ISSN No. 0976-5697

Volume 7, No. 3, May-June 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Research Issues and Scope of Data Security by Self Destruction Mechanism in Cloud Computing

Dr. Gyaderla Ranjith
HOD &Assistant Professor
Department of Computer Science and Engineering
Warangal Institute of Technology and Science
Warangal,Telangana State,India.

Jadala Vijaya Chandra
Assistant Professor
Department of Computer Science and Engineering
Warangal Institute of Technology and Science
Warangal,Telangana State,India.

Sirupa.Vijaya Laxmi
M.Tech Student (Software Engineering)
Department of Computer Science and Engineering
Warangal Institute of Technology and Science
Warangal,Telangana State,India.

Abstract: Cloud computing used not only for storage, different services and applications are emerging day by day, protecting data is becoming challenge and life time research issue, data security is the major issue in the cloud computing, as the cloud user does not have any idea where his sensitive confidential data is placed. As the requirement of storage capacities are increasing drastically, the users requirements are forcing to adopt cloud and security is the major issue. We discussed implementation of time based self-destruction for data privacy. We focused on different attacks such as hopping attack, Sybil attack, sniffer attack and advanced persistent attack. Cryptography is playing a major role in securing data from ancient time addressing the solution for problems from intruders. Encrypted data is stored in different storage servers and data centers all over the world while secret keys are retained by the data owners. Time Based Self Destruction Mechanism destroys electronic data automatically without human interaction, after certain period of the time period, if the data owners wants the data retrieved based on the authentication and authorization the data will be reconstructed from log-files. If the key is destroyed the data in cloud will be useless and an easy prey for the intruders. Time based self-destruction mechanism design and implementation issues are discussed along with the mathematical and statistical analysis. An experimental analysis is given with results.

Keywords: Self Destruction, Cloud Computing,Cryptography, Advanced Persistent Attack**.**

INTRODUCTION

Self-Destruction Mechanism proposes data security and a research issue that enables users to reliable over the cloud computing regarding sensitive and confidential data. It is also used to associate applications and servers and also changes relationship between software and hardware for better data protection and security. At early stages this mechanism is based on the public distributed hash table network and data decryption key is shared in large, instead of revealing the data encryption key openly to the authorized users. Information sharing protocols are used to share the decryption key to public by distributed hash tables. It discards the data after a certain period of the time; the key will be permanently unreadable after the data expiration. Once the data is destroyed based on the protocols after the specified period of the time then the space provided for the old data will be occupied by new data to secure electronic sensitive data for cloud security. The Time Interval plays a greater role, since the concept is based on the time specific constraint and the self-destruction mechanism.

A Defense system or methodology is the used to protect data against different types of attacks on cloud servers, as the cloud servers transfers the user's data among different servers or data centers, where a user will not have any idea about cross cloud data storage and big data environment.

The major challenges faced by cloud today is security, where continuous monitoring and adopting of new technologies, systematic investigation procedures in problem solving, a thorough survey what is going on all over the world in specific field makes research more prominent and reliable.

Self-destruction mechanism is the ancient mechanism adopted by Rulers to protect confidential information. Implementation of different algorithms and protocols for Data Privacy became most common and eternal research issue, In 2009 RoxanaGeambasu., et al., proposed and implemented a system called vanish where data will be decentralized at global-scale using P2P infrastructures and Distributed Hash Tables (DHTs). The system encrypts user's data locally with a random encryption key notknown to the user, destroysthe local copy of the key, andthen sprinkles bits of the key using Shamir's Secret Sharing is an algorithma secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret [1]. When a cloud user does not get enough parts of key, he cannot decrypt the data stored in cloud that means the key is destroyed. But intruders may reconstruct the key, hence data destruction became mandatory, which is disadvantage of vanish mechanism. It can be implemented on cloud computing for data and information security purposes where log files and auditing mechanisms can be used.

II. RELATED WORK

Normally when a person wants to keep data confidential then after certain period of time, if he don't wants data to be leaked and the use of that data is completed automatically he tries to destroy the data. In the same way the goal of this mechanism is to determine automatic destruction of sensitive data after a specified time, this data should be available to the user until the expiration of time as this mechanism is time based, no additional and special infrastructure should be required, no alteration to the regular procedures and cryptographic schemes and final and most important principle is defending and resisting the different attacks.

