International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Self Destruction Of Data On Cloud Computing

Pradnya Harpale[1] ,Mohini Korde[2],
Pritam Kore[3],Bhagyashree Pawar[4],
Prof.S.H.Patil[5]
[1,2,3,4,5]Computer Engineering JSCOE,
acronyms acceptable,
Pune, India
pradnyah1396@gmail.com,
mohinikorde8321@gmail.com ,
Pritamkore123@gmail.com,
bpawar1206059@gmail.com ,
Shpatil012@gmail.com

May 24, 2018

Abstract

Cloud computing is an most emerging technology today which is used most of the social media sites to store the data. The data stored on the to cloud is not public data of the user so it must not be tampered by other entities. We propose a system to enhanced security, the data uploaded by user is shuffled between the number of directories within cloud after a particular interval of time to avoid the tracking of the data. The data backup of the data will be taken timely into the backup directory. The proposed system enhances the security as well as the ease to use the cloud.

***Key Words*:**Centrality; Cloud security; Fragmentation; replication; performance; SHA; AES; Cloud Computing.

1 Introduction

Cloud computing enables on-demand network access to a shared pool of configurable computing resources such as servers, storage, and applications. These shared resources can be rapidly provisioned to the consumers on the basis of paying only for whatever they use. Private cloud storage is built by exploiting the commodity machines within the organization and the important data is stored in it. Now a days, to storing the data of social media sites cloud Computing technology mostly used. The data stored on the cloud is private data of the user so it must not be tampered by other entities. We propose a system to enhance the security, the data uploaded by a user is shuffled between the numbers of directories within cloud after a particular interval of time to avoid the tracking of the data. The backup of the data will be taken timely into the backup directory. The proposed system enhances the security as well as the ease to use the cloud.

2 LITERATURE SURVEY

1] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A.Zomaya, On the characterization of the structural robustness of data center networks, IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013, pp. 64-77. This paper indicates about Data Center Network (DCN), which is used as a backbone of data repository that ensures high performance boundaries in the field of cloud. The DCN needs to be forceful to failure and should satisfy the required Quality of Services (QoS) level and Service Level Agreement (SLA). Hence, they have proposed a deterioration metric that meets the requirements of DCN robustness.

2] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya,Energy-efficient data replication in cloud computing datacenters, In IEEE Globecom Workshops, 2013, pp. 446-451. Data replication plays vital role for services in cloud that brings the data consumer closer to the data. This paper mainly deals with the efficient data replication in cloud computing data center. Energy-efficiency and bandwidth consumption mainly results in communication delay. The result of simulation minimizes the energy consumption, bandwidth and delay in communication and provides a

better solution for data replication.

3] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, An analysis of security issues for cloud computing, Journal of Internet Services and Applications, Vol. 4, No. 1,2013, pp. 1-13. Security problem mainly arises due to different attack that takes place. Security problem may lead to degradation in use of cloud. By understanding different attacks exist in cloud computing can help the organization to make change towards the use of cloud. This paper presents different security issues for cloud model: Iaas, Paas, Saas that can change depending on the cloud models.

3 PROPOSED SYSTEM

In proposed system, the main aim is to secure the files stored on cloud to enhance the security. The data uploaded by a user is shuffled between the number of directories within the cloud after particular interval of time to avoid the tracking of data. The backup of the data is also taken into backup directory. For load balancing techniques, we have splitted the file into three chunks and stored into three different location and the access is only for authorized user who has login credentials with valid user key(private key) that is given by the admin on approval. This system also has the functionality to ask information to the user for login and send username, password and private key to user with the help of admin. Those who have login credentials and private key are able to perform upload, download, and view and delete operations. Data Security and load balancing is managed by Advanced Encryption Standard (AES) and Secure Hash Code Algorithm (SHA). The hash code is generated according to file data and stored in to the database. If the code is same then duplicate file message will arrive otherwise if the code is unique then the file is splitted and stored at three different locations. If the login credentials do not match then the user is unable to perform operation like upload, download and delete. If the login credential matches the all three chunks gets merged into a single file and then download or delete operation can be performed that is more secure and faster. There are three main modules in the system:

1. User: User can apply for login credential. It can also per-

form different operations like upload, download and delete.

2. Admin: Admin is mainly used for approval and disapproval of user request. If user is approved then username, password and private key is sent to the user and it can perform upload, download and delete operation. If the user is disapproved then user record is deleted and disapproval email will be sent.

3.Cloud: Cloud is mainly used for storages purpose and performing the operations on cloud. It is used for controlling all operation performed on cloud.

Fig 1: SYSTEM ARCHITECTURE

In this system mainly consist of three modules:

Owner-In these owner modules, owner add the multiple users in the cloud system. Owner also uploads the text files in the cloud storage. He can delete the files.

User-In user module, user completes the registration process and login the system. He can upload the text files on cloud storage. He can delete, update or modify the files

Cloud Admin-In this module, the views the all status, views user, view owner, and reports send back. The Cloud admin module file can fragments using the fragment placement and fragments replication algorithms.

4 ALGORITHMS

A. A. T-COLORING ALGORITHM FOR FRAGMENTS ALLOCATION:

Using DROPS method file split into various fragment. For Security and Optimal Performance in cloud Division and Replication is used. For enhanced access time we have to choose central nodes offered in cloud storage. T-coloring technique selects nodes in cloud

for fragment placement by keeping focus on performance and security. The DROPS method utilize centrality concept to decrease the access time. Centrality concludes central node based on various measures.

