Volume 2, Issue 12, December 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal Of Science, Engineering and Information Technology

Chief Editor
Dr. Bilal Ahmad Malik

Publisher

Dr. Bilal Ahmad Malik

Associate Editor

Dr.Nagendra Mani Trapathi

NAIRJC JOURNAL PUBLICATION

North Asian
International
Research Journal Consortium

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: -North Asian International Research Journal Consortium (NAIRJC) 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

IRJIF IMPACT FACTOR: 3.821

IMPROVE DATA EFFICIENCY AND PRIVACY USING SELF DESTRUCTION

PROF. KRISHNA TAYADE [1], MISS. PRIYANKA LANDE [2], MISS. MAMATA GODSE [3], MISS. JYOTI DALAVI [4] & MISS. NAYAN DESHMUKH [5]

[1] Prof. Department of Computer Engineering, Nutan Maharashtra Institute of Engineering & technology, pune, India

[2345]Students, Department of Computer Engineering, Nutan Maharashtra Institute of Engineering & technology, pune, India

ABSTRACT:

Cloud computing with the impact of current computing technologies, IT industries drastically changed. IT industries have started to deliver the resources, via computing and technological media. Now-a-days cloud is in better rush. Although cloud offers storage services which are best than other storage systems, ,in which users have rights to use the space on cloud by storing their important data, still in concern with security it's still have some doubts. Multi-owner data storing and sharing strategies in a dynamic environment stores huge amount of data files in the cloud, which remains in cloud for long period of time. Since it is for a long period of time the important data stored may misused by the miscreant or may be by the service providers. Its mandatory to remove unwanted files to maintain the cloud's file security. To overcome this drawback, a self-destructing system can be used to remove unwanted files automatically when the time which was settled for the same is out of the limit, for sharing specifies by data owner has been expired.

***Keywords:* Cloud storage network, data self-destruction, data privacy, attribute-based encryption**

I. INTRODUCTION

A Network of computing is a connected group of interconnected same/similar/autonomous computing nodes, which are using a well-defined, well-structured, mutually agreed set of rules and conventions known as protocols, interact with each-another intermittently and allow/give access to resource sharing preferably in a predictable and controllable and statistical manner. Communication has a major flash on today's business world. It is unconditional to communicate the data with high security. Security Attacks compromises/loses the security, privacy, authorized access and hence various Symmetric (i.e. Private key encryption) and Asymmetric cryptographic algorithms(i.e. Public key encryption) have been proposed to achieve the security services and better performance ratio such as Authentication(Finding weather the user is authenticated by the procedure or not), Authorization(weather user have authorized access to the system or not), Confidentiality(a set of rules or a restriction that limits the access or places restrictions on certain types of information so only the authorized users can access it.), Integrity, Non-Repudiation and Availability. In concern with Today's techniques, various types of cryptographic algorithms provide high security to information on controlled networks. These algorithms should provide the security of data, protecting data and users authenticity. To improve the strong bonding of these security algorithms, a new security protocol for online transaction process can be designed using combination of both symmetric(i.e. private key encryption) and asymmetric cryptographic techniques(i.e. Public key encryption). This protocol provides three cryptographic primitives is rules such as nobility, confidentiality and authentication. These three regulations can be achieved with the help of Revert Cipher (RC6). That all there algorithm used for the encryption on single file with creating different chunk. This new security protocol/rule has been designed for better security/performance with integrity using a combination of both symmetric and asymmetric cryptographic techniques. In this system this algorithm is used to maintain the security of file while transmitting from source to destination. File is sent by user with specified/already settled timestamp, the user at destination can download this file before time expiration only. After a given timestamp file will be automatically discarded. This system creates secure environment for file transmission.