Sybil attack is the attack which named from the concept of Dissociative identity disorder (DID), in humans generally known as multiple personality disorder. Data Redundancy is the major problem that cloud faces after this attack. A single piece of data is copied multiple times and placed at different places. Identities are the informational abstractions which perceives, if the local entity has no direct physical knowledge about remote entities. The system must ensure that distinctidentities refer to distinct entities; otherwise, when the local entity selects a subset of identities to redundantly perform a remote operation, it can beduped into selecting a single remote entity multiple times, thereby defeating the redundancy is major task .We term the forging of multiple identities as a Sybil attack on the system.

Sniffer attacks are the application based attacks that mainly concentrates in capturing network packets for intruding the cloud. Sniffers are network protocol analyzers used for troubleshooting networks. While these network troubleshooting tools are used by hackers for hacking network and to read the data in packets. Sniffing refers to the process used by attackers to capture network traffic once the packet is captured using a sniffer, the contents of packets can be analyzed. Sniffers are used by hackers to capture sensitive network information, such as passwords, account information etc.

Hopping attack is a type of Sybil attack which are in generally concentrates at the virtual networks, to overcome it, safe vanish mechanism is introduced by extending vanish (self-destructing) mechanism. It extents the length range of the key shares to increase the attack cost sustainability by combing hopping strategy and screening strategy and also made improvement on the Shamir secret sharing algorithm then implemented as the safe vanish system.

Advanced Persistent Attack is a stealthy, sophisticated and targeted to achieve specific goal based on a zero-day exploits. It may be a targeted email attack or a legitimate website which redirects to a fake website. To defense such attack measures should be taken such as hacking, phishing and pharming detection, powerful virus scanners, malicious site filters, patches as remedy to vulnerability and perfect third party auditing protects the cloud computing, which is responsible for storage accuracy, Reliability Security, protection, prevention and performance guidance [2]. The Cloud Architecture model consists of the data center where the data is stored, retrieved and distributed. Where this model is composed of set of hosts which is responsible to manage and maintain the virtual machines which is based on the space and time related optimization techniques. The components of cloud model are cloud let, cloud let scheduler, virtual scheduler [3].

The self-destructing mechanism is a time based mechanism that is used to protect the security of the sensitive data which is only valuable to the user for a limited period of time. In 2010 FengshunYue., et al., proposed and implemented a notation called vanishing data object where it compresses user data for protection from information leakages, where third party auditing is provided for data security and intrusion prevention. The attacks on this security model are persistent where the authorized user's confidential data will be captured and the potential adversaries would attack the vanishing data object after it expires or attacks the distributed hash table network before the expired time [4].

Social networking platforms made cloud more popular and commonly used by researchers and academics. Where the peers cooperate and establish the network, the result can be constructing the relation among themselves. Social network allows the social analytics and scientists' to use formal language and use to go analysis and compared to go to formal mathematical and sophisticated analysis, to compare the value of these properties and reliability as there are chances of data corruption and intrusion. Penetration and vulnerability testing must be performed as the continuous process [5].

Intrusion detection system should be developed and continuous monitoring without human interaction is used to detect the outside attacks; it is an audit system that monitors cloud computing or defense activities to identify malicious activities and stop them. Intrusion Detection and Prevention System is principally emphases on the detecting risks, threats and attacks [6].

Safe Vanish mechanism is the solution for hopping attack and the sniffer attack. Safe Vanish mechanism is implemented on cloud computing for data self-destruction feature which clear up old data for every speculated period of time. So no one can obtain the key shares through the location tables for improved approach. It is an improved self-destruction mechanism for data protection in cloud computing, which is based on extending the length range of key shares and applies the public-key cryptography to defend hopping attack and includes the storage requirement and the network bandwidth and to avoid the sniffing attack. In 2010 LingfangZeng., et al., proposed and implemented a mechanism called safe vanish, for vanish an intruder must not be able to interpret the user's traffic to the Distributed hash table, if not intruder could simply sniff and record the shares while they are stored. Implementation of this mechanism encrypt the key shares that vanish will send to the Vuze Distributed Hash Table through public key cryptography to complete the task of improvement approach, so cloud computing data will be protected for the safety of

transmission in the route as key shares will not lose transmission under sniffing attack [7].

