Implementing Fragment Placement and Replication Technique for Cloud Security

Pragathi V[1], Robinsingh Chauhan[2], Shruti Vishwanatha Bhat[3], Karishma Jaiswal[4], Ravichandra M[5]

[1,2,3,4]UG student, [5]Assistant Professor, Dept. of Information Science and Engineering, Sapthagiri College of Engineering, Bengaluru, India

---***---

Abstract: *Cloud storage is cloud computing model in which data is stored on remote servers accessed from internet. All the data is stored in third party space which results in security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are meant to be taken to protect data within the cloud and it should be simple to use. However, the employed security strategy must also take into account the optimization of the data retrieval time. Fragment placement and replication technique is proposed that it approaches the security issue. T-coloring to forbid an attacker of guessing the fragment's location. Moreover, the technique which is used does not rely on the traditional cryptographic techniques to secure the data.*

Key words: Cloud Storage, Fragment placement, Data security, T-coloring, Sole Replication

1. INTRODUCTION

The cloud computing introduced a whole new way of file storage to the world. Cloud computing is characterized by self-services, on demand, sharing of resources, network accesses and other services. The goal of cloud computing is to cut down the cost as much as possible and allow users to take benefit from all the services provided by the cloud and helps them to focus on their core business. Cloud computing and storage provides users capabilities to store and process their data in third-party data centres. Cloud storage is made up of many distributed resources, acts as one, either in a federated or a cooperative storage cloud architecture. It is highly fault tolerant through redundancy and distribution of data. Organizations use cloud in variety of different service models. Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing. Cloud security issues may stem due to the core technology implementation. Security concerns associated with cloud fall into two broad categories; the security issues faced by cloud providers and by their customers. For a cloud to be secure, all the participating entities should be secure. In a cloud, the security of the assets does not solely depend on an individual's security measures. The neighbouring entities may provide an opportunity to an attacker to bypass the users defences. The provider must ensure that their infrastructure is secure and their client's data and applications are protected, while the user should take measures to strengthen their application and use strong passwords and authentication measures. Data stored on to a public cloud must be secured. Unauthorized data access by other users and processes must be prevented. Any compromised node present in cloud network can put the whole cloud at threat. In such a scenario, the security mechanism must increase an attacker's effort to retrieve a reasonable amount of data even after a successful attack in the cloud. The fragmentation method is used to distribute the data fragments into different data centres which prevents the system from single point failure situation. Then using T-coloring graph algorithm, these fragments of file are stored on the nodes. In large scale systems, the problems of data reliability, data availability, and response time are dealt with data replication strategies [5].

2. LITERATURE REVIEW

2.1 Authentication and Encryption Based Technique

In this paper their main concern is to provide the security to end user to protect files or data from unauthorized user. Security is the main intention of this technology through which unauthorized intruder can't access user file or data in cloud[1]. They have used the technique called Rijndael Encryption Algorithm to encrypt the data or file at the user end and this technique provides security to data at rest as well as at motion.

Limitation

Rijndael Algorithm is used to secure data but it consumes more computational power and time.

2.2 RSA Algorithm Based System

This paper has been written to highlight the cloud security and privacy issues. Their research mainly focus on service provider's side security. They must protect their client's data by unauthorized access, modification or misuse, denial of service and any repudiation[2]. To ensure the security of client data in cloud, they purposed the RSA algorithm.

Limitation

RSA Algorithm is used to secure data but it does not support for data recovery when there is loss of data.

2.3 Attribute Based Data Sharing Scheme

In this paper they introduced the concept of attribute with weight, being provided to enhance the expression of attribute, which not only extend the expression from binary to arbitrary state, but also lighten the complexity of access policy. Therefore, both storage cost and encryption complexity for a ciphertext are relieved[3]. They have used Ciphertext-policy attribute-based encryption (CPABE) which is a very promising encryption technique for secure data sharing in the context of cloud computing.

