Enhanced Security in Cloud Computing: From Single to Multiclouds

Prof. Shiwani Sthapak
Department of Information Technology,
Dholepatil College of Engineering,
Pune,India

Khushbu Garg
Department of Information Technology,
Dholepatil College of Engineering,
Pune,India

Riddhi Shah
Department of Information Technology,
Dholepatil College of Engineering,
Pune,India

***Abstract*—The cloud computing is a modern technology of storing the information or large amount of data on the internet and accessing it from there. It may happen at times that many malicious users may hack the data or vital information from the cloud, so providing security to these clouds is the major concern today.A cloud can be private or public. In this paper we will describe the multi-clouds which is the clone of the cloud so that users can access information from any one of them and it is readily available.It surveys the recent research related to single and multi-cloud and suggests possible solutions. Also in later section,we are providing security to these clouds because the research shows that cloud security has received less information in past.This paper aims at promoting the use of multi-clouds so that maximum users can make use of this technology.This paper describes how can we overcome the problems related to clouds such as making service availability,increase the response time and to prevent the system from crashing down.Most of these issues can be overcome by using the "multi-clouds" also called as "inter-clouds".This work reduces the security risks related to cloud computing that affect its users.**

Keywords—cloud computing; basic structure; cloud storage; secret sharing algorithm; security,data integrity.

I. INTRODUCTION

The increasing maturity of cloud computing has caused many organizations to migrate from their basic IT infrastructure of storing data and information to adopt the modern cloud technique for storing of the data and information.Cloud computing has become the boom invention of today's internet world. It allows users to fetch the required data at any point of time and from anywhere. Initially people had to buy resources or softwares to store huge amounts of databases but now they can freely avail the service and store the information .Cloud computing is a highly cost effective and readily available technology. It provides service on demand[5].

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single clouds" providers is becoming less popular and a matter of great concern with clients due to potential problems such as service availability, failure and possibility that malicious insiders may exist inside the cloud. This paper focuses on issues related to security of data stored on the cloud as this data will be shared by a third entity the cloud computing users want to avoid any untrusted cloud provider. Protecting the private and critical information such as bank details ,credit card details or a pateint's medical information is of utmost importance [7].

In the diagram below, the architecture of cloud has been shown in which multiple clients have been served by a single cloud.

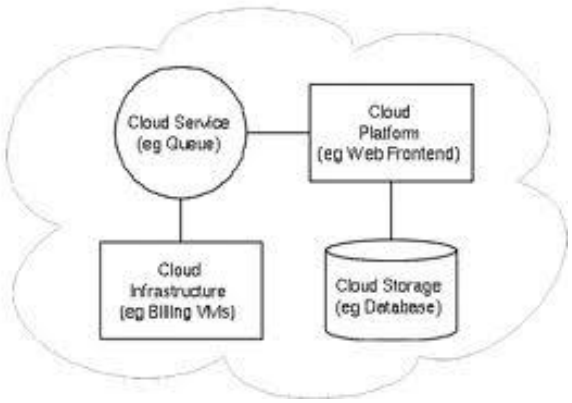

Fig 1.1 Basic Structure of cloud

II. EASE OF USE

The main attributes of cloud computing characteristics are[1]:

- data integrity,
- service availability and
- massive scalability.

A cloud service user may see a different set of attributes and ease of using the cloud service. Let us see some of the benefits of using the cloud services[6].

A. Demand on service:

It is the ability to allocate memory,data and service on demand at any point of time without depending on the external or internal factors [8].Users can avail data as and when required. This manages computing,storage and other applications without it support.

