Use of Cryptography and Secrete Sharing Riven the Secrete into Multi-Cloud

Jivan Pandurang Parihar
Department of Information Technology
G. H. RCEM, Pune, India

Vrushali Vyanktesh Kulkarni
Department of Information Technology
G. H. RCEM, Pune, India

Nlam Dilip Acharya
Department of Information Technology
G. H. RCEM, Pune, India

Poonam Dhamal
Department of Information Technology
G. H. RCEM, Pune, India

ABSTRACT
Cloud computing is one of the rising topic in the field of information technology. Now a day many organizations use this technology. There are many benefits of Cloud computing in terms of low cost and accessibility of Data. It is the smart technology and very popular, among all other computing paradigm. Security of cloud computing is a major factor in the cloud computing environment. Users store sensitive information with cloud storage providers but these providers may be untrusted. Due to risks of service availability failure and the possibility of malicious insiders in the single cloud Single Cloud is less popular. Security is one of the major factor that affect the growth as well as the development of cloud computing. This paper aims at the service availability of cloud. In this paper we give the solution for the cloud availability.

Keywords
Cloud computing, single cloud, multi-clouds, cloud storage, DepSky system, Shamir Secrete sharing algorithm, Data transfer security

1. INTRODUCTION
Currently most of the organizations use the cloud computing to store own information of organization. When user deals with the single cloud provider there has problems such as service availability failure and the possibility that there are malicious insider in the single cloud. In recent days, customer has to move towards the multi-cloud. There are many security issues and challenges in cloud computing. In this paper we focuses on the data security of cloud computing. To protecting the data which has been stored by the users on cloud security plays an important role in that. Security plays an important role to the customers trust. According to the National Institute of Science and Technology [NIST] cloud computing is a model forenabling convenient, on-demanding network access to a shared pool of configurable computing resources(i.e., network, server, storage, application, other services) that can be rapidly provisioned and released with minimal management effort or service provided interaction. Cloud computing is classified into four deployment models, i.e. public, private, hybrid, and community. Public cloud is used in a public domain and private cloud is available for specific organization. The hybrid is combination of the different cloud deployment models, whereas the community cloud is for groups of organizations which take care of their agreement and privacy among the organization. There are three delivery models of cloud i.e. infrastructure as a service (IaaS), platform as service (PaaS), and Software as service (SaaS). IaaS, provides infrastructure, i.e servers, hardware, software and other supporting tools to fulfill. User do not need to buy the Infrastructure. In Paas, service providers provide the resources to the user on that user runs custom applications. In SaaS, user do not need to install software on their own machine. All required software are install and run on servers of cloud providers.

2. CLOUD COMPUTING SECURITY
Now days use of cloud computing has been increased very rapidly. Cloud computing refers manipulating, configuring, and accessing the applications online or decreasing the infrastructure costs [1]. Cloud computing security is most important issue for cloud service provider and users. To understand such aspect would help us to design a secure system in cloud computing. Cloud computing suffer from many issue related to its security such as data loss-leakage, shared technology venalities, insecure application interface, malicious insiders, abuse and nefarious use of cloud computing, account service and traffic hijacking. Since all the data is transferred over the internet, data security is major issue in cloud computing. Traditional security mechanism such as authentication, authorization is not only sufficient to cloud computing security.

2.1 Single Cloud In Cloud Computing
Privacy protection and data integrity are the two main issues faced by single Cloud service providers. In his/her own organization one can ensure strong security policies. But in case of cloud computing one has to trust completely on his service provider [9]. Also there is an overhead of managing huge amount of data on a single server. It is easier for malicious outsider to penetrate through security if the data is not actually stored by organization itself; instead they are trusting on third party for taking care of their data. Single Cloud computing require a High cost for cloud maintains process .And in single cloud computing Data has been loss in many times.
Computing
Single cloud can fail in ensuring the complete security from possible threats.

Security Risks In Single Cloud
We have to add more security control to cloud computing so that client’s sensitive data is secure and available all the time when needed. Cloud computing security is major aspect of data intrusion, Service availability and data integrity. To understand such security aspect is very helpful to design secure system in cloud computing. Following are security issues in single cloud or cloud computing.

