the instances of objects to be removed from system automatically after their usage time or lifecycle is over. By implementing such solution the storage capacity is also saved along with improvements in security. At the analytical evaluation and measurement, the approach is serving the user's needs for improved security and optimized storage. The work had also focused of specific designed synchronous operations. Whenever the data usages period or lifecycle of the data is over, the self destruction mechanism is called which removes the data completely with all its remnance proofs. Here the networked storage can be used for improved performance over accessing the storage locations. It holds the actual data encapsulated in an object with the destruction time. The server calls the deletion time or the stored object with destruction time triggers the safe removal of the data from the location. The full secure version of object is stored at the storage location with fixed destroying time so the copies can't be created from this and if it occurs than it destroy the object copy also. After the final operations of data removal the ZRP transmits the acknowledgement is sent to the sender. Realistic performance of solution can be achieved by applying the above method for both HDD and TD-ZRP storages.

III. LITERATURE REVEW

During the last few decades various approaches had presented to effectively handle the storage issues regarding their security concern. Here we present some of the related articles which somewhere derive us to design the novel phenomenon.

The paper [8] proposes a scheme for Zero Data Remnance Proof (ZDRP). It uses two methods of comprehensive data shredding has been consulted for this task, Kishi's methodology by which data may be shredded comprehensively within a storage subsystem and the Gutmann algorithm which provides a similar methodology for secure deletion of data. They have presented here a scheme for Proof of Zero Data Remnance (PZDR) in a web environment. The focus of our work is on a probing engine/destructor which will probe the environment and based on the rules on the data store, will shred them partially or fully. This prototype can further be extended as a service on Web. This destructor will systematically modify/update the most significant bit of every data chunk, thus ensuring that the data is so corrupted/ impaired that no part of the data will make any sense to whomever gets hold of it later.

Some of the authors focus on the encryption mechanism for securing the users data and metadata. Likewise suggested in the paper [9], in which a formal cryptographic based model for secure deletion is given. According to it the deletion or removal can be monitored by several policies of data removal from storage systems whose security totally relies on some of the cryptographic functions and keys. They work regularly maintains some of the deletion class in which the members are regularly updating their entries and those who required complete removal can be erased automatically with all its related entries. A prototype implementation of the approach is proving its efficiency through Linux based file system. The approach has been validated through a prototype implementation of policy-based secure deletion in the form of a virtual file system layer of the storage system stack. It is coming with a pragmatic approach to show typical attributes from practical systems through defining a suitable policy graph.

Some of the authors also focused their intentions towards the deletion of less important data or used data from the P2P systems. In such systems the type of attacks occurred due to remaining residues of the deleted files is very high. Specifically the copies related to the data have to be taken over specifically because their locations are different from the actual copies. In the paper [10] a Vanish system is proposed for completely removing the data using a global scale cryptographic technique and web hash table container. The method had also applied a prototype for the suggested mechanism in OpenDHT Vuze Bit Torrents application online. Practical evaluations of the approach can be applied by adding a plug-in for different browsers. In Vuze, for example, the fixed data timeout and large replication factor present challenges for a self-destructing data system. Therefore, one exciting direction of future research is to redesign existing DHTs with our specific privacy applications in mind. Our plan to release the current Vanish system will help to provide us with further valuable experience to inform future DHT designs for privacy applications.

Carrying forward the above approach of Vanish and updated model Safe Vanish is proposed in [11]. This is an improved mechanism by which the data can be able to destruct itself after the end of use and increases the privacy parameter. The approach implements a threshold function k for generating the composite key. It sustains the self destructing nature by limiting the attacker's prone zone and sniffing the attacks in real systems. At the primary work stages and implementation prototypes is proving the efficiency of the suggested approach.

In the paper [12], there are three modifications suggested which includes cascading operation, triode operation and Existing Vanish mechanism. On the basis of above mechanism improvements in the existing destruction phenomenon is measured. According to cascade operation, multiple key storage system is taken as a combined system which increases the attack resistance. Similarly tide is a new key storage phenomenon through apache servers online. Various attacks and their preventions is simulated after applying the suggested approach and measured a performance improvement and applicability generalization by Vuze, Open DHT and Vanish. The calculated result shows that these defenses provide a countable improvement over the original Vuze DHT, which is

DOI 10.17148/IJARCCE.2016.5248

impractical in most of the situations. It also depicted the Cascade architecture, an extensible skeleton for coordinating heterogeneous key-storage frameworks. Generally speaking, Elaborate accept that this work moves handy destructing toward oneself data frameworks much closer to reality.