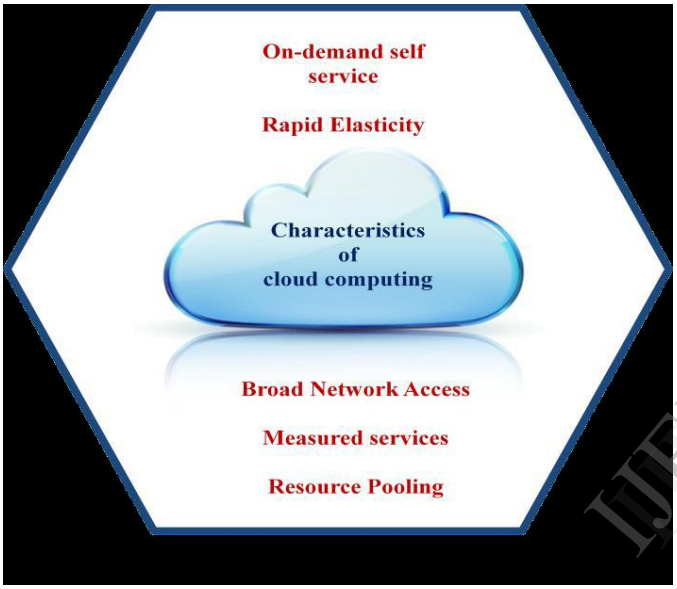

Fig 2:Characteristics of cloud computings

B. Ubiquitous network access :

The ability to work with cloud resources from any point with internet access,cloud service providers are not dependent on being in corporate headquarters or in a data centre to have access to an enterprise cloud[3].

C. Elastic Scalability and Flexible Pricing:

Cloud consumers decide how much of the resource they utilize at any time allocation is driven by immediate demand not the need to maintain capacity.Also it has flexible pricing that means it is very cost effective to use. It does not cost anything to use the cloud services.

III. PROBLEM REPORT AND SYSTEM ARCHITECTURE

The cloud computing service has the following system formation for its structure.

1) user

2) cloud service provider

3) multiple cloud servers

4) service access point

A. Making service access points and time initiation

So as to keep the data away from server failure in every data inclusion by unauthorized person or any internal and external attack coming. One access point is given to the cloud server when the client does some deletion,modification or updation in the files that has been uploaded or downloaded.

B. Loss of availability:

When the data has been removed from the internal company network to an external data center or third party it is inevitable that service unavailability will be experienced.The same type of problem can be caused by the denial-of-service attacks same like the ones that attacked the Amazon E3[2].The Depsky architecture described here deals with this problem by forming clones or replicating for the storage purpose allowing access to the data as long as the data is reachable.One of the common problems can also be the loss or corruption of the consumer data due to various reasons such as system crash,traffic over network,low response time,etc and many such reasons.The Depsky uses the Byzantine fault tolerant replication to store the data on several clouds so that the problems listed above can be recovered.For example- we can say that when the multiple clouds will be created of the same cloud where data will be readily available on all the clouds and the users can easily avail the data from any of the clouds this will definitely increase the response time and reduce the traffic over a single network.Also if one system crashes down or has any problem the users can avail the information from any other clone cloud of the same.

C. Loss of privacy:

As we all know that the cloud service provider has access to all the data stored on the cloud private or public and also to the access patterns.So any of the cloud service provider may be trustworthy, but there may be malicious insiders in the cloud that are causing a widespread security threat to the cloud.This may be a part of serious concern as the cloud may involve storage of critical information like a persons health records or his credit card and bank details[2].Some might suggest to encrypt the data but if the data is consistently being required and used then this may not be an appropriate solution.Because it requires cryptographic keys and generating such keys every time may be a complex process to undergo[10].
The Depsky provides a secret sharing technique and erasure codes to avoid storing clear data on a cloud and also to improve the efficiency of cloud.

D. Disadvantages of the existing system architecture:

Even though it concentrates more on time consuming for user almost every user has to depend on TPA for data integrity whenever he doesn‘t have time for auditing and he automatically can‘t have any stored data size after such type of malicious, Byzantine and system failures to know about data 3 modification, deletion and append in ones own knowledge. But it does not tell about its (data) fixed storage capacity for user‘s stored data in cloud before and after in cloud storage

IJERT

area or in server (how much of data has been stored in server for particular clients in his own allotted storage server area). So it is a major issue to user and also almost users have to depend on CSP for extensive security analysis and depend partially on TPA. It does not tell effective way for server failure. It doesn't make efficient route for data integrity whenever user want required data from his earliest storage in the cloud servers existing. But here the complete access is going to CSP. So it can behave in its own way by hiding any loss of data since the existing system does not tell about the weight or value of stored data using any algorithm.

