Enhanced Secure Data Sharing in Multi Clouds Environment using Shamir Approach

M.Sowndharya[1], **S. Duraisamy**[2]

[1]M.Phil Research Scholar, Dept. of Computer Science, Chikkanna Government Arts College, Tirupur,
Bharathiar University, Coimbatore, Tamil Nadu, India.
[2]Assistant Professor, Dept. of Computer Science, Chikkanna Government Arts College, Tirupur,
Bharathiar University, Coimbatore, Tamil Nadu, India.

---***---

Abstract: *Cloud computing is convenient and on-demand computing. Cloud computing provides storing, retrieving and processing of resources and data in a cloud environment. Cloud computing provides several service models and deployment models. These features will help provide outsourcing the data with third party storage service providers. The storage provider must assure that the data stored by the user is secure. Data encryptions, hemimorphic encryption, secret sharing algorithms are the techniques extensively used as securing data outsourcing. Single cloud computing provides fast access to their applications and services. But due to the reason that single cloud suffers from many security issues, users and customers are opting for "multi-cloud" otherwise known as "cloud of clouds" or "interclouds". These multi-clouds are secured by various techniques and one of them is Secret Sharing Algorithms. There are many different Secret Sharing Algorithms. This paper focuses more on the issues related to the data security and privacy aspects in cloud computing, such as data integrity, data intrusion, service availability. It proposes a Multi-clouds Database Model (MCDB) which is based on Multi-clouds service providers instead of using single cloud service provider such as in Amazon cloud service. This paper applies Shamir's secret sharing algorithm to secure data outsourcing in Multi-clouds.*

Key words: Cloud Computing, Data Encryption, Secret Sharing Algorithm, Single cloud, Cloud of Clouds, Inter-Clouds, Multi-Cloud, Techniques.

1. INTRODUCTION

By using cloud computing accessing the applications and their utilities through the Internet. By using Cloud Computing create and configure, customize the applications in online. Cloud computing is a technology which is mainly about resource sharing with the motive of high availability and scalability, equivalent to providing utilities over a network. Cloud computing as a whole is providing services and resources on demand, that is on cloud (network). Cloud computing, or in other words "The Cloud", focuses mainly on effective resource sharing. Resources in cloud are not only accessed by multiple consumers rather dynamically reallocated based on its demand. This will improve resource allocation in cloud. The secret sharing schemes are a perfect fit in the multi cloud environment to provide data security in cloud without the drawbacks of encrypting data and service availability failure due to single cloud providers. In this paper, the Shamir's Secret Sharing Algorithm has been used for the implementation of security of multimedia such as video and images in the multi-cloud environment. In order to protect data from hackers, we can encrypt it. But in order to protect the encryption key, we need a different method which increases the complexity of the intended solution. In this work, we propose a new approach to increase the user trust in the cloud using the secret sharing scheme.

2. CLOUD COMPUTING OVERVIEW

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

1. Deployment Models

2. Service Models

2.1 CLOUD SERVICE MODELS

2.1.1 IAAS

Infrastructure as a service should fulfill the essential characteristics to support cloud services. It is built using a shared pool of computing resources, such as virtual compute, virtual storage, operating systems and virtual network. Building a cloud infrastructure is a phased approach, it begins with existing physical infrastructure, its elements and its process and extending to set a Virtualized classic data centers to maintain the data and enables faster resource provisioning.

An example of IAAS providing company is Amazon EC2 and EMC2.

2.1.2 PAAS

Platform as a service is within IAAS. Within the PaaS model, customer's area unit supplied with associate degree package, artificial language execution setting, database, and internet server. they're not concern with the price and management within the hardware and package layers. PaaS is that the use of cloud computing to supply platforms for the event and use of custom applications. The PaaS solutions embody application style and development tools, application testing, versioning, integration, readying and hosting, state management, and different connected development tools.

An example of PAAS is FORCE.COM, Microsoft azure.

2.1.3 SAAS

Software-as-a-Service could be a computer code distribution model during which applications are hosted by a vender or service supplier and created accessible to customers over a network, usually the net.

Example of software as a service is SALESFORCE.COM which provides CRM application on demand.

2.2 VARIOUS DEPLOYMENT MODELS IN CLOUD

2.2.1 PRIVATE

An organization gets access to a private cloud by renting it and also it gets all the permissions to access the resource for its private use.