B. FRAGMENTS REPLICATION

Algorithm 2 Algorithm for fragments replication
for each Ok in O **do**
select Si that has max(Ri
k
k)
if colSi = open color and si >= ok then
Si _ Ok
si _ si ok
colSi _ close color
Si_ distance(Si; T) P /*returns all nodes at
distance T from Si and stores in temporary set Si*/
colSi. _ close color
end if
end for

C. ADVANCE ENCRYPTION STANDARD (AES)

AES is an insistent rather than Feistel cipher. It is based on substitutionpermutation network. It composes of a series of linked operations, some of operations which involve replacing inputs by specific outputs (substitutions) and also others involve shuffling bits around (permutations).

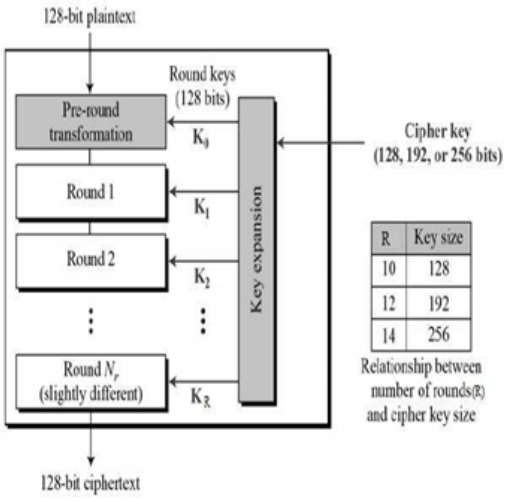

Fig2: AES STRUCTURE

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

D. SECURE HASH ALGORITHM

Hash functions are very useful and also it is appear in almost all information security applications. A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. For hash function the input is of arbitrary length but output is always of fixed length.Values returned by a hash function are called **message digest** or simply **hash values**. Family of SHA contain of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. The original version of SHA, is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993. It had few weaknesses so it didnt become very popular. After that in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.

5 MATHMATICAL MODEL

Let Assume S be the system which execute Self Destruction of Data in Cloud Computing

S={s , e , X, Y, T,F_{main}, NDD, DD, Success, Failure}

- **S(System)** = It is proposed system of our project having following tuples.
- **s (initial state at time T)** = Graphical User Interface of search engine. The GUI gives the space to enter a query or an input for user.
- **X (input to the system)**:- Input or Query. The user must enter the query first. The query may or may not be ambiguous. What user wants to search represents the query.
- **Y (output of the system)**:- The output is list of URLs having Snippets
- **T (No. of steps that will be performed)**:- 6. These are nothing but the total number of steps that are required for processing the query and generating results.
- F_{main} (main algorithm):- The main algorithm contains process P. The process P contains input, output and subordinates functions.
- **DD (deterministic data)**:- Deterministic data contains the data of database. Databases we have considered here are MySQL, SQLite.
- **NDD (non-deterministic data)**:- Our non-deterministic data is the number of queries that are given by user.
- **Memory shared**: - MySQL. MySQL will store information like User Authentication, Performing Operations likeUser can upload the file.
- CPU_{count} : - 1. For server in our system, we require one CPU.

- **Success** = successfully recommended best system as per users interest
- **Failure** = If application will not send the notification to user it will fail.

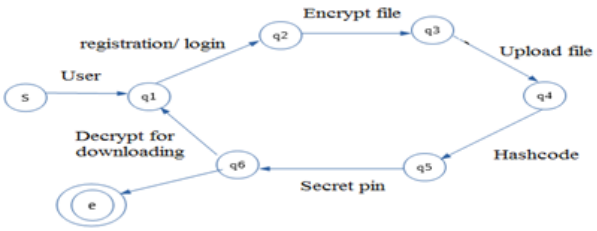

Fig 3: State Transition Diagram

6 Acknowledgment

It is pleasurous for us to present the project report on Self Destruction Of Data In Cloud Computing .We would like to thank our internal guide Prof. Swati H. Patil for giving us her precious guidance and help that we needed. We are grateful to her for her support and guidance. Their worthwhile ideas were very useful.

We are also grateful to Prof.H.A.Hingoliwala, Head of Computer Engineering Department, JSPMs JSCOE for his absolutely necessary support and valuable guidance. At the end we are especially thanking to Pro.Swati H. Patil for providing us various resources like laboratory having all required software platforms along with continuous internet connection which was required for our project.

7 Conclusion

This system is maintaining data theft. Reduce the data tracking. With the help of Hash code, algorithm data is divided into three different chunks and stored into different location so data load will be managed and provide the fast performance. This system is avoiding data duplication and reduce wastage of space.

References

[1] 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.304309.

[2] R. D. Binns, D. Millard, and L. Harris, Data havens, or privacy sans frontieres?: a study of international personal data transfers, in Proc. Of the ACM conference on Web science (WebSci), 2014, pp. 273274.

[3] R. Lu, H. Zhu, X. Liu, J. Liu, and J. Shao, Toward efficient and privacy preserving computing in big data era, IEEE Network, vol. 28, no. 4,pp. 4650.