IV. DEPSKY SYSTEM ARCHITECTURE

This section will explain the recent work that has been done in the area of multi-clouds[4]. Because of this increase in the maturity of cloud computing technology many organizations are moving from IT to adopt to this approach.

A. Depsky architecture:

This section will be representing the DEPSKY system . It starts by presenting the system architecture, then defines the data and system models, the two main algorithms, and a set of auxiliary protocols. Figure 3 is presenting the architecture of DEPSKY. As mentioned before, the clouds are storage clouds without the capacity to execute users's codes. So they are accessed using their so called as standard interface without modifications[2].The DEPSKY algorithms are implemented as a software library in the client. This software library offers an object store interface,which is similar to what is used by the parallel file systems, allowing read and write in the back-end.

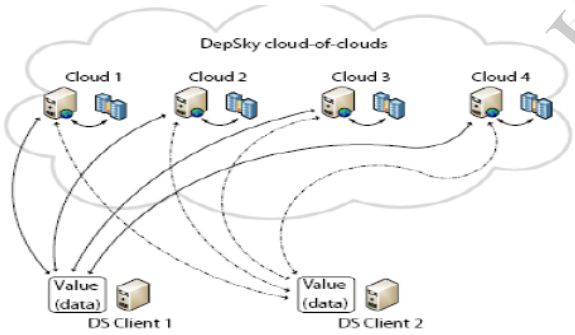

Figure 3:depsky architecture(4 clouds , 2 clients)

The use of diverse clouds requires the DEPSKY library to deal with the heterogeneous interface of each cloud provider. An important aspect is that it is in the format of the data accepted by each cloud. The data model allow us to ignore these details when presenting these algorithms.

Figure 4 represents the DEPSKY data model with its three abstraction levels. In the first (left), there is the conceptual data unit, which corresponds to the basic storage object with which the algorithms work in distributed computing. A data unit has a unique name (X in the figure), a version number (to support updates on the object), verification data (usually a cryptographic hash of the data) and the data stored on the data unit object.[9]. In the second level (middle), the conceptual data unit is implemented as a generic data unit in an abstract of storage cloud. Each of the generic data unit or container, is containing two types of files: a signed metadata file and the files that stores the data. Metadata files contain the version number and the verification data, together with other information's that applications may demand[3]. Notice that a data unit maybe conceptual or generic can store several versions of the data, i.e., the container can contain a number of data files. The name of the metadata file is simply metadata, whereas the existing data files are called value<Version>, where <Version> is the version number of the data (e.g., value1, value2, etc.). Finally, in the third level (right) there is the data unit implementation, i.e. the container is translated into the specific constructions supported by each cloud provider (Bucket, Folder, etc.).

The data which is stored on a data unit can have arbitrary size, and this size can be different for different versions. Each data unit object supports the usual object store operations:

- creation (create the container and the metadata file with version 0)
- destruction (delete or remove access to the data unit),
- write and
- read.