Example, a cloud developed to solve and serve business applications of a firm.

2.2.2 PUBLIC

A service provider owns the public cloud and he provides it for public for rent. Resources can be owned and also can be scaled in future based on end users requirements.

Some examples of public cloud are Google, Amazon, Rackspace, Microsoft and Salesforce.

2.2.3 COMMUNITY

A community cloud is almost equivalent to a private cloud but it serves to a group of users or in other words to a community. An example of a community cloud is the Media Cloud set up by Siemens IT Solutions and Services for the media industry. A third party can maintain a community cloud or it also can be maintained in a collaborative fashion.

2.2.4 HYBRID

Combination of multiple cloud infrastructures is known as hybrid cloud and the combination can be of any cloud like public, private or community. Hybrid cloud's main objective is to resolve the problem of high demand of resources, that is to obtain effective scalability and availability to serve the consumers with effective cloud service. In this fast developing world, all cloud users are opting for hybrid cloud so as to enjoy better performance cloud facility and security for their data.

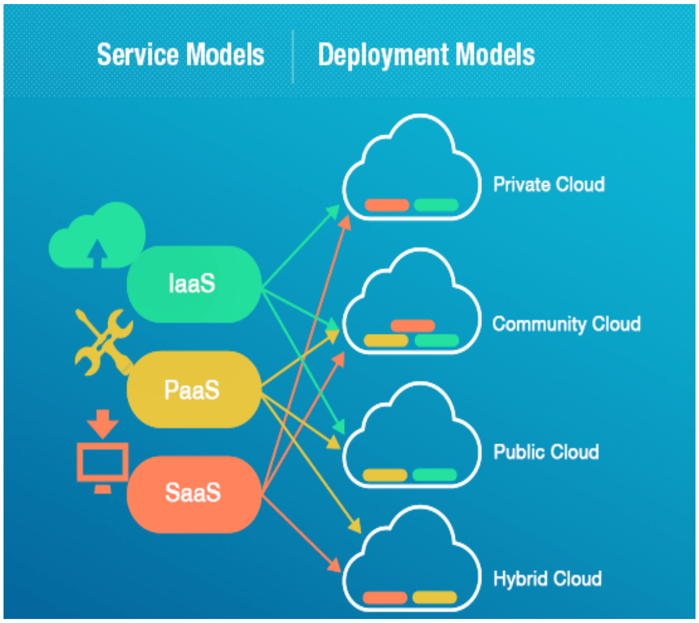

Fig -1: **Cloud services and Cloud deployment models**

In the Figure1 represents the Cloud services and Cloud deployment models.

2.3 SINGLE CLOUD STRATEGY

Cloud computing is another way of maintaining its infrastructure, applications of the organization. Users can interact with data over the Internet by delegating administrative tasks of maintenance to Cloud computing providers.

2.3.1 SECURITY ISSUES IN SINGLE CLOUD DATA INTEGRITY

Data integrity is major security thread in cloud security. Data integrity means stored data may corrupt or loss during transition operation. Ex of data integrity is given bellow In January 2009, servers Magnolia have loss of total data due to a failure; the loss of half a terabyte of it does not possible to recover the data, making the site dead

Data intrusion: Another cloud security risk is data intrusion. If anyone accesses the password of any accounts, then they will be accessing the account's instances and resources, by using the stolen password the hacker to erase all the information user accounts and modify the data or even disable its services.

Service Availability: Another major issue in cloud computing is service availability. If we entrusted our data to store in a single cloud and it does not survey a backup solution or it store the data in a single platform or in a same geographical area they may increase the risk at downtime, and it impacts on customers. Example is Amazon. Amazon underlines in its contract that a service may be cut down at any moment.

2.4 MULTI-CLOUD STRATEGY

Multi-cloud means is the combination of two or more clouds. Multi-cloud overcomes the security risks in a single cloud. In Multi-cloud reduce the service unavailability, loss, and damage of data, loss of privacy. The service unavailability is occurred when hardware breakdown of software or system infrastructure. Replication of data in several cloud infrastructure is one serious advantage of multi cloud. So when one cloud structure is subjected to an attack, another cloud will provide the data. Thus the availability of data is not affected in this type of cloud. Still the attacks and security breaches on multi-cloud are a big threat to confidentiality and they should be prevented. To achieve this many techniques are welcomed and under use by many providers. Some of the techniques are secret sharing algorithms, homomorphic algorithms, Private Information Retrival(PIR) and many more. A multi-cloud strategy can also improve overall performance by reducing "vendor lock-in".

