Efficient and Secure Auditing To Cloud Storage in Cloud Computing

K.Sai Sowmya*1, M.KrishnaSivaPrasad*2

M.Tech (CS) Student, Department of CS, QISCET, ONGOLE, Dist:Prakasam, AP, India
Assistant Professor, Department of CSE, QISCET, ONGOLE, Dist: Prakasam, AP, India

ABSTRACT:

Cloud computing is a prominent technology and computing paradigm bringing forward to many new challenges for security and access control. When users share the private or sensitive content using cloud servers some security issues are raised here. In recent years many number of access control third party software’s are control the data loss and data leakages issues. Third party software’s does not provide the better integrity and confidentiality results content, but still some issues are not resolve. This paper resolves many number of security issues in different dimensions like data access, data sharing, collaborating and etc using multi cloud architectures and Shamir’s secret sharing algorithm. These approaches provide the fault tolerant results.

Keywords: Cloud computing, single cloud and multi cloud architectures, layer wise security, Shamir’s secret sharing algorithm, MD5,

I.INTRODUCTION

Cloud provides data storage related services. All enterprises store the sensitive content on clouds. Enterprises have sensitive information like bank transactions, financial, medical records and other business transactions information. Cloud is not just provide the data storage other services are also provide for customers. Those services are accessing, sharing, streaming, integrity data and collaborating. Cloud data storages are saving the data with the help of third party service providers. In sharing of data from cloud server to customers locations some security issues are generated here, because of security issues we get the disadvantages are data leakage and data loss. Now we introduce the other cryptographic algorithms to provide the integrity and confidentiality results.

This paper includes a list of steps, strategies, techniques and algorithms design to help these decision makers security offers from different number of clouds. Enterprise
information technology business decision makers consider the security implications for provide the secure services to all customers. Security implications like set of policies, controls and technologies provide the protection for data. Layered wise security technology provides the effective security solutions.

![Cloud data Storage Architecture](image)

**Fig 3.1: Cloud data Storage Architecture**

### III. Proposed System:

The data on the cloud has a minimum concern about sensitive information such as social security number, medical records, bank transaction and shipping manifests for hazardous material. We provide additional security by using Shamir’s secret sharing algorithm. Shamir's Secret Sharing is an algorithm in cryptography. It is developed by Adi Shamir. Secret data is divided into multiple parts or shares, which will be stored at multiple different clouds. To reconstruct the original data from multiple shares, we need to have at least k or more shares. WE cannot reconstruct the original data with share value than (k-1). We don’t need all shares to reconstruct the original data and therefore the threshold value (k) is used where any of the parts are sufficient to reconstruct the original secret.

**Advantages of Proposed scheme**

2. Minimal: The size of each piece does not exceed the size of the original data.
3. Extensible: When k is kept fixed, we can add or delete Di shares dynamically without affecting other
4. Dynamic: We can change the polynomial to increase the security and we can reconstruct the new shares.
5. Flexible: for authentication, we can maintain the security unlock categories based on its hierarchy.
IV. Architecture of Proposed Scheme:

Our new architecture supplies the secure cloud database that will assure to prevent all security issues like data leakage and data loss. Shamir’s Secret Sharing algorithm uses the multi clouds architectures reduce the risks and provide the integrity results. Upload and download the file of information into multi clouds. Any cloud compromise with byzantine attacks we get the failure results then same file of information we collect from replicated other clouds data storages. Shamir’s Secret Sharing divide the file into different parts and store into different locations as a secret data of content with different keys. Download the different parts of information from different clouds environment. Any faults are occurring here we use the fault tolerance protocol and supply the integrity results to customers. After download verification with message digest algorithm if its match total data is original data.

V. ALGORITHM:

Algorithm:

Secret Sharing Algorithm:

- In cryptography, secret sharing refers to a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret.
• The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.

Why do we need Secret Sharing Algorithm?

• Gives tight control and removes single point vulnerability.

• Individual key share holder cannot change/access the data.