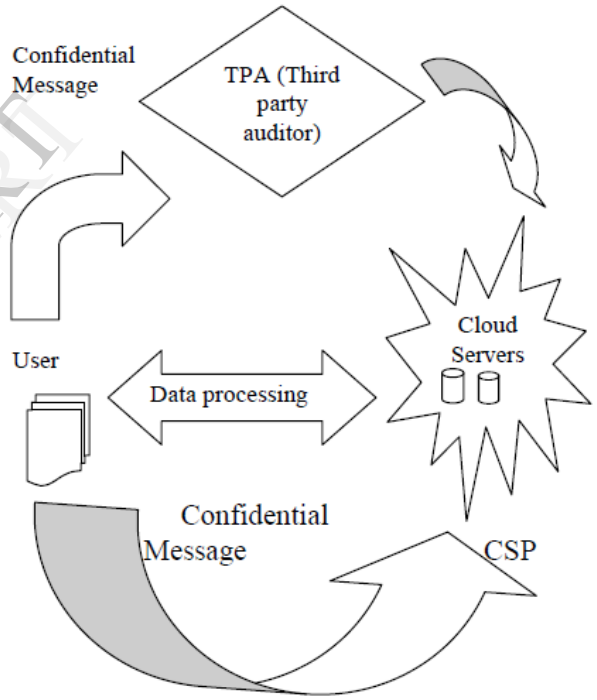

Figure 4: cloud architecture and data processing way

B. Algorithm :

Secret sharing

A secret sharing scheme is a means for *n* parties to carry *shares* or *parts si* of a message *s*, called the *secret*, such that the complete set *s*1, . . . *sn* of the parts determine the message. This scheme is said to be *perfect* if no proper subset of shares leaks any information regarding the secret. Two party secret sharing. Let *s* be a secret, encoding as an integer in Z/*m*Z. Let *s*1 *2* Z/*m*Z be generated at random by a trusted party. Then the two shares are defined to be *s*1 and *s* − *s*1. The secret is

IJERT

recovered as $s = s1 + s2$. Multiple party secret sharing. Let s 2 Z/mZ be a secret to be shared among n
parties. Generate the first $n - 1$ shares $s1, \ldots, sn-1$ at random and set

$$s_n = s - \sum_{i=1}^{n-1}.$$

The secret is recovered as

$$s = \sum_{i=1}^{n} s_i.$$

A (t, n) *threshold* secret sharing scheme is a method for n parties to carry shares si of a message s such that any t of the them to reconstruct the message, but so that no $(t - 1)$ of them can do so easily. The threshold scheme will be *perfect* if knowledge of $(t - 1)$ or fewer shares provides no information regarding s.
Shamir's (t, n)-threshold scheme. A scheme of Shamir provide an elegant construction of a perfect (t, n)-threshold scheme using a classical algorithm called Lagrange interpolation. Firstly so we introduce the Lagrange interpolation as a theorem.Theorem 10 (Lagrange interpolation) *Given t distinct points* (xi, yi) *of the form* $(xi, f(xi))$, *where* $f(x)$ *is a polynomial of degree less than t, then* $f(x)$ *is determined by*

$$f(x) = \sum_{i=1}^{t} y_i \prod_{\substack{1 \le j \le t \\ i \ne j}} \frac{x - x_j}{x_i - x_j}.$$

Shamir's scheme is defined for a secret s 2 Z/pZ with p prime, by setting $a0 = s$, and choosing $a1, \ldots, at-1$ at random in Z/pZ. The trusted party computes $f(i)$, where

$$f(x) = \sum_{k=0}^{t-1} a_k x^k,$$

for all $1 \cdot i \cdot n$. The shares $(i, f(i))$ are distributed to the n distinct parties. Since the secret is the constant term $s = a0 = f(0)$, the secret is recovered from any t shares $(i, f(i))$, for I ½ $\{1, \ldots, n\}$ by

$$s = \sum_{i \in I} c_i f(i), \text{ where each } c_i = \prod_{\substack{j \in I \\ j \ne i}} \frac{i}{j - i}.$$

Properties: Shamir's secret sharing scheme is (1) *perfect* — no information is leaked
by the shares, *ideal* — every share is of the same size p as the secret, and involves no unproven hypothesis. If we compare, most public key cryptosystems rely on certain well-known problems (integer factorization, discrete logarithmic problems) to be hard in order to guarantee security.

