# Enhancing Security through Data Swapping and Shuffling Across the Servers in Cloud

Bindia
Assistant professor, S.P.N College, Mukerian.

**Abstract – The shuffle technique is used recently for organizing and accessing data in cloud. We use distributed data allocation among more than two independent servers. Dynamic re-allocation is done by swapping across the servers in such a way that accessing a given node implies re-allocating it to a different server. There is more protection that derives from the use of independent servers as compared to the use of one server. In this paper, we introduce shuffling technique for the use of multiple servers for storing data; introduce a new protection technique (shadow copy) and enhancing the original ones by operating in a distributed system.**

**Index Terms - Access confidentiality, Data distribution, Swapping.**

## 1. INTRODUCTION

While database services provide information sharing and retrieval, there is also a threat to attacks on user privacy. If no proper security is there, a database query transaction will gain access to private information. Cloud computing offers many advantages in data storing, data accessing with proper data management. To reduce down overhead of maintaining data, companies started relying on cloud platforms. End users use cloud as they can access the data anytime anywhere even on their smart-phones. Very good examples of such services are amazon cloud and google app engine. In cloud computing, due to large number of the servers, there is a poor security for the stored data. The threat of data accessing is directly depend on the storage pattern of the data in different servers of cloud. The solution of this threat is swapping across the servers and data swapping. Data swapping implies changing the physical location of accessed data by swapping them between the three involved servers. So there should be a procedure which reallocates data by constant swapping between the many servers, so it will be impossible to access the cloud confidential data by any illegal means. The main idea behind the distribution of data across the number of cloud service providers is to restrict the intruders for retrieving the data, as intruders can retrieve the data in and only if they have access to all of the nodes where data is being distributed. Cloud data confidentiality is getting affected due to various reasons such as software bottlenecks, operator's bugs, and external vulnerabilities. We also introduce a shadow copy technique that ensures protection by making observations by each server as if the server was the only one involved in the access.

## 2. PROVIDING CONFIDENTIALITY

Several techniques were being proposed to maintain access confidentiality. The common thing between all those methods is to cut the link between the data and the location where data is being stored. Shuffling the servers and data items solves the problem. By doing this, it preserves the access confidentiality of the data. The previous system has two servers for normal operation, and each is under attack by a malicious client blended with legitimate clients. The proposed system introduces more additional servers and repeatedly shuffles clients until only one server is being attacked.

### Access Confidentiality

It means to give specific access rights to the specific node. Index structure of static encrypted form does not have the access confidentiality because there is a chance of losing data. The shuffling method discussed above is the best for protection against above attack.

### Content Confidentiality

The content security of the data is similar to the traditional security of the data. Only authorized consumers are able to access the content. Normally life cycle of data in cloud has five phases as

Data Generation: It is a process of generating the data which is to store on cloud.

Data Transfer: It is a process of transferring the data so data integrity and confidentiality of data is need to maintain.

Data use: In this stage the data is in clear format and not secured by the technique of csp encryption

Data Share: It is the process of sharing the data by the data owner, in advance they can share the same data to another parties where the integrity of data is maintained.

Data storage: It is the way by which data is needed to store. It can be SaaS or PaaS.

Archival: It is the phase where the risk of data leakage is maintained.

Destruction: when the data is no longer required for future, then it is necessary to destruct the data as it is unnecessarily

acquiring the space which in turn can be given to the another parties if required.

Pattern Confidentiality

Pattern confidentiality is a process of giving protection to data against the capability of the server to recognize the two separate accesses to the individual node.

Data Distribution

Cloud owner never have the data on their own servers. Their data is located remotely and it is managed by cloud service providers. The main idea behind the distribution of data across the number of cloud service providers is to restrict the intruders for retrieving the data, as intruders can retrieve the data in and only if they have access to all of the nodes where data is being distributed. So for this reason data owner cannot rely on single service providers. Hence reliability and integrity of cloud data can be easily achieved by fragmenting the data and storing across different physical locations. The described fragmentation can be done effectively by using four methods, as

1. Horizontal fragmentation
2. Vertical fragmentation
3. Mixed fragmentation
4. Derived fragmentation

Many techniques were proposed to fragment the data with less amount of encryption so that there will minimum amount of data exposure. In horizontal fragmentation, each fragment consists of a subset of the tuples of a relation R. It is defined using Selection operation of relational algebra as: $\sigma p(R)$. In vertical fragmentation, each fragment consists of a subset of attributes of a relation R. It is defined using projection operation of relational algebra as: $\Pi a1,\ldots an(R)$. In mixed fragmentation, we can also mix horizontal and vertical fragmentation. Derived horizontal fragmentation is a horizontal fragment that is based on horizontal fragmentation of a parent relation. It ensures that fragments that are frequently joined together are at same site. It is defined using Semi-join operation of relational algebra.