Limitation

CPABE- this scheme take lot of time to encrypt the data as well as there is a key management issue.

2.4 Security Aware Data Placement Mechanism

They proposed data placement in cloud storage systems addressing the security challenges. With the security constraint, they first formulated the data placement problem as a linear programming model that minimizes the total retrieval time of a data, which is divided and distributed over storage nodes. They then developed a heuristic algorithm namely Security-awarE Data placement mechanism for cLOUd storage Systems (SEDuLOUS) to solve the problem[4]. They demonstrated the usefulness of the proposed algorithm through comprehensive simulations. The simulation results declared that the proposed algorithm reduces the retrieval time of Internet2-topology system compared to baseline methods.

Limitation

SEDuLOUS is used to secure data storage. It consumes more computational power and time.

3. EXISTING SYSTEM

In previous storage strategies file uploaded by user was stored on single node of cloud network. Hence, due to which is under any circumstances the node is compromised then the file present on the particular node is also compromised. Also suppose if successful intrusion happens then the whole file is accessible to attacker and also in order to try to get more information may the attacker may attack neighbour nodes which will be more harmful and by doing so whole data is compromised.

Drawbacks of existing system

a) The cryptography schemes does not protect the data files against tempering and loss due to issues arising from virtualization and in connectivity problems.

b) Data loss in cloud datacentres.

c) Consumed huge time for data processing.

4. PROPOSED SYSTEM

In this proposed system methodology, the file is fragmented into pieces and replicated at specific locations within cloud. The division of file into fragments is performed based on given criteria of such that individual fragments do not contain any meaningful information. A node consists of only one fragment of any file which increases security. A successful attack must not reveal the locations of other fragments within cloud. For selecting the nodes T– coloring algorithm is used. The performance of system is also affected in positive manner. As the system does not use cryptographic operations, system is faster to perform the required operations. The methodology focus more on security of files on cloud. The locations of nodes which are having the fragments of file are not revealed to user. This improvement was made to avoid successful attack. Replication technique called sole replication is used, this technique makes sure that every fragment of data is replicated only for a single time. Sole replication increases the data security without having the multiple copies of fragments thereby reducing the unwanted storage area. Node selection and placement of the fragment for replicated fragments is same as the original file fragments. Data admin will select the number of nodes greater than the number of replicated fragments as done while fragmenting. By repeating the same process will help in avoiding the storage space of any replicated fragments in any node holding the original fragment.

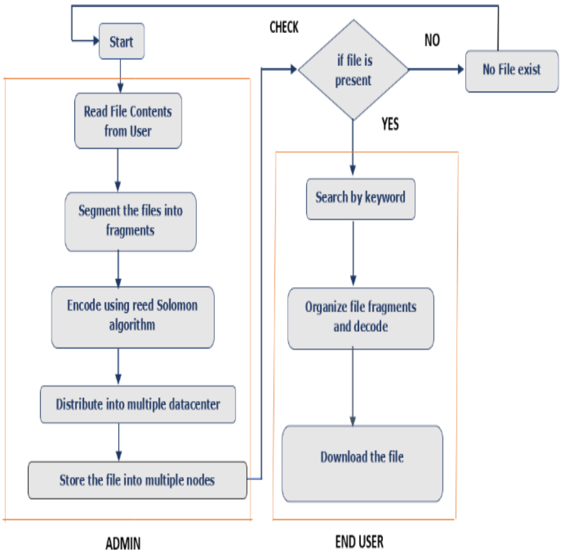
Start
CHECK
if file is present
NO
No File exist
YES
Read File Contents from User
Segment the files into fragments
Encode using reed Solomon algorithm
Distribute into multiple datacenter
Store the file into multiple nodes
Search by keyword
Organize file fragments and decode
Download the file
ADMIN
END USER

Fig 1: Proposed System Flowchart

From Figure 1 of the proposed flowchart, when the process is started initially at the admin end, the contents are read from the user file and then the file is segmented into fragments. Encoding of fragments take place using Reed Solomon algorithm. Then the fragments are distributed into different datacentres by using T-coloring technique. That file is stored in multiple nodes and is used for replication purpose. At user end, if the file is present, the user can enter the keyword to search the operation. And organization of file fragments and decoding takes place using Reed Solomon algorithm and then user will be able to download the complete file.