In the Figure 2 denotes DepSky architecture in Multi-cloud. It is a combination of several different storage clouds. This architecture secures availability and confidentiality of data. DepSky model contains clients and a cloud of several cloud storage providers.

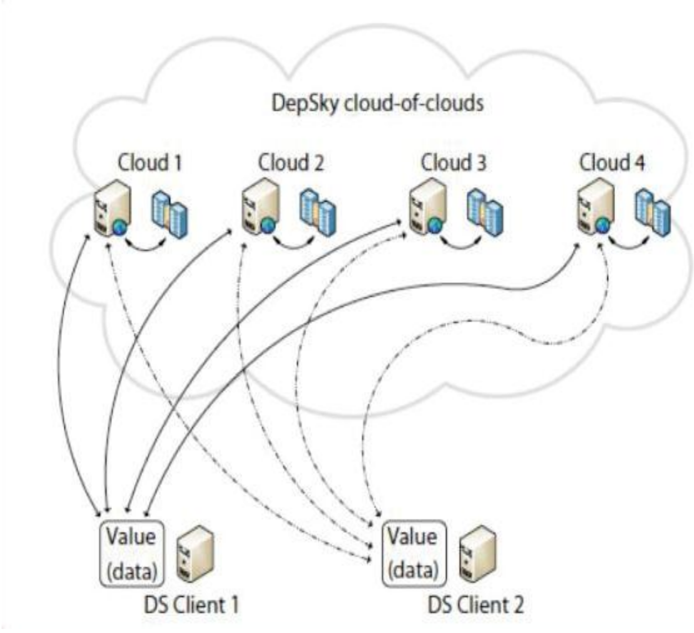

Fig -2: **Depsky Architecture**

3. EMPLOYING SECRET SHARING ALGORITHM

This paper aims to provide a better way to secure cloud database and assure the cloud computing community with highly effective security measures. Secret sharing scheme is a decent tool for cryptography that allows secret information to be shared among a group of people/machines such that predefined set(s) of them can together reveal the secret. To achieve this we are going to employ Shamir's secret sharing algorithm to reduce the risk of data intrusion and service availability in the cloud. It provides authentication to clients and also provide security by encryption and decryption using secret key. There are different schemes of secret sharing as shown in figure 3. We will focus only on one category of secret sharing schemes called threshold schemes.

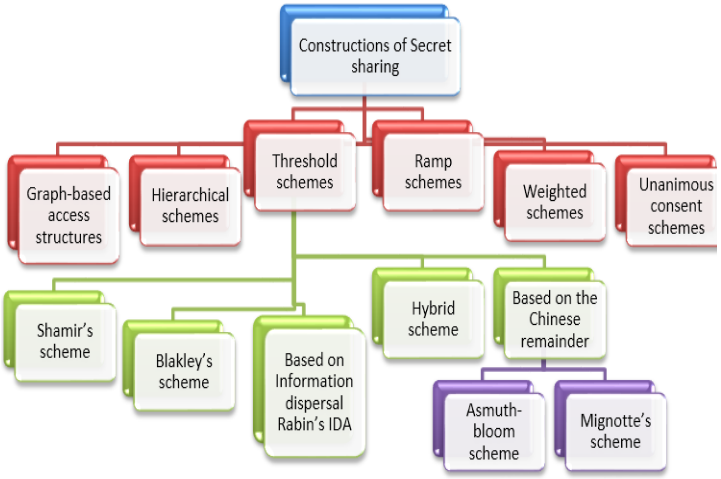
Constructions of Secret sharing
Graph-based access structures
Hierarchical schemes
Threshold schemes
Ramp schemes
Weighted schemes
Unanimous consent schemes
Shamir's scheme
Blakley's scheme
Based on Information dispersal Rabin's IDA
Hybrid scheme
Based on the Chinese remainder
Asmuth-bloom scheme
Mignotte's scheme

Fig -3: **Schemes of Secret Sharing**

3.1 THRESHOLD SECRET SHARING TECHNIQUES

Let k and n be positive integers, k ≤ n. A (k, n)-threshold scheme is a method of sharing a secret K among a set of n participants in such a way that any k participants can compute the value of the secret, but no group of k −1 or fewer can do so.