Thus the aim is to remove all the data and its copies completely from the server and storage locations. It makes the data privacy a stronger hand over other security parameters. Most of the existing mechanism is suggesting the approaches based on copies, but none of them focusing on complete deletion. Complete removal and self destruction is the primary aim of the approach SeDas in [13]. It causes sensitive information, such as account numbers, passwords and notes to irreversibly self-destruct, without any action on the user's part. Our measurement and experimental security analysis shed insight into the practicability of our approach. Our plan to release the current SeDas system will help to provide researchers with further valuable experience to inform the future object-based storage system designs for Web services.

Carrying forward the approach of active storage, this paper gives a virtualization realization phenomenal of applications running at client ends and the data treated as an object by which the throughput and latency is increased [14]. Here the virtual machines are acting as an active object and generating keys for each of the active partitions. By using this mechanism the encrypted files are uploaded and downloaded from the server using the agent structure. The evaluations and verifications apply in both the cases of uploading and downloading to check the authenticity of process, application and the user. The proposed concept in this paper is self-destructing data. There is an extensible framework for integrating multiple key-storage mechanism into a single self-destructing data system. It has the different key storage approaches to provide security against the attacks. In self-destructing data system, all copies of the data permanently unreadable at the user specified time.

The article given by [15] presented a disk based erasing mechanism for P2P systems which can be further modified and can be used for Web and storage technologies also. The mechanism is serving a simple understanding about the complete removal of the data from the servers or storage locations which practically containing some of the disks which needs to be erased. They are dependent on the policies, serving the user's needs about the self data disposals after a fixed time period of data Lifecycle.

User required the clean data removal from the existing medium through these policies. This article gives an option answer for data erasure software is a hardware gadget called a degausser. A degausser utilizes solid magnetic fields to demagnetize a drive – destroying the data in the process.

IV. PROBLEM STATEMENT

As studied in various research papers there are so many systems which are performing the self destruction of data like Vanish and SeDas [16]. But still there are some unsolved issues which the approaches faces while performing these automatic destruction incomplete manner. Thus, this work had identified a few of the working are for operating on such deletion actively. After the deletion the removal of data is not complete and there exist its residues which might be able to reconstruct the data. Lifecycle factors must be added with each data and their removal and migration policy must be operated in such a way that controls the dynamic demand of data.

This condition gives the customer trust over the asserted information suggests for any progressions the modification will be uniform and will redesign to the all current copies of the same information. In fact, with destruction all the copies must be emptied completely. In the meantime the current framework is not ready to achieve this destination. In the wake of considering the different examination articles, this work shows a novel TD-ZRP approach for improved trigger driven zero remnance proof for satisfying the contrivance of completion. Here, recommended approach satisfactorily uses the element to move and controlled the change with consistency in nature. By this framework, progressions joined will be reflected to every one copy with synchronous operations even with the wiping out or clearing furthermore.

V. PROPOSED WORK

Security is the major concern for large organization and individuals as well. It mainly deals with protecting the confidential or important information. Sometimes it might be intentionally affected or theft but most of the times there is some human mistakes which gives a way to loss that data. Thus, zero remnance proof works for complete data removal with all its replicas. Deletion must be initiated after a specific condition was met and when we are dealing with the lifecycle then the expiration time is considered to be the specific condition. Data lifecycle is a information management toll having details regarding the phases from which an information transforms starts from the generation to the removal. The users and organization will generate the single copy of data but during its lifecycle it travels from different nodes and devices and goes though several changes which causes temporary copies generation along with multiple replicas of same data or serialized data. In such distributed nature of data we need to take care about each copy of data along with temporary metadata to be removed as a security constraint after the task is completed. Some of the processing system will also generates the local copy or replica of data before working directly on the primary copy. All the modifications are performed on that temporary view and once the task was completed then these changes was reflected on the main copy. But after the changes these copies must be removed completely else it was used somewhere by the malicious users. S

This work proposes a novel model which deals with the lifecycle deletion phase with triggering events using an automated destruction mechanism. As it removes all the copies, replicas, temporary data, meta-data and serves