II. RELATED WORK

The proposed architecture is a distributed object-based storage system in which self-destructing knowledge operates. We are dealing with the use of Sedas system with the assistance of Shamir's algorithmic program for secure fund dealings. In this paper Methodology combines an active moreover proactive approach within the storage of object techniques and method of object, victimization processing capabilities/utilities of OSD to attain the knowledge of self-destruction. User will specify the key longevity time of distribution of key and uses the settings of swollen interface to export the life cycle of a key, by giving access/permission to the user to manage the subjective life-cycle of personal knowledge. Vanishis a kind of system for making messages that mechanically or may be with the other supporting characteristic, destroys once an amount of your time. The secret is for good lasting, and also the encrypted (cipher text) knowledge (hidden data)is for unclear data once knowledge expiration is been carried out. Vanish is a motivational and creative approach to a very important which assures the privacy downside, but, in its current kind, it's insecure. Vanish was the previous approach of

Sedas System, it moreover supports key generation algorithmic program however at a single period/at a time it generates just one key thus rather than that Sedas, it generates multiple keys with the assistance of Shamir's algorithmic program thus its best for security purpose. Also, we tend to grant Associate in nursing improved approaches used against sniffing attacks by means of victimization in the general public key cryptosystem (asymmetric key encryption) to stop from sniffing operations. These proposed by tang et al provides a contribution for the self-destructing data by determining the cryptographic techniques. The data will be encrypted into the cipher text before sending it to the destination root. This system will discard the files and make them unrecoverable/unresponsive by revoking the file's access permissions. One more additional system called File System Design with assures delete proposes three types of file deletion. First is the expiration of the file/data known at the time of file creation, second is on demanding deletion and destruction of separate files and third is the usage of custom keys for big classes of data. As given above, many systems have been proposed to implement and work on and executing a self-destructing systems, in-between those systems only some systems provide remarkable results. User cannot control the system's self-expiration of data time. They rather have a fixed time (i.e. after a particular time period, even if the receiver not confirmed with the data i.e. no checking of mails/data/messages) for file expiration (in this system) which is not an efficient approach for the self-destructing scenario.[2]Vanish is the system that gives the basic idea of self-destructing mechanism over a data along with its core properties. The system developed is a kind of prototype which is created and implemented using Distributed Hash Table (DHT). This system used the concept of bit torrents Vuze DHT that can support eight hours of timeout or Planet Lab hosted Open DHT that can support one week timeout. This respecting system provides a plug-in kind of concept for Firefox browser that creates a message which automatically disappears or we can say gets invisible after a specific interval of time. Here the expiry/destruction time for the data to be controlled by the DHT service and not by the user (as previously mentioned user cannot control the system's limited expiration time of the data). Later many extensions which were using previous techniques are been implemented on the Vanish system. Traditional active memory device executes custom applications code on a large amount of knowledge by utilizing/developing the unused process power of the storage nodes(storage media) for computation interactive application and characteristic use, the performance could be quite low as compared to other mechanisms, thanks to insufficient process of power storage nodes. The development of high performance computing i.e. HPC is based on storage capacity and storage capabilities and I/O performances; the given storage system has entered the peta byte era. The storage system (in which the data can be stored) scale is of high performance while computing and is very big, the amount and space of storage nodes is very huge. Active storage system in the context of parallel file systems and has explained that, with enhanced runtime interfaces, we can improve the performance of data prediction of kernels significantly. In this given approach, the parallel runtime environment along with the interfacing enables application codes to consume the data analysis kernels dipped in the parallel file system. In order to enable an individual file, the server needs to perform active storage operations without client intervention, our proposed approach dynamically adjusts/modifies to deal with data objects and elements that cross stripe or predefined boundaries. We have also implemented server-to-server communication for reduction and aggregation to allow and grant access to the pure server-side computation. Our experimental results using a set of data analysis kernels describes that our scheme/system brings significant performances capabilities and improvements as compared to the traditional storage system.The data movement often dominates/poor's the applications' run time walkthrough. Active storage provides a creative and remarkable solution for these applications by shuffling appropriate computations from computational nodes to storage nodes. The communication of this system is three way. First, It used to demonstrate that the data dependence in operations offloaded to storage servers have a clear impact on the system performance. Second, it presents a new DAS system to address this issue. The DAS has a bandwidth requirement analysis component embedded and makes the offloading decision dynamically on the fly. An improved data distribution method was founded and adopted in the DAS to minimize the data movement. Third, it have built a prototype/rule and evaluated the proposed DAS with representative and cohesive processing kernels. The results show that the proposed DAS architecture outperforms existing active storage schemes.

III. SYSTEM ARCHITECHTURE

System providing following security importance:

1. Security of data is important.
2. Cryptography is used to secure data.
3. Main requirements of cryptography are to maintain data confidentiality
4. Data integrity
5. Authentication, authorization and will not be able to successfully challenge from unauthorized end-users.
6. To protect above properties/characteristics, symmetric i.e. (private key encryption) or asymmetric cryptography i.e.(public key encryption) is used.

