International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Multi-Cloud Data Security Using Shamir Secret Algorithm

Mahale Paritosh[1], Mahale Roshan[2], Sonawane Vishal[3,] Shinde Dipak[4], Mr.Wani Vipin[5]

[1]Department of Information Technology, S.N.J.B's KBJ COE, Chandwad,paritosh.mahale@gmail.com
[2] Department of Information Technology, S.N.J.B's KBJ COE, Chandwad,roshan77mahale@gmail.com
[3] Department of Information Technology, S.N.J.B's KBJ COE, Chandwad,vishalsonawane141@gmail.com
[4] Department of Information Technology, S.N.J.B's KBJ COE, Chandwad,deepak77shinde@gmail.com
[5] Department of Information Technology, S.N.J.B's KBJ COE, Chandwad,wani.vipin@gmail.com

Abstract— Cloud Computing is very popular world wide use now a days. It is a service provider that provides different Type of services like Software as a service (SAS), Infrastructure As a Service (IAS), Operating System As a Service (OAS) etc. Security is major issue with single cloud, that's why we using Multiple cloud to store the data. By using Shamir's secret algorithm and permutations and combination we divide the single file or data in different part and store it on different type of cloud servers and we can get original data using same opposite technique and for reconstruction we not need all part of file. For reconstruct we need min 50% - 60% data file parts. For Eg. If we divide one file into 6 parts and upload it on different clouds and in case some cloud servers may be hacked or crashed by using other data parts available on remaining cloud we can get original file.

Keywords- Shamir's Secret Algorithmic multi-clouds, cloud storage, data integrity, data intrusion, service availability.

I. INTRODUCTION

We aim to provide framework to supply a secure cloud database that will be guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity.

In relation to data intrusion and data integrity, assume we want to distribute the data into three different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder. This depends on Shamir's secret sharing algorithm with a polynomial function technique which claims that even with full knowledge of (k–1) clouds, the service provider will not have any knowledge of vs. (vs is the secret value) . We have used this technique in previous databases-as-a-serves research. In other words, hackers need to retrieve all the information from the cloud providers to know the real value of the data in the cloud. Therefore if the attacker hacked one cloud provider's password, the still need to hack the third cloud provider (in case where k=3) to know the secret which is the worst case scenario. Hence replicating data into multi-clouds by using a multi-share technique may reduce the risk of data intrusion and increase data integrity. In other words it will decrease the risk of the Hyper-Visor being hacked and Byzantine fault-tolerant data being stolen from the cloud provider.

Regarding service availability risk or loss of data, if we replicate the data into different cloud providers, we could argue that the data loss risk will be reduced. If one cloud vide Fails, we can still access our data live in other cloud providers.

This fact has been discovered from this survey and we will explore dealing with different cloud provider interfaces and the network traffic between cloud providers [1].

II. LITERATURE REVIEW

As we know that data security is important issue in cloud computing. There are various algorithms and methods available for encrypting the data and providing security for the data. For implementing security various encryption algorithms are provide like RSA, DES and Blowfish algorithm etc. But there are some disadvantages of these algorithms used in cloud computing for a secure data encryption. So we are moving towards the AES algorithm. Following table 2.1 shows the comparison between various algorithms. Storage outsourcing is a rising trend which prompts a number of interesting security issues, many of which have been extensively investigated in the past. However, Provable Data Possession (PDP) is a topic that has only recently appeared in the research literature. The main issue is how to frequently, efficiently and securely verify that a storage server is faithfully storing its clients (potentially very large) outsourced data. The storage server is assumed to be untrusted in terms of both security and reliability.

II. PRAPOSED METHODOLOGY

Methodology is a process which consists of the initial task which is necessary for the unknown user to become a registered user to use this type of service. It is basically step by step process from signup to use the service provided by application. The steps used in methodology are as described below [3].

1) SIGNUP

It is the prior step for the user to become a valid user to use the multi-cloud service for the storing data on multiple clouds. It is a part of web front end.

2) AUTHENTICATION

It is a process of verification and confirmation of the registered user account on application of the particular user. After the valid authentication user can do further operations or user this application. It is a part of the web front end.

3) DIVIDE

Accept the data from the user e.g.-text document, image. It is depend on the user in how many parts data going to be divide and also select the unique key which is also used for reconstruction of original data. Then application going to perform mathematical operation on the data to divide and encrypt the data.

4) UPLOAD/DOWNLOAD

From divided data each part is selected to upload on different cloud to store data. Number of cloud to store data is depend upon user.

In downloading phase user login to cloud account download available parts. Minimum 50% parts of original data is required for reconstruction.

5) RECONSRTUCTION

For reconstruction of original data downloaded parts are given as a input to the algorithm. Shamir's secret algorithm is executed to obtain the original data. it is possible to obtain original data from at list 50% part of the divided data. User have to provide key which is used while dividation of data for authentication. If user has valid key and sufficient parts for reconstruction then and only the user can access the original data

III. SYSTEM ARCHITECTURE

In the system architecture has a following four actors are present.