III. RESEARCH ISSUES IN SELF-DESTRUCTION MECHANISM

1. Vanish : Self –Destruction Mechanism :

It permits user to have control over the security issues of sensitive confidential data in cloud computing and introduced a concept vanishing data object *(VDO)* which prevents information leakage. Vanish architecture consists of the Distributed Hash Tables (DHTs) is a distributed, peer-topeer(P2P) storage network consisting of multiple participating nodes. Basically DHT performs three operations: ***lookup, get, and store***.

Lookup isto determine the nodes that are responsible for the index; it then issues a ***store*** to the responsiblenode, who saves that (index, value) pair in itslocal DHT database. The ***get*** operation performs to retrieve the value at a particularindex, the client would *lookup* the nodes responsible forthe index and then issue get requests to those nodes. Internally,a DHT may replicate data on multiple nodes toincrease availability.

The Vanish: Self – Destruction Mechanism designed for privacy and security of data in cloud concept of DTH.

2. Safe Vanish : Self - Destruction Mechanism:

To be protected from different attacks such as hopping and Sybil attacks, Safe Vanish is introduced for data privacy. Cryptographic Techniques are implemented at large scale and VuzeDHT was introduced to clear up unwanted data at specified time interval and even verifies data for security and implements digital signature to get enhanced data security in cloud computing.

3. SeDas : Self - Destruction Mechanism:

Improved Mechanism in cloud computing is *SeDas* which means Self -Destruction Data System where object based storage and active storage are introduced to overcome the weaknesses of vanish and safe vanish. Object Based Storage (OBS) uses OSD which means Object Based Storage Device, is an intelligence based storage system and an evergreen research issue all over the world. Active Storage System frame work is a backbone for the SeDas Architecture based on the three major properties that are meta- data server, application node and storage node.

Meta Data Server takes the responsibility to manage the user management system, server management system, session management system and the file meta data management.

The Application node is a client to use storage service of SeDas, object based storage system for data protection and data privacy in cloud environment which handles the sensitive information such as passwords, accounts and confidential data will be self-destructed without any human involvement.

Storage Node uses the Object Based Storage Devices as they have two major sub systems such as storage sub system and active storage object used to manage the method objects and policy objects [8].

4. CP-ABE approach : Self - Destruction Mechanism:

Cipher text policy Attribute Based Encryption approach is cryptographic and intelligence fuzzy based identity approach which access is associated with the structure access tree with the private key which contains a set of attributes.

The Advantage of this model is it resists collision attacks where as the disadvantage of this mechanism are the specific group only constructed under the generic group.

5. Key Policy ABE: Self -Destruction Mechanism:

Key Policy Attribute Based Encryption is the advanced mechanism of previous system the cipher text consists of a set of attributes and the private key is related to access the structure, when a user made a secret request, the trusted authority determined which combination of attributes must appear in the cipher text for the user to decrypt as it is attribute base encryption and decryption [9].

6. KP-TSABE: Self -Destruction Mechanism

Key Policy Time Specific Attribute Based Encryption is the time based where the authorization period a time interval between upper and lower limit will be defined by the data owner starting from the desired release time and ending at the expiration time. The cipher text is associated with this interval; the user can construct the decryption key only when the time instant is within this interval. The expiration time is the threshold time instant predefined by the owner. The shared data can only be accessed by the user before this time instant because the shared data will be self-destructed after expiration. The time interval from the creation of the shared data, authorization period to expiration time which is the full life cycle privacy protection for shared data in cloud computing.

In this model the access control and the data security and privacy, a new approach is discussed and implemented. The secured data access control during the authorization period and implementation of self-destruction after expiration time period of the shared data in could. Specially the different players that is the roles in data protection such as data owner who can provide data or files that contain some sensitive information, which are used for sharing with his/her friends that is data users. All these shared data are outsourced to the cloud servers to store. Authority is an indispensable entity which is responsible for generating, distributing and managing all the private keys and is trusted by all the other entities involved in the system.

Time reference server takes responsibility of the implementation of release time and collapse time that is start time and end time. Cloud servers are the servers where the user can store a large quantity of data and has security issues which are used to store and manage all the data or files in the system. Finally the Key Policy Time Specific Attribute Based Encryption is a security model designed and

implemented for the data security based on the different attributes [10].