USER AUTHENTICATION AND AUTHORIZATION

First user need to register. Once the user registration is done, then he/she will access the appliance. For registration user need to enter the fundamental info regarding himself. User even have to line the username and watchword. This all registration info is get keep into information. The IMEI variety is mechanically get keep into information once user do the registration. Once the registration client will login through mentioned username and watchword.

File Upload

User uploads a block of files in the cloud with encryption by using his secret/private key (Private key encryption). This ensures the files to be protected from unauthorized user i.e. from unauthorized access.

File Download

The user to download the file using his secret key to decrypt the downloaded data of blocked/(users in blocked state) user and verify the data and reload the block/defined structure of file structures into cloud server with the use of encryption .This ensure the files to be protected from unauthorized use.

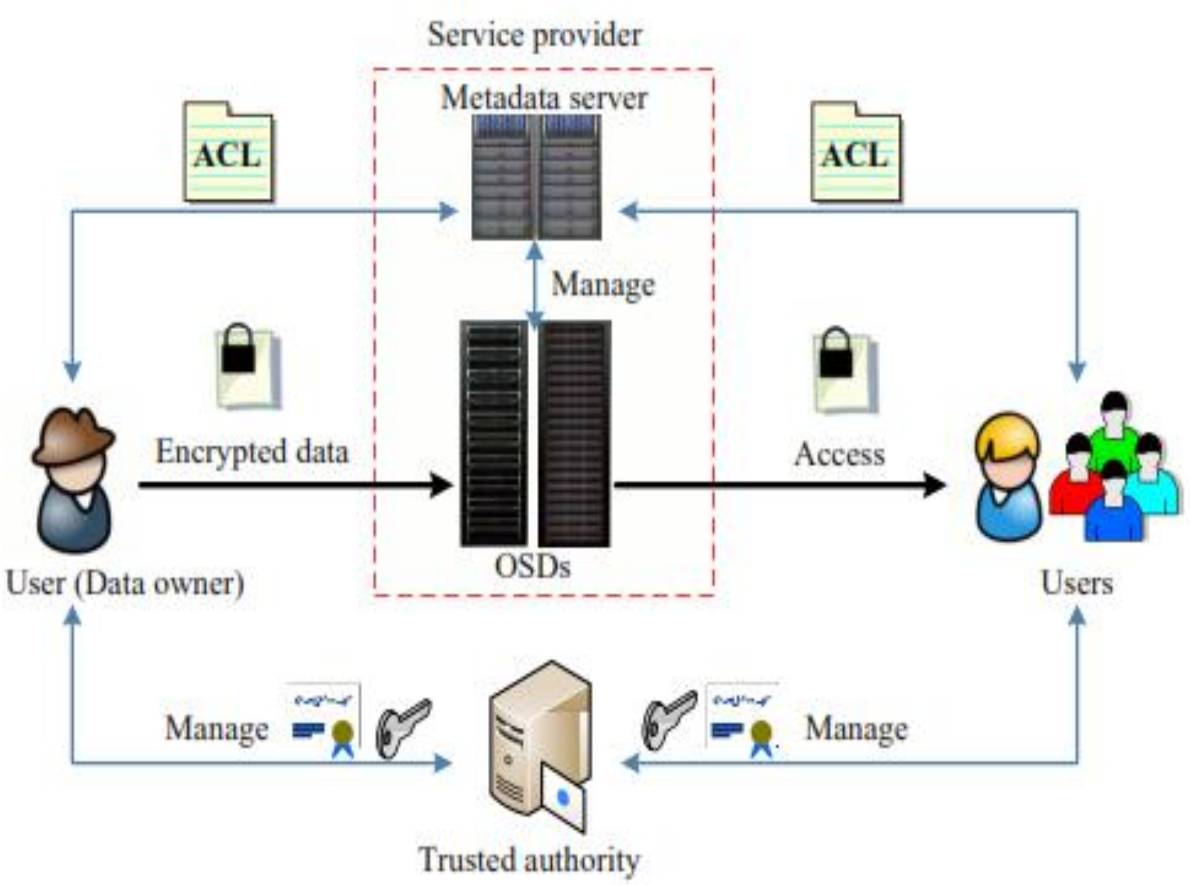
File Verification with set time limit

The cloud provider is able to correctly check the integrity of uploaded data. The data owner can set time limit of shared data with storing the entire data from the cloud, even if some blocks in shared data have been re-signed by the cloud.