Advantages of proposed system

a) To keep an attacker unsure about the fragments location and also to improve security.
b) To improve the retrieval or data access time.
c) To make efficient prevention of access

5. SYSTEM ARCHITECTURE

A system architecture is a conceptual model that defines the structure, behaviour and more views of a system. An architectural description is a formal description and representation of a system in a much organised manner.

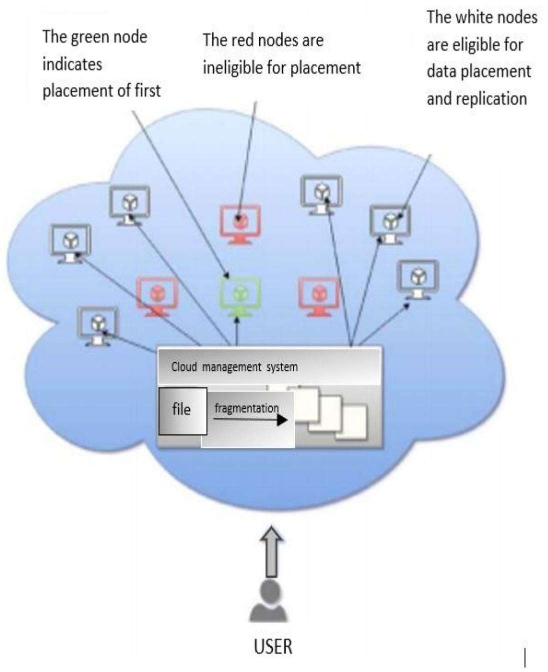
The green node indicates placement of first
The red nodes are ineligible for placement
The white nodes are eligible for data placement and replication
Cloud management system
file
fragmentation
USER

Fig 2: System Architecture

In above figure 2 of system architecture, there are nodes of three different colours. The nodes are coloured with green, white and red colour. Green colour indicates the location of the very first node where the fragment of the file which is fragmented is being placed immediately after fragmentation. White colour indicates the available node for data placement. This node is not adjacent to any node where fragment of same file is placed and it is considered as eligible node. Red colour indicates the node which is ineligible for placing a fragment of a file as it is adjacent to the node having fragment of same file which is already placed. This method of fragments placing ensures that no two fragments of same file are on adjacent node in a network of cloud. The node is present at different geographical location hence the file fragments are spread across the network making it difficult for the intruder to detect. Even if there is successful attack on cloud network and devices, the intruder will get only slice of data which is irrelevant to him.

6. CONCLUSION AND FUTURE SCOPE

Data security has become the vital issue of cloud computing security. The proposed methodology, a cloud storage security scheme collectively deals with the security and performance issues in terms of retrieval time and prevention of efficient access. The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by means of T-coloring. Fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. Currently, users can only use this technique for the text files. This methodology can be improvised for images also in the near future.

REFERENCES

[1] Sanjoli Singla & Jasmeet Singh "Cloud Data Security Using Authentication and Encryption Technique", Global Journal Inc USA(2013).

[2] Sadia Marium, Qamar Nazir, Aftab Ahmed "Implementation of EAP with RSA for enhancing the security of cloud computing" International Journal of Basic and Applied Science(2012)

[3] Shulan Wang, Kaitai Liang, Joseph K. Liu "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing" Member, IEEE, Jianyong Chen, Jianping Yu, Weixin Xie.

[4] Kang, Seungmin, Bharadwaj Veeravalli, and Khin Mi Mi Aung "A Security Aware data placement mechanism for big data cloud storage systems", IEEE 2016

[5] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters", IEEE Globecom Workshops, 2013, pp. 446-451.