Proof of Lagrange interpolation theorem: Let $g(x)$ be the right hand side of .For each xi in we verify directly that
$f(xi) = g(xi)$, so that $f(x) - g(x)$ is divisible by $x - xi$. It follows that

$$\prod_{i=1}^{t} (x - x_i) \Big| (f(x) - g(x)),$$

but since $\deg(f(x) - g(x)) \cdot t$, the only polynomial of this degree satisfying equation (4) is $f(x) - g(x) = 0$.

V. CONCLUSION

Thus it is clear that cloud computing security was a great concern and we have been dealing with this issue in this paper by providing security by using encryption and decryption techniques. Also keys will be provided for security so that no outsider can access the confidential data of the cloud user that has been stored on it. Customers do not want to loose their private information as a result of malicious insiders or hackers in the cloud. Now the users can feel free to use the cloud computing technology for their use as we have dealt with the most serious issue i.e security issues. The purpose of this research paper was mainly to focus in the security of multi-clouds and to promote its use as much as possible. At the same time this paper describes what are the advantages of cloud computing and the algorithm that we have used for the same. We support the multi-clouds system as well as it increases the response time and data will always be available even if one of the servers is crashed other is available for use.
In this paper we have analysed the various issues related to cloud computing security from single cloud to multicloud. We have propose a secured and cost-effective security approach that the cloud users can use which is the cryptographic technique that is within the budget and also assures quality work.
Here complicated, internal, external and malevolent attack is known by our proposed scheme in efficient manner by storage data measurement (i.e., since there can be some modifications in the cloud data). Thus our main idea is giving integrity to the cloud storage area with strong trustworthiness so that user can feel free of worry for his uploaded data in his allocated space. Here our scheme ensures for any extra inclusion of unwanted bits or related things in cloud area so that they can be so easily found out by our data measurement concepts in an efficient way. And it also tracks down how many changes have occurred there in its cloud area.

IJERT

REFERENCES

1) "Cloud computing Challenges and Related Security Issues ". A survey paper, Traian Andrei, ta8@wustl.edu, 14th May 2009

2) Dhulipala. SivaKumar, B.Narsimha, Dr. N. SubashChandra, G.CharlesBabu , SP. Santhosh , "Secured Multi-cloud Environment using DEPSKY Architecture", International Journal of Computer Science and Management Research, Volume 2, Issue 7, July 2013, ISSN 2278-733X

3) B.Arun ,S.K.Prashanth , "Cloud Computing Security Using Secret Sharing Algorithm ", Indian Journal of Research, Volume 2, Issue 3, March 2013, ISSN 2250-1991

4) Vinod Kumar Paidi* , P.Varaprasada Rao , Department of CSE & JNTUH India, " Multi-Cloud Architecture to Reduce Security Risks in Cloud Computing " , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013, ISSN 2277-128X

5) Keiko Hashizume1, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1, " An Analysis of Security Issues in Cloud Computin", Journal of Internet Services and Applications, Volume 4, Issue 5, 2013

6) Sravan Kumar R, Ashutosh Saxena, "Data Integrity Proofs in Cloud Storage", IEEE 978-1-4244-8953-4,2011

7) Saranya Eswaran1 and Dr.Sunitha Abburu2, Adhiyamaan College of Engineering, Department of Computer Application, Hosur, Professor and Director, Adhiyamaan College of Engineering, Department of Computer Application, Hosur. "Identifying Data Integrity in the Cloud Storage " International Journal of Computer Science Issues, Volume 9, Issue 2, No 1, March 2012

8) Satyakshma Rawat, Richa Chowdhary and Dr. Abhay Bansal " Data Integrity of Cloud Storages (CDSs) in Cloud", Intenational Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013, ISSN 2277-128X

9) Shaik.Aafreen Naaz1, Pothireddygari.Ramya2, P.Vishunu Vardhan Reddy3, " Cloud Computing : Use of Multi-clouds"

10) Dinesh.C, P.G Scholar, Computer Science and Engineering " Data Integrity and Dynamic Storage Way in Cloud Computing,."

IJERT