2.2 Data Integrity
Data integrity is one of the most important issue in the cloud computing. Data stored in cloud computing may be lost or damage during the transition operation in the cloud storage provider. Data integrity in cloud computing security means data stored in cloud server only alter by only by authorized person. Computational integrity implies that the program is executed without being distorted by malware, cloud provider, or other malicious users and any incorrect computing will be detected [2]. Data stored on the cloud is not modified and access by cloud service providers [3]. We have to add more security control to cloud computing so that client’s sensitive data is secure and available all the time when needed. Cloud computing security is major aspect of data intrusion, Service availability and data integrity. To understand such security aspect is very helpful to design secure system in cloud computing. Following are security issues in single cloud or cloud computing.

• Service Availability:
Service availability means cloud service is available whenever user want his or her data i.e. cloud service available on demand. If user want to access his data but cloud server is down then there is huge loss of the user. In July 2008 due to some technical problem in Amazon cloud, the service of Amazon cloud is down for 6-8 hours [4]. Now days Companies seek to protect their data and services from such failure they use of multiple Cloud service providers.

• Data Intrusion And Security Risk
Data security is the most important aspect of the cloud computing security. Cloud computing have three service model Infrastructure as a service (IaaS), Platform as a service (Paas), Software as a service (SaaS) [6]. Cloud computing security involves the identification of threats and challenges and implementing the important step to provide the cloud security.
cloud service [14]. In addition, it also includes arbitrary and crash faults [11]. This paper presents DepSky, a dependable and secure storage system that influences the benefits of cloud computing by using a combination of various commercial clouds to build a cloud-of-clouds. In other words, DepSky is a virtual storage cloud, which is accessed by its users by invoking operations in several individual clouds [12]. This system improves the availability, integrity and confidentiality of information stored in the cloud through the combining Byzantine quorum system protocols, encryption, secret sharing and replication of the data on varied clouds that form a cloud-of-clouds. We deployed our system using four commercial clouds.

**Datamodel**

As the DepSky system deals with different cloud providers, the data format is accepted by each cloud, the DepSky library deals with different cloud interface providers and consequently. The DepSky data model consists of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation.

**System Model**

The DepSky system model contains three parts: readers, writers, and four cloud storage providers. Readers can fail arbitrarily whereas, writers only fail by crashing. For example, they can fail by crashing; they can fail from time to time and then display any behaviour.

In order to reduce the risk in cloud storage, consumers can use cryptographic methods to protect the stored data in the cloud.

### 4.2 Replication Of Encrypted Data Into Multicloud

If in case some data store in one cloud due to server down it can arise the problem of data availability in order to prevent this data(text, image, etc.) has to be encrypted and each copy of encrypted data can be Stored in multi cloud. If user want to download the data from cloud and if in case the matches with the original key then decryption will take place by means of which the user can retain its original data. Simply replicate the data on multiple clouds solves the problem of data availability, but what about security. If there are multiple copies of the data, it will just open more doors for the gate crasher to hack in.

![Fig 4: Replication of Encrypted Data into Multicloud](image)

Thus there needs to be a way in which we can make sure that the data over multiple clouds is safe, or safer than it was in a single cloud. This is when we can apply the Secret sharing algorithm presented by, Adi Shamir elaborated in [10].

**C. Shamir secret sharing**

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. We need secret sharing because 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.

**Construction:**

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.

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

**Reconstruction**

In order to reconstruct the secret any 3 points will be enough D. data transfer security

The Secure Sockets Layer (SSL) is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients. The SSL data security transfer module establishes a SSL safe connection between the client terminal and the front end server of platform by SSL protocol in order to avoid interception, tamper and forgery by non-authorized clients in the process of data transfer [13].

### 5. CONCLUSION

Cloud computing security is still major issue in cloud computing because customer store it’s secret and important information on the cloud server so, its cloud service providers responsibility to provide secure cloud storage. Data Intrusion, service availability and data integrity are major aspect of single cloud security. In this paper we proposed secure and efficient multicloud architecture by using DepSky model, Shamir Secret Sharing Algorithm and use of secure data transfer by using SSL. This Multi-Cloud architecture provide the very secure data transfer and storage on cloud server and also solve the major security problem in cloud computing security.

### REFERENCES