3.2 SHAMIR SECRET SHARING SCHEME

Adi Shamir, one of the researchers who invented the RSA cryptosystem, designed the first secret sharing scheme in 1979. He published this scheme, based on polynomial interpolation. Data can be compromised or lost in the cloud. Hence securing the data is a vital process in the cloud environment. Therefore to secure the data in multi-cloud, Shamir proposed to store the data in more than one cloud and encrypt the same in the cloud before it transferred and saved.

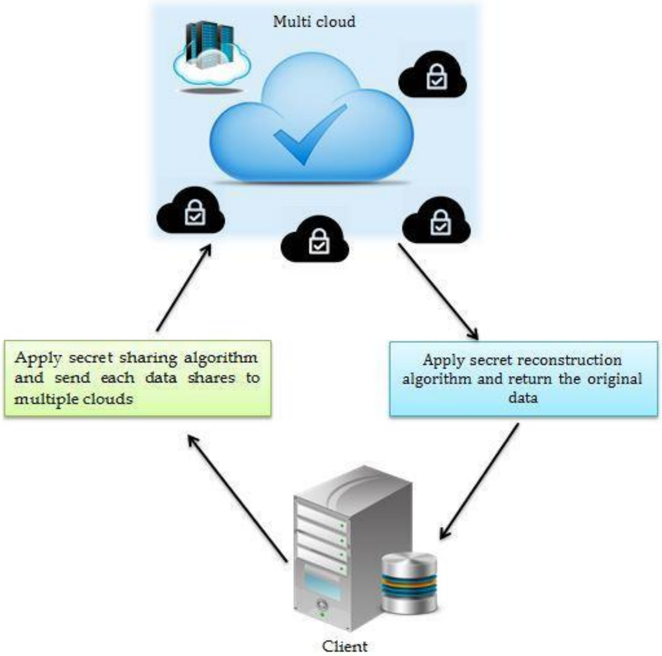
Multi cloud
Apply secret sharing algorithm and send each data shares to multiple clouds
Apply secret reconstruction algorithm and return the original data
Client

Fig -4: **Block Diagram of the Sharing Algorithm**

3.2.1 MATHEMATICAL DEFINITION

The goal of the algorithm is to divide the data DATA into n pieces ($DATA_1$, $DATA_2$, $DATA_3$, $DATA_4$ ……

$DATA_n$) so that,

1. Retrieving any k or more DATA $_i$ pieces makes DATA easily computable.

2. Retrieving any k-1 or fewer DATA $_i$ pieces leaves DATA thoroughly undetermined.

The above scheme is known as threshold (k, n). if k=n, then all pieces are available for reconstruction of DATA.

The objective of Adi Shamir's secret sharing algorithm algorithm is that, k points are enough to define a polynomial of degree k-1.

Choose an approximate k-1 coefficients c^0, c^1, c^2, c^3….c^{k-1} in H, and let c^0 = S, where S is the Secret data which is going to be stored in cloud. Build the polynomial $H(z) = c^0 + c_1z^1 + c_2 z^2 + …… + c_{k-1}z^{k-1.}$ Then n points are defined, for example set i=1,2….n to retrieve (i, H(i)) . A pair is formed with input to the polynomial and output.

Given any subset of k of these pairs, using interpolation the coefficients of the polynomial can be found and the constant term a^0 is the secret.

3.2.2 SHAMIR'S APPROACH

The secret is divided into pieces by considering an approximate degree polynomial

$$H(z) = c^0 + c_1 z^1 + c_2 z^2 + \ldots\ldots + c_{k-1} z^{k-1}$$

In which $c^0 = S$, $S^1 = H(1)$, $S^2 = H(2)$,…………, $S^n = H(n)$ and represent each share as a point

$(z^i, G(z^i) = y^i)$

3.2.3 EXAMPLE

Given example illustrates the algorithm. For understanding, integer arithmetic is used instead of any other vector or scientifically based arithmetic. Therefore the example provided does not ensure perfect secrecy and is not a perfect example of secret sharing scheme.