Mathematical Definition:

• Goal is to divide some data D (e.g., the safe combination) into n pieces D1,D2….Dn in such a way that:
  
  – Knowledge of any k or more D pieces makes D easily computable.
  
  – Knowledge of any k-1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

• This scheme is called (k, n) threshold scheme. If k=n then all participants are required together to reconstruct the secret.

Pseudo Code:

• Suppose we want to use (k, n) threshold scheme to share our secret S where k < n.

• Choose at random (k-1) coefficients a1,a2,a3…ak-1 , and let S be the a0

\[
f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}
\]

• Construct n points (i,f(i)) where i=1,2……n

• Given any subset of k of these pairs, we can find the coefficients of the polynomial by interpolation, and then evaluate a0=S, which is the secret.

Example:

• Let S=1234

• n=6 and k=3 and obtain random integers a1=166 and a2=94

\[
f(x) = 1234 + 166x + 94x^2
\]

• Secret share points

\[(1,1494),(2,1942),(3,2598),(4,3402),(5,4414),(6,5614)\]

• We give each participant a different single point (both x and f(x) ).

Reconstruction:

• In order to reconstruct the secret any 3 points will be enough

• Let us consider

\[(x_0,y_0)=(2,1942),(x_1,y_1)=(3,2598)\]

Using Lagrange polynomials

\[
l_0(x) = \frac{(x-x_1)(x-x_2)}{(x_0-x_1)(x_0-x_2)} = \frac{(x-3)(x-6)}{(2-3)(2-6)} = -\frac{x-3}{2}\]

\[
l_1(x) = \frac{(x-x_0)(x-x_2)}{(x_1-x_0)(x_1-x_2)} = \frac{(x-2)(x-6)}{(3-2)(3-6)} = \frac{x-2}{3}\]

\[
l_2(x) = \frac{(x-x_0)(x-x_1)}{(x_2-x_0)(x_2-x_1)} = \frac{(x-2)(x-3)}{(6-2)(6-3)} = \frac{x-2}{4}\]

\[
f(x) = f(0)l_0(x) + f(1)l_1(x) + f(2)l_2(x)
\]

\[
f(x) = 1234\cdot\frac{(x-3)}{2} + 1942\cdot\frac{(x-2)}{3} + 2598\cdot\frac{(x-2)}{4} = 1234\cdot\frac{x-3}{2} + 647\cdot\frac{x-2}{3} + 649\cdot(x-2)
\]

\[
f(x) = 1234(66x - 94x^2)
\]
VI. RESULTS

Each plot gives the times spent by the client finding a random B-bit prime $p$ and creating $k$ shares for each of the $m$ secrets. We then plot the times spent by the colluding servers recovering $p$ and the $k$ bases. We also give the time spent recovering all $m$ secrets, which is the same for the colluding servers as it is for the client.

![Graphs showing recovery integrity results](image)

**Fig 6. Recovery integrity results**

**Performance Graph**

VII. CONCLUSION AND FUTURE WORK

All Business organizations move their workload to cloud computing. Cloud clients are fear to lose the private information in single cloud. That’s why present paper design to provide the integrity results with multi cloud architectures. We are making the strongest cryptographic technique named as a Shamir’s secrete key algorithm. This algorithm provides the security results like integrity and aggregation. Integrity or aggregation results report is generate from k servers. Multi cloud architectures reduce the security issues. It’s give final results like high availability.

In future we design the some more new cryptographic algorithms and gives the less burden, integrity and confidentiality solutions.

VIII. REFERENCES


Authors Profile:

Name: K.Sai Sowmya, M.Tech (CS) Student, QIS College of Engineering and Technology, Vengamukkapalem, Ongole, Prakasam, AP, India.
Name:
M.KrishnaSivaPrasad,
Assistant Professor,
Department of CSE,
QIS College of
Engineering and
Technology,
Vengamukkapalem,
Ongole, Dist:
Prakasam, AP, India