1. User.
2. Local machine.
3. Internet Service Provider.
4. Cloud.

User:

User uses the system for to securely store important data on multiple clouds. User is must be register on the application because this system is only made for register user. It is important that user must provide same key while dividing data using as well as reconstruction of original data using Shamir's Secret Algorithm. If the user login with valid username, password and also the valid key which is used for divide the data then and then only user is allow to use the service provided by application. As the application provide cloud based service user can allow using the service from any ware.

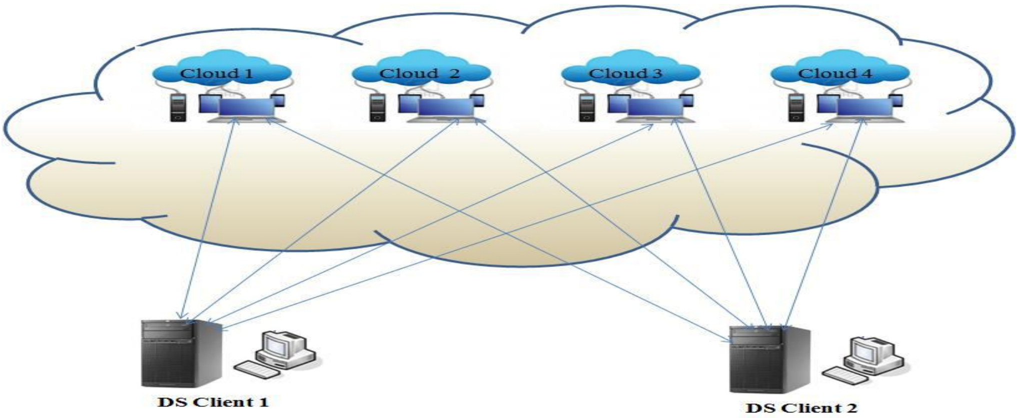


Fig .1.:Multi-cloud architecture.

Local machine

It is a machine on which the application is install. It work on the input data that is received from the user; the user confidational data user wish to store on cloud(e.g-image,text document) is the input for the system for completing storing process. A local server accepts the data input from user. Local server is capable to divide the data into the number of part user wish too because the application is install on the local server. This input consists of digital data like image, text document. Local server check user is valid user or not by validating username and password given by the user. Suppose user is not valid on the application that time application not allows the user to access the service. If the user is new then user has to be signup to access the service. If user is register then that time application allow to user to access the service. User need to provide the key for security purpose. Application accept the data, key and performs mathematical operation on that data to dived and encrypt the original data as per user's requirement. After this, application uploads each part of the data on separate cloud.

Internet Service Provider:

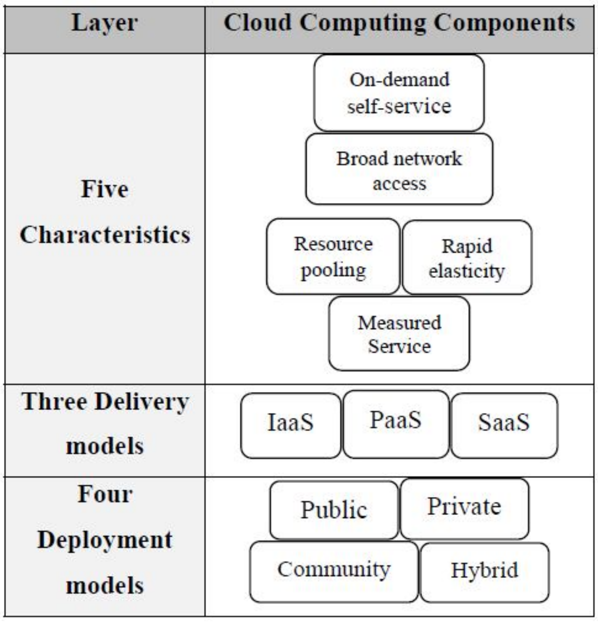
Internet service provider takes input from application. Then this email receipt is send to the user's mail ID which contains the encryption key provided by user at the time of dividing and encrypting the data with the help protocols. An Internet service provider use the
Following protocol
1. Simple Mail Transfer Protocol (SMTP)

2. Post Office Protocol (POP3).
3. Message/Mail Transfer Agent (MTA).
4.File Transfer Protocol(FTP).

Cloud:

The cloud computing is a cost-effective, service availability, exile and on demand service delivery platform for providing business through the internet. Cloud computing resources can
be quickly extracted and scaled with all the processes, services and applications are provisioned on demand service despite the consequences of the user location or device. Hence, the opportunity for an organization to enhance their service deliverance is achieved through cloud computing. The issues in cloud security series from substantial security of the cloud and hardware infrastructure, through the architectural security of function and data deployments, to the actual security of the cloud framework in the presence of peripheral attacks and the mechanisms accessible to respond to and recuperate from these attacks. The use of cloud computing argue services for many reasons including because this service provide fast access the applications and reduce service costs. Cloud computing providers should address privacy and security as matter for higher and urgent priorities. The dealing with single cloud providers is becoming less popular service with customers due to potential problems such as service availability failure for some time and malicious insider's attacks in the single cloud. So now we move from single cloud to multi clouds, intercloud or cloud of clouds. Aim of the project the data security aspect of cloud computing, data and information will be shared with a third party without any problem. Every cloud users want to avoid untrusted cloud provider for personal and important documents such as debit or credit cards details or medical report from hackers or malicious insiders is the importance. It supply secure cloud database that will prevent security risks.