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

complete deletion we called it as Trigger Driven Zero Remnance Proof (TD-ZRP) [17]. The work is having an active object phenomenon which controls the deletion with an attached trigger elements for auto initiated deletion event. The system was implemented as prototype in web based architecture having some more security primitives added for getting the robust protection against the attackers. This paper will shows the performance evaluation of proposed work in comparison with the existing mechanism. The suggested zero remnance mechanisms is having different types of trigger associated for selective conditions applicable on various situations. Triggers will define the initiation conditions after which the complete destruction is called or zero remnance is guaranteed. For authenticating the sender and the receiver the data is having a controlled access which is maintained and recorded using the executable. Once the data is distributed then the removal is assured after the trigger condition is met even without any other interaction from the sender. The approach suggests the two type of trigger i.e. time and read count.

VI. RESULT ANALYSIS

The suggested approach of TD-ZRP is serving the different aspects and hence shown an implemented proof of concept. The approach is also handling the replica distribution and will maintain the complete record of the overall copies generated for a particular file. It also handles the changes which is applied in the primary copy and will be replicated in its secondary copy. The above intension is kept in the mind for generating the results so as the final output can be measured and evaluated. Here in results analysis the proof of concepts is formulated into some parametric evaluation for their accurate quantitative assessments. At the level the approach is serving all its requirements and showing its great presence towards making a place to win for user. Also the control must be regularly monitored and verified against each minute detail such as response time etc.

Table1: User Details

S. No	User Name	User ID	Get Details (Hyperlinked)
1	Admin	1	Get Details
2	A	2	Get Details
3	B	3	Get Details
4	D	4	Get Details

Table-2: Get Details User Activity Description

S. No	User ID	Title	Length (Bytes)	Time Taken (ms)	Trigger Attached
1	1	File Length	8802	47	Read Based Count
2	1	Chat Length	26	0	Min
3	1	Chat Length	11	16	Min
4	1	Message Length	19	0	Sec 10
5	1	Chat Length	6	0	Sec 10
6	1	Message Length	10	0	Time Based
7	1	File Length	516424	93	Time Based

The table 1 and 2 cover the system usability and analyses the systems performance by making the file exchanges securely. It also restricts the unauthorized distribution of the replicated copies along with the self destructive trigger assessment. The main analyses are shown in the table two where the trigger options are evaluated by measuring the file length and the trigger application execution time for efficiency analysis.

Table 3 Summarized Data

S. No	UID	Service	Avg (Data in Bytes)	Avg (Processing Time)
1	3	Message	18	2.0
2	1	Chat	16	4.0
3	1	Message	10	1.15
4	1	File	262613	70.0
5	4	Chat	19	1.28
6	4	Message	11	16.0
7	4	File	17457	62.0

Here the service used is to perform the triggering operation along with the size of the data used against that service for exchanging the information. Normally the comparison is made with respect to the size of the data transmitted to the time required for that transmission.

Table-4: Security analysis of Proposed TD-ZRP (txt)

User	File Type	Size (Bytes)	Encryption Time (ms)	Decryption Time (ms)	Trigger Attached
abc	txt	100	87	12	Read
abc	txt	200	317	19	Count
def	txt	540	92	32	Read
def	txt	670	456	34	Count
pooja	txt	800	126	40	Read
pooja	txt	900	659	67	Count

Table-5: Security analysis of Proposed TD-ZRP (jpg)

User	File Type	Size (kb)	Encryption Time (ms)	Decryption Time (ms)	Trigger Attached
abc	jpg	10	3.17	1.9	Count
def	jpg	13	4.12	3.4	Read
pooja	jpg	30	6.59	6.7	Count
efg	jpg	40	7.7	5.4	Read
hij	jpg	56	5.4	9.2	Count
klm	jpg	60	8.1	8.1	Read
Pooja2	jpg	100	72	6.7	

Table 4, 5 & 6 describes that the working efficiency of proposed TD-ZRP on security parameters and working efficiency.