IV. MATHEMATICAL ANALYSIS

Bilinear mapping is a function that combines elements of two different vector spaces, where G_1 is the bilinear group and let g be a generator of the bilinear group of prime order p, the bilinear mapping is G_1 X $G_1 \rightarrow G_2$, Let T be the maximum time in the system of Time Server.
The Mathematical Notation of the Self-Destruction mechanism is divided into the 4 steps they are setup, Encrypt, Key-Gen and Decrypt.

Setup(1^*,U) where U is the universal attribute notation is given as {1,2,3…..n}. Then, we choose y from Z_p randomly. The public parameters *params* is known as
params = $\{g, g_1, g_2, \{\forall i=1:n, u`_{i,1}, u`_{i,2}\}, \{\forall j=1:T, u_j\}\}$
The master key MSK is g_r^y where r is for random key generation.

Encrypt is a step where the message will be converted to the hidden format where original message will be converted to cipher text that involves a set of attributes S_{attr} and public parameters *params* implemented on the Message M and the Time Interval T with upper and lower boundaries where L≤T≤U, where the conversation of plain text to cipher text is considered as attribute based encryption, choose the random value r and will be published as

$$CT(M) \quad \{M.e(g_1, g_2)^{ry}, g^y, S_{attr}, \{E, E', T_i'\}_{i \in S_{attr}}\}$$

The data owner chooses an attribute set S_{attr} for the shared message M and defines time interval set T_i for S. Then, the cloud security system automatically invokes the algorithm without human involvement and finally CT is sent to the Cloud Servers and gives output as follows Encrypt(M, *Params*, S, T_i) to encrypt M to its Cipher text CT, which is associated with the set S and T_i . The Time Server takes the responsibility of managing time constraint.

Key-Gen is the mechanism that inputs the public parameters *params,* the master key MSK ϵ G_1, the access tree Γ and the time based instant set T_i' in which the element of T_k is associated with the leaf node of Γ, these polynomials are chosen in a top-down manner, starting from the root node r. The Authority runs the algorithm KeyGen(MSK,Γ, T_i') to generate a private key.
Decryptis a step which takes the input a cipher text CT and the private key SK when a set of time specific attributes satisfies Γ, it is able to decrypt the cipher text to the plain text, where the data user can receive the pain text in the cloud environment.
Decrypt(CT,SK) where the decryption procedure is the reverse of the encryption, in order to decrypt the cipher text to plane text successfully based on the valid attribute set, where the final output is given by the following notation.
$\Omega = e(g, g_2)^{s.y}$
Where Ω to decrypt CT(M) a recursive algorithm implemented on which is from bottom to up to obtain the shared message M.

V. EXPERIMENTAL ANALYSIS

At this Stage we mainly focused on the test method and implementation of the self-destruction mechanism. In cloud computing there is multiple storage services for user to store data and for researcher multiple issues to explore. Research Issues comparison of self-destruction is a significant mechanism and finally the Key Policy Time Specific Attribute Based Encryption is proved to be the highly secured under the standard secure mechanisms.

We Implemented a Test Method of KP-TSABEand then give analysis on secure mechanisms in cloud computing which support the self-destructions. We created a virtual cloud computing environment in a small scale for experimental purpose; there are multiple storage services for a user to store data meanwhile, to avoid the security breaches and possibly to be produced by the centralized trusted third party auditors' cryptographic mechanisms are implemented on the cloud computing [11].

The Experimental project is divided different sessions such as Authority and Time Server, Data owner, Cloud Server, Data Users and Potential Adversary. Every user should register as per category such as data user, data owner, Auditor. An Authorized Data Owner can upload sensitive confidential data, which will be sent to Authority where without any human involvement data will be encrypted as per time based and master key will be generated where the log files are handled by the auditor where they can be managed and there will not have any chances of vulnerability.

Intelligence fuzzy identity based encryption is associated with the Authority and Time based encryption is associated with the Time Server, by combination of the authority and time server setup where the attributes are identified and parameters are generated. The master key will be generated without any human interaction and involvement based on the algorithm under the policy of random key generation.

Potential Adversary monitors the setup to generate *params* and MSK(Master Key) at the first stage, it generates repeated private keys corresponding attributes. Cloud Servers are the data storage systems where the user will not have any idea where his data is stored. Privacy and Security are the major concerns in the cloud computing as the data stored in cloud is encrypted where only the authorized users can see the data in plain text.