We apply multiclouds concept using Shamir's Secret Sharing algorithm that reduce risk of data intrusion and loss of service availability for ensuring data.



Layer	Cloud Computing Components
Five Characteristics	On-demand self-service Broad network access Resource pooling Rapid elasticity Measured Service
Three Delivery models	IaaS PaaS SaaS
Four Deployment models	Public Private Community Hybrid

Fig. 2. : Cloud layer view

IV. MATHEMATICAL MODULE

In this system, there are three main stages .Firstly user access the each part of data securely store on cloud. Systems read these parts, perform reverse mathematical operation and reconstruct original data.
1. Divide and encrypt the data.
2. Reconstruct original data
For completion the operations of this system we add all this two operation.

1. Divide and encrypt the data.

Suppose that our secret is 1234 (S=1234). User wish to divide the secret into 6 parts (n=6), where any subset of 3 parts (k=3) is sufficient to reconstruct the secret. At random we obtain two (k-1) numbers: 166 and 94. (a1=166; a2=94) Our polynomial to produce secret shares (points) is therefore: F(x) =1234+166x+94 x2
From the above polynomial, we construct following six points: (1, 1494); (2, 1942); (3, 2578); (4, 3402); (5, 4414); (6, 5614). On each cloud will store this shares separately as (x and f(x)).

2. Reconstruct original data

The value of k=3, so we need to have at least three shares to reconstruct the original data. Let us consider the 1st share (x0,y0)=(2,1942), 2nd share (x1,y1)=(4,3402) and the third share (x2,y2)=(5,4414).
To reconstruct the original data, we use Lagrange basis polynomials:

$$l0 = \frac{(x-x1)}{(x0-x1)} * \frac{(x-x2)}{(x0-x2)} = \frac{(x-4)}{(2-4)} * \frac{(x-5)}{(2-5)} = \frac{1}{6}x^2 - \frac{3}{2}x^2 + \frac{10}{3}$$

$$l1 = \frac{(x-x1)}{(x1-x0)} * \frac{(x-x2)}{(x1-x2)} = \frac{(x-2)}{(4-2)} * \frac{(x-5)}{(4-5)} = -\frac{1}{2}x^2 - \frac{7}{2}x^2 - 5$$

$$l2 = \frac{(x-x0)}{(x2-x0)} * \frac{(x-x1)}{(x2-x1)} = \frac{(x-2)}{(5-2)} * \frac{(x-4)}{(5-4)} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore

$$f(x) = \sum_{j=0}^{2} y_{j.\,l_{j(x)}}$$

$$f(x) = 1234 + 166x + 94x^2$$

Recall that the secret has the free coefficients, which means that S=1234, and we are done.

CONCLUSION

The reason of this work is to survey the recent research on single clouds and multi-clouds using secret sharing algorithm and to address the security risks and solutions using Shamir's Secret Sharing algorithm. These algorithms generate their own secret sharing schemes and use secure channels to distribute shares among themselves. The Shamir's secret sharing scheme has a good abstract foundation which provides an excellent framework for proofs and applications. So we are proposing a secure computation platform based on a simple secret sharing scheme than Shamir's. Cloud computing is currently the latest trend when it comes to online computing, it may help the enterprise and the end user by fulfilling their needs, but the user has to make sure that they are valuable and customer data is safe. We support the migration to multi clouds due to its ability to decrease security risks that is affect the cloud computing users. For future work, we aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. The Security can be enhanced if in future any security algorithm is developed.

REFERENCES

[1]T. Paigude and T. A. Chavan, Privacy preservation using shamirs secrete sharing algorithm for data storage security," in International Journal of Computer Trends and Technology (IJCTT), vol. 8, Feb 2014.
[2] A. Pokharana and M. Shweta, Review in cloud computing security," in IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, Mar 2014.
[3] M. K. Alam and K. B. Sharmila, An approach secret sharing algorithm in cloud computing security over single to multi clouds," in International Journal of Scienti_c and Research Publications, vol. 3, April 2013.
[4] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, Cloud computing security: From single to multi-clouds," in IEEE Hawaii International Conference on System Sciences, Aug 2012.
[5] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing," in Journal of Network and Computer Applications, July 2011.