Table 6 Throughput Comparison of Security Approaches

Size (Kb)	Encryption Time (Sec)			
	DES	AES	Blowfish	Proposed TD-ZRP
10	7.5	11.5	4	3.17
13	10	14.7	4.7	4.12
56	50.25	24.5	15.7	5.4
100	92.8	40	45	72
Avg. Throughput = Size/ Time	1.2	1.63	2.763	4.51

DOI 10.17148/IJARCCE.2016.5248

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

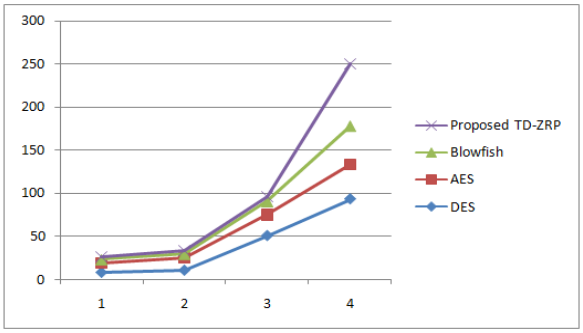


Figure 1: Comparison of Elapsed Time of different Algorithm with Proposed TD-ZRP

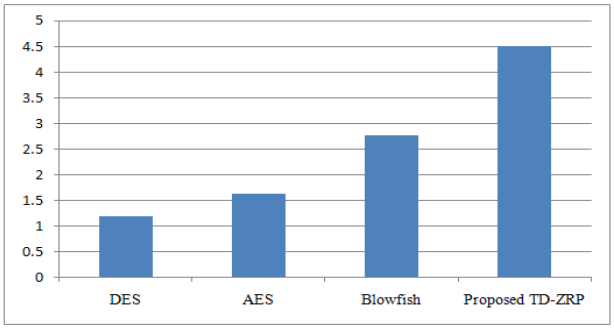
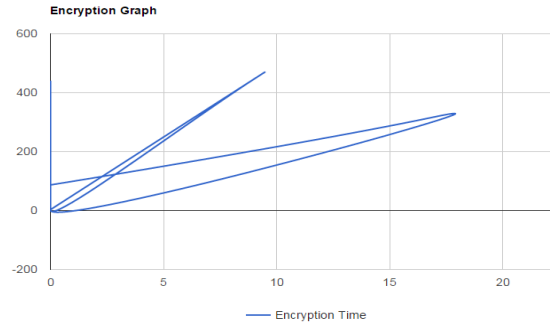
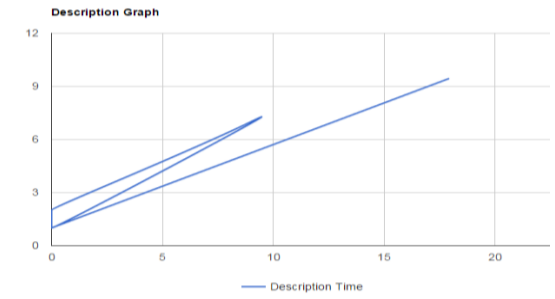


Figure 2 Comparison of Throughput different Algorithm with Proposed TD-ZRP

Description: As shown by above graph and the table 8 the proposed TD-ZRP is showing effective throughput gains while comparing the values with traditional approaches. Also the elapsed time for processing the different file sized data shows the working efficiency of suggested mechanism. Also the chart shows the throughput comparison in which the proposed work is leading with size per time encryption performed on other algorithms.



(1) Encryption Time



(2) Decryption Time

Figure 3 Encryption and Decryption Time Graph of Proposed TD-ZRP using RSA

Description: The above graph shows the system outperforms the various considered parameters over the traditional approach. It also gives the time based and robust analysis of the security offered by the system. While comparing the results we found the text based small size data is giving better results than the file based auto removal due to the dependencies of file trigger execution on the system files and privileges restricted by the operating system. Overall the performance of developed prototypes is setting the new goals in zero remnance based forensic fields and can be considered as novel implemented solution for security in social networks and transaction based systems.

VII. CONCLUSION AND FUTURE WORK

With this work TD-ZRP will proves as a milestone in the field of data organization, lifecycle handling and auto destruction using triggered events. Even the means of storage solution having aged data or the authentication approaches which handles record numbers, passwords and notes will also prefer the use of suggested approach. The complete process is an automatic execution and does not requires the client role to take participate in any of the auto destruction activity. Result evaluations and the performance monitoring will shows that the committed proof for the practicability and effectiveness of the approach. We are also planning to release the open version of TD-ZRP to facilitate the researchers who was working with storage security and forensics.