Functional Relation:

In data server, following process is done:

- **Service provider:** Service provider play the role of publishing services and applications onto our service repository, called Service Community Platform.
- **Application architects:** Taking into consideration of charge of maintaining services and service-oriented situational applications, and encapsulating some reusable task template.



IV. PURPOSE AND SCOPE

Self-destructing data importantly deals with protection of the data privacy. All the data and its copies will become destructed or unreadable or irresponsible, after a user-specified period, without any user intervention. Evaluate analytically the functionality of the proposed system. Secure and flexible proposed system to protecting shared data.

V. APPLICATIONS

1) In the organizations where high security tasks are day-in and day-out.

2) Securing transmission.

VI. CONCLUSION

Cloud Sky creates a secure and trustworthy environment for file transmission. It uses RC6 for cryptography which gives shield data to transmit. Source can perform file sending operation any time but and destination can load this file only during the timestamp. Self-destruction system automatically removes unwanted files after user specified time period has expired. Proposed scheme allows secure sharing of data files by leveraging secret sharing scheme. Encrypted secret can be decrypted by recombination of individual keys which results in shares of group members satisfying minimum threshold count. The whole system produces data confidentiality.

VII. ACKNOWLEDGEMENT

I would like to extent my sincere and heartfelt obligation towards all personage who have helped me in this endeavor for their active guidance, help cooperation & encouragement. I am extremely thankful and pay my gratitude to my project guide **Prof. Krishna Tayde**. For him valuable guidance and support on completion of this project work and also thankful to project coordinator **Prof. Ashwini Jadhav**. We would also like to thank our H.O.D **Prof. Shyamsunder Ingle**. Who always has enough time to solve everyone’s problem. I also acknowledge with deep sense of reverence, my gratitude towards my parents an member of my family, who has always supported me morally as well as economically.

REFERENCES

1 Lingfang Zeng _, Yang Wang _, and Dan Feng “CloudSky: A Controllable Data Self-Destruction System for Untrusted Cloud Storage Networks” 2015

2 X. Fu, Z. Wang, H. Wu, J. qi Yang, and Z. zhao Wang, “How to send a self-destructing email: A method of self-destructing email system,” in *Prof. of the IEEE International Congress on Big Data*, 2014, pp.304–309

3 J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, “A full lifecycle privacy protection scheme for sensitive data in cloud computing,” Peerto-Peer Networking and Applications, June 2014.

4 R. D. Binns, D. Millard, and L. Harris, “Data havens, or privacy sans frontieres?: a study of international personal data transfers,” in *Proc. Ofthe ACM conference on Web science (WebSci)*, 2014, pp. 273–274.

5 M. Arafati, G. G. Dagher, B. C. M. Fung, and P. C. K. Hung, “Dmash: A framework for privacy-preserving data-as-a-service mashups,” in *Proc. of the 8th IEEE International Conference on Cloud Computing (CLOUD)*, 2014.

6 G. Wang, F. Yue, and Q. Liu, “A secure self-destructing scheme for electronic data,” *Journal of Computer and System Sciences*, vol. 79, no. 2, pp. 279–290, March 2013.

7 L. Zeng, S. Chen, Q. Wei, and D. Feng, “SeDas: A self-destructing data system based on active storage framework,” *IEEE Transactions on Magnetics*, vol. 49, no. 6, pp. 2548–2554, 2013.

8 C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward secure and dependable storage services in cloud computing,” *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.

9 G. Wang, Q. Liu, J. Wu, and M. Guo, “Hierarchical attribute-basedencryption and scalable user revocation for sharing data in cloud servers,” *Computers & Security*, vol. 30, no. 5, pp. 320–331, July 2011

10 S. Yu, “Data sharing on untrusted storage with attribute-based encryption,”Ph.D. Dissertation, ECE Department, Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609-2280, July 2010.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- North Asian International Research Journal Consortium (NAIRJC)
221, Gangoo Pulwama - 192301
Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com