## 3. DATA SWAPPING AND SWAPPING ACROSS THE SERVERS

Shuffling technique continuously rewrite and re-encrypt the data to deal with the issue of security of outsourced data. In this technique, actual data is remain hidden from the external storage. In this method client can hide the actual request within the fake request and by doing so it shuffle the content within the block. The shuffling is done in such way that not only third parties but also the server is unable to find the link between the actual data and request data. Shuffle index algorithm is first proposed by the author Sabrina De Capitani di Vimercati and later on they started evaluating by other studies.

To overcome the problem of continuous re-writing and re-encryption, here we are introducing the concept of swapping where more than two independent servers are used to manage the data structures. The main idea behind making use of these servers is security. The protection is giving in such way that for every request to access the node should be transfer to the different server. Also fail of any server will not harm the data. If there is more traffic or if one server gets attacked, then request is shuffled from that server to another server. That's why such system always plays an important role in access confidentiality.

While implementing the technique, less amount of encryption is used. They are making minimum amount of encryption so that the less amount of data will get seen by the other parties. Swapping is a process of changing the server of data once it accessed by the users. Swapping creates confusion to the intruders as data keep on swapping continuously. In data swapping values of data are adjusted in such way that it swaps the fraction of records between the records so the third part intruders will not get actual data. Instead they got garbage data.

To accomplish the task, There is a new technique i.e SHADOW COPY is proposed. Thus system gives the more security with reduced cost. Here two servers are maintained to store the data and the view of each server is maintained in such way that there is only the single server have all the information. One of the major advantages of the system is that while preserving the security it is not degrading the performance of the system.

Data partitioning is used to break down data into smaller chunks to manage and store it quickly without having overhead of storage management. Normally partitioning is performed in alphabetical manner by using certain set of indexes. It fetches the first two letters and checks whether the same folder with the fetched username is existed or not, if the folder is not existed then creates the folder and store file in that folder. This store file is in encrypted format with the key of encryption. When user wants to access the base file that time reconstruction of the partitioned file takes place to serve users. Data partitioning scheme increases the efficiency of the cloud data storage. System effectively reduces the cost of storage and thus reducing the time complexity of the system. Apart from this dynamic operation scheme is proposed where secure encryption and decryption operations are takes place. One more plus point of the system is that it checks the integrity of the stored data to deal with the third party intruders.

## 4. CONCLUSION

Paper gives overall idea about data swapping and swapping across the servers to provide more confidentiality in cloud. Our approach is based on data swapping and swapping across the servers, and on the use of shadow copy for providing to each server a view as if it was the only server storing the data. There is more protection that derives from the use of independent servers as compared to the use of one server. Less encryption is required due to shuffling technique. If One server fails or get attacked, then data will be swapped accross other safe servers.

## REFERENCES

[1] .Priti V. Bhagat, Rohit Singhal, "A review paper on partial shuffle for database access pattern protection using reverse encryption algorithm", IJAIEM(2013).
[2] De Capitani di Vimercati, Sabrina, et al. "Efficient and private access to outsourced data." Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011.
[3] Rautela, Sangita, Arvind Negi, and Prashant Chaudhary. "Data Security and Updation of Data Lifecycle in Cloud Computing using Key-Exchange Algorithm."
[4] De Capitani di Vimercati, Sabrina, et al. "Protecting access confidentiality with data distribution and swapping." Big Data and Cloud Computing (BdCloud), 2014 IEEE Fourth International Conference on. IEEE, 2014.
[5] Reddy, B. AmarNadh, and P. Raja Sekhar Reddy. "Effective Data Distribution Techniques for Multi-Cloud Storage in Cloud Computing." CSE, Anurag Group of Institutions, Hyderabad, AP, India.
[6] Vijay. G.R, A.Rama Mohan Reddy," Data Security in Cloud based on Trusted Computing Environment", IJSCE(2013).
[7] Ali Gholami and Erwin Laure,"Security and privacy of sensitive data in cloud computing: a survey of recent developments,(2015).
[8] https://en.wikipedia.org/wiki/Cloud_computing.
[9] http://www.webopedia.com/TERM/C/cloud_computing.html.
[10] Barik, Sachida Nanda. "Data Swapping in Cloud Computing." (2015).