FUTURE WORKS

This work deals with protecting the users data using some self destruction mechanism based on triggering phenomenon. We had studied various papers and concluded the problem of auto erases and zero remnance and let it linked with the lifecycle of the data. Thus the designed solution is named as trigger based zero remnance proof (TD-ZRP). While taking the components developed and the kind of solution which we are getting with recent technologies, we found that it was lacking somewhere with computation time and the impact on which it was making in the field of forensics.

Some of the directions on which this work can be expanded. These are –

(i) The computation time used by the system is showing delays somewhere due to its validation and cross checking processes. Thus, it can handle by using some lightweight functionality during the developments.

(ii) Triggers can also be increased for more robust protection levels Mainly the copy based count can be handle in such a way that the coping of files can also be comes under this TD-ZRP.

ACKNOWLEDGMENT

I would like to honestly thank **Mr. Rakesh Kumar Lodhi**, Assistant Professor, Dept. of Computer Science, PCST, for his valuable suggestions and supervision. I would also like to thank to our allied faculty members for their remarks and motivations.

REFERENCES

[1] R. Perlman, "File System Design with Assured Delete," In Proceeding of. 3rd IEEE International Security Storage Workshop (SISW), 2005.
[2] M. Paul and A. Saxena, "Zero Data Remnance in Cloud Storage", In International Journal of Network Security & Its Applications (IJNSA), PP. 256-265 Vol.2, No.4, October 2010.
[3] Web Article, "Leave No Trace: How to Completely Erase Your Hard Drives", available at[ONLINE]http://www.gizmodo.com.au/2010/03/leave-no-trace-how-to-completely-erase-ypur-hard-drives/, March 2010.
[4] Technical Report by Privacy Technical Assistance Center, "Best Practices for Data Destruction", PP. 1-10 2014.
[5] Technical Report by Online Trust Alliance, "Data Protection & Breach", PP. 1-40 in Feb 2015.
[6] Y. Xie, K. Kumar Muniswamy-Reddy, Dan Feng and others, "Design and Evaluation of Oasis: An Active Storage Framework Based on T10 OSD Standard", a presentation on Storage System Research Centre, 2012.
[7] P. Pilla, "Enhancing Data Security by Making Data Disappear in a P2P Systems", in Computer Science Department, Oklahoma State University, Stillwater, PP.1-18.
[8] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "FADE: Secure overlay cloud storage with file assured deletion," in Proceeding of SecureComm, PP. 1-18 2010.
[9] D. Logue and K. Ontrack, "SSDs: Flash Technology with Risks and Side-Effects", in data recovery blog available at [ONLINE] http://www.thedatarecoveryblog.com/tag/data-destruction/,2013.
[10] R. Geambasu, Tadayoshi Kohno, Amit A. Levy and Henry M. Levy, "Vanish: Increasing Data Privacy with Self-Destructing Data", in University of Washington, Supported work of Grant NSF-0846065, NSF-0627367, and NSF-614975.
[11] L. Zeng, Z. Shi, S. Xu and D. Feng, "SafeVanish: An Improved Data Self-Destruction for Protecting Data Privacy", Presentation at CloudCom, PP. 1-13 Dec 2013.
[12] C. Cachin, K. Haralambie and H. C. Hsiao, "Policy-based Secure Deletion", at IBM Research, Zurich, PP. 1-25 Aug 2013.
[13] R. Geambasu, T. Kohno, A. Krishnamurthy, A. Levy and H. Levy, "New Directions for Self-Destructing Data Systems", in University of Washington, 2010.
[14] S. Backya and K. Palra, "Declaring Time Parameter to Data in Active Storage Framework", in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), PP. 3127-3131 Vol 2(12), December 2013.
[15] M. Nandhini and S. Jenila, "Time Constrained Data Destruction in Cloud", in International Journal of Innovative Research in Computer and Communication Engineering, PP. 339-343 Vol.2(1), March 2014.
[16] L. Zeng, S. Chen, Q. Wei and D. Feng, "SeDas: A Self-Destructing Data System Based on Active Storage Framework", in IEEE Transaction on Knowledge and Data Engineering, 2013.
[17] Pooja Bhavsar and Rakesh kumar Lodh, "TD-ZRP: Trigger Driven Zero Remnance Proof Technique for Self Data Removal in Web Services", in International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6 (5), 2015.

DOI 10.17148/IJARCCE.2016.5248