Encryption and Preparation

Consider 1999 as the secret data. Dividing it into 6 parts (N = 6). Parts required to reconstruct the secret is 3 parts (k = 3). numbers are selected in random. Let it be 154 and 19. a1 = 154 and a2 = 19. Our polynomials to produce shares are

$H(p) = 1999 + 154p + 19p2$

6 parts are constructed from the polynomial. (1, 2172) ; (2, 2383) ; (3, 2632) ; (4, 2919) ; (5, 3244) ; (6, 3607) Different single point is given to each participant, both p and H(p).

Reconstruction

Any 3 points are enough to reconstruct the secret.

Assume: (r0, s0) : (2, 2383) ; (r1, s1): (4, 2919) ; (r2, s2) : (5, 3244)

Apply Lagrange basis polynomials:

$I0 = r - r1/r0 - r1 \,.\, r - r2/r0 - r2 = 1/6r2 - 3/2r + 10/3$

$I1 = r - r0/r1 - r0 \,.\, r - r2/r1 - r2 = 1/2r2 - 7/2r - 5$

$I2 = r - r0/r2 - r0 \,.\, r - r1/r2 - r1 = 1/3r2 - 2r + 8/3$

Therefore, $H(p) = j=2sj.Ij(p)$

$H(p) = 2383\,(1/6p2 - 3/2p + 10/3\,) + 2919\,(1/2p2 + 7/2p - 5\,) + 3244\,(1/3p2 - 2p + 8/3\,)$

$H(p) = 1999 + 154p + 19p2$

4. PROPOSED SYSTEM

Cloud customers may expect on behalf of their past experience and requirements. But the best approach is to gather information about the best and efficient cloud service provider. Customers are also prescribed to ensure the level of security of these important characteristics of the cloud: Confidentiality, Integrity, and Availability (CIA). Security in Cloud computing is organized into different sections: security categories, security in service delivery models and security dimensions. Security in cloud services is dependent on the following:

1. Strong network security should be applied to the service delivery platform.

2. Data Encryption.

3. Authorization is given every Access.

Logs are to be strictly maintained and secured to note down the activities of the system administrators and other restricted users. They can also be used to produce reports that mix events relating to different customers of the service. Security should be applied and maintained in both the organizations seeking cloud solutions and the service providers. Identity and Access Management (IAM), Good governance, compliance, Availability, privacy, Data protection, Business Continuity and Disaster Recovery plans etc.. are some of the measures to ensure security in cloud

5. CONCLUSIONS

Now a day's Cloud computing usage is rapidly increases. The purpose of this work is to study and secure the Multi-cloud using secret sharing algorithm. This objective is achieved using Shamir's secret sharing algorithm. This secret sharing scheme has a good foundation that provides an excellent platform for proofs and applications. Also the disadvantages of single cloud and advantages of multi cloud were addressed in this paper.

Migration to multi cloud is encouraged by keeping in mind about its ability to reduce breaches and other security issues. The Shamir's secret sharing scheme provides best abstract foundation and excellent framework to users application. Applying the secret file sharing (SFS) for all types of files such as (image, document, system file, audio, and video … etc) increases the trust and achieves the security goal.

REFERENCES

[1] I. MOROZAN, "Multi-clouds database: A new model to provide security in cloud computing," CNS, 2014.

[2] Jaya Nirmala, S.Mary Saira Bhanu, Ahtesham Akhtar Patel "A Comparative Study of the Secret Sharing Algorithm For Secure Data In The Cloud". International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.No.4, August 2012, DOI : 10.5121/ijccsa.2012.240663.

[3] Swapnila S Mirajkar, Santoshkumar Biradar, Cachin et al.(2014) ,"Secret Sharing Based Approach to Enhance Security in Cloud Computing", Mirajkar et al., International Journal of Advanced Research in Computer Science and Software Engineering 4(6), June - 2014, pp. 53-57.

[4] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi, "A surveys on gaps, threat remediation challenge, and some thoughts for proactive attack detection in the cloud computing", School of Information and Communication Technology, CQ University QLD4702, Australia. 15 August 2011.

[5] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, "Security and Privacy in Cloud Computing: A Survey" ,Sixth International Conference on Semantics, Knowledge and Grids, August 2010.

[6] Midong Yhou, Zygmunt J. Hass, Securing Ad-Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.