Self Destruction mechanism will be implemented on the data system which is an active storage framework. The self destruct method object is associated with each secret key apart from the survival time parameter for each secret key part. It supports the security erasing files and random encryption keys that are stored in cloud environment after the collapsing of the time period. It destructs all the data copies and log files simultaneously and makes them unreadable and unrecoverable.

VI. CONCLUSION AND FURTHER SCOPE

As cloud computing rapidly developing for its resourceful services, a lot of new mechanisms and challenges have emerged. Risks, Threats and attacks on cloud making cloud challenging and research issue. Self destruction is an important concept for privacy and security of data and how securely data will be deleted? Is there any possibilities of regeneration of data by the attackers, hence self destruction is not only a solution for security problem, where the problem is still arriving in the form of hash files and log files and regarding regeneration. In this paper different research issues are discussed and practically analyzed.

As more and more services are provided on cloud, security is the major issue, managing and controlling the sensitive confidential user data is the major challenging task and research issue. Data Privacy has become increasingly important in cloud environment. Upcoming researches are mainly concentrated on the new approaches to challenge the security problems. Security issues are tested and risks, threats and attacks possibilities are calculated to by giving the results according to the possible vulnerabilities and other possible destruction procedures different testing tools are used most of them are penetrating testing tools and performance testing tools [12].

VII. REFERENCES

[1]. Roxana Geambasu, Tadayoshi Kohno, Amit Levy, Henry M. Levy, "Vanish: Increasing Data Privacy with Self-Destructing Data", In Proc. of the USENIX Security Symposium, Montreal, Canada, pp. 299-315, August 2009.

[2]. J. Vijaya Chandra, NarasimhamChalla, Mohammed Ali Hussain, "Data and Information Storage Security from Advanced Persistent Attack in Cloud Computing", *International Journal of Applied Engineering Research*, vol 9 (20): PP 7755 –7768, 2014.

[3]. G.Ranjith, J.Vijayachandra, P.Sagarika, B.Prathusha,"Intelligence Based Authentication-Authorization andAuditing for Secured Data Storage", *International Journal ofAdvances in Engineering & Technology*, Vol8, issue 4, PP628-636, August 2015.

[4]. F. Yue, G. Wang and Q. Liu, "A Secure Self-Destructing Scheme for Electronic Data", *IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), 2010*, Hong Kong, 2010, pp. 651-658.

[5]. J. Vijaya Chandra , NarasimhamChalla, SaiKiranPasupuleti, Thirupathi RK, Krishna RV,"Numerical Formulation and Simulation of Social Networks using Graph Theory on Social Cloud Platform", *Global Journal of Pure and Applied Mathematics*, 2015; 11(2):1253–64.

[6]. J. Vijaya Chandra , NarasimhamChalla, SaiKiranPasupuleti,"Intelligence based defense system to protect from advanced persistent threat by means of social engineering on social cloud platform", *Indian Journal of Science and Technology*, 2015; 8(28):1–9.

[7]. L.Zeng, Z.Shi, S.Xu and D.Feng, "Safevanish: An improved data self-destruction for protecting data Privacy", in *Proc. Second International Conference on Cloud Computing Technology and Science (CloudCom)*, Indianapolis, IN, USA, Dec. 2010. Pp. 521-528.

[8]. L. Zeng, S. Chen, Q. Wei and D. Feng, "SeDas: A self-destructing data system based on active storage framework," APMRC, 2012 Digest, Singapore, 2012, pp. 1-8.

[9]. J. Xiong*et al*., "A Secure Data Self-Destructing Scheme in Cloud Computing," in *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 448-458, Oct.-Dec. 1 2014.

[10]. X. Fu, Z. Wang, H. Wu, J. q. Yang and Z. z. Wang, "How to Send a Self-Destructing Email: A Method of Self-Destructing Email System," *2014 IEEE International Congress on Big Data*, Anchorage, AK, 2014, pp. 304-309.

[11]. Y. Zhu, L. Yang and D. Ma, "Secure Snaps: A New Forward Secrecy Cryptosystem for Self-Destructing Messages in Mobile Services," *2015 IEEE International Conference on Mobile Services*, New York, NY, 2015, pp. 142-149.

[12]. Reddy, M.R., Yalla, P., J.Vijaya Chandra, "Design and implementationof integrated testing tool based on metrics and quality assurance",pp.10463-10472,*International Journal of Applied Engineering Research*,Volume 9,Number 21(2014).