Vol. IX
Number-3
ISSN 2319-8265
(Special Issue) January, 2018
UGC Number-62976

# EDUCATION TIMES

A Multidisciplinary International Peer Reviewed Journal

# Fretfulness in Inter Cloud Environment

Bharat Chhabra*

**Abstract**

Cloud Computing providers are currently serving customers throughout the world. Inter-Cloud Computing, where a number of providers come together, has already paved its way, to address the growing challenges of load balancing and optimal utilization of resources. At the same time, its objectives also include QoS and SLA accomplishment.

A centralized Inter-Cloud Federation is a confederacy of cloud providers attached to and dependent upon a single unified broker entity. This unified broker acts as a linchpin for the entire system.

This paper envisions and elaborates upon the idea of centralized Inter-cloud federation environment. We propose issues open to centralized Inter-Clouds at two levels namely unified broker and the cloud providers.

***Keywords:*** QoS, SLA, Inter-Cloud computing, broker, centralized federation of clouds.

## INTRODUCTION

Cloud Computing is a relatively new paradigm in the history of computing. Cloud computing offers services and computing resources over the most common medium of access and communication i.e. Internet in a pay-per-use basis. Numerous authors have defined the term "Cloud Computing" in their own ways. The most acceptable and standardized definition out of these turns out to be that by National Institute of Standards and Technology (NIST) [1]:

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Most common characteristics of Cloud Computing paradigm are on-demand access to resources, scalability, ubiquitous network access, multi-tenancy, metered service, elasticity etc. Cloud Computing has a layered architecture with IaaS (Infrastructure as a Service, PaaS (Platform as a Service) and SaaS (Software as a Service).

Next leap in the history of Cloud Computing has already made its way and it involves association between various Cloud Providers to efficiently and impeccably render their services to the Cloud Consumers. When a Cloud Provider serves a number of consumers, sometimes load becomes more than it can be provisioned. Under such circumstances, some of the consumers are denied of services and the overall response time increases. This leads to loss of trust and poor SLA accomplishment. Less optimum but still a solution is to increase the infrastructure. But this infrastructure remains idle most of the time when the workload is at its average rate. To optimally utilize the infrastructure and to reduce the response time, Inter-Clouds have come up, where one Cloud provider can utilize the resources of other Cloud Providers. This is especially useful in case of heavy load and also during

*Department of Computer Science, Govt. College, Kaithal Haryana, India.

Cloud outages. Inter-Cloud is a generic term used for all types of associations between various Cloud Providers. If this association is mutual and with the agreement of all the Cloud Providers, it is termed as a federation of Clouds.

## RELATED WORK

Modern day Cloud providers cannot contain islands of data and set of Virtual Machines aloof from each other. Liang-Jie Zhang and Qun Zhou [2] in their paper "CCOA: Cloud Computing Open architecture" also assert that a cloud should rather behave as an integrated "ecosystem" of cloud service providers, partners and consumers that share resources in a cloud computing environment.

Nicholay Grozev and Rajkumar Buyya [3] in their paper discuss the benefits of moving from proprietary cloud-based applications to inter cloud computing. Due to legislative reasons or response time constraints, a consumer may want to store data at a nearest or a particular data center. It is not possible for a cloud provider to have data centers at every location across the globe. The solution to this problem is using multiple clouds. Secondly, inter cloud computing also results in better application resilience due to more service availability even in case of cloud outages. Another benefit cited by them is "vendor lock-in", is avoided since same workload can be shared among multiple cloud providers. Cloud vendors are equally benefitted by being able to scale-up their resources whenever workload is bursty and increases beyond their limits.

Various cloud Providers come together to form an inter-cloud. This association can take various forms. The federation of clouds can either be peer-to-peer or centralized federation of clouds [4]. In a peer-to-peer federation, each cloud provider has its own broker resulting in a distributed association of cloud brokers. In a centralized federation, there is a single broker entity and all the cloud providers publish their services in the form of SLAs to this unified broker. This broker entity acts as a mediator between cloud consumer and multiple interoperable cloud providers. Broker matches the specifications (QoS, cost etc.) of the consumer request with providers' SLAs and allocates the best fit to the consumer. This is the idea behind centralized Inter-Clouds.

In this paper focus is primarily on centralized Inter-Cloud Federation and various issues associated to the adoption of such an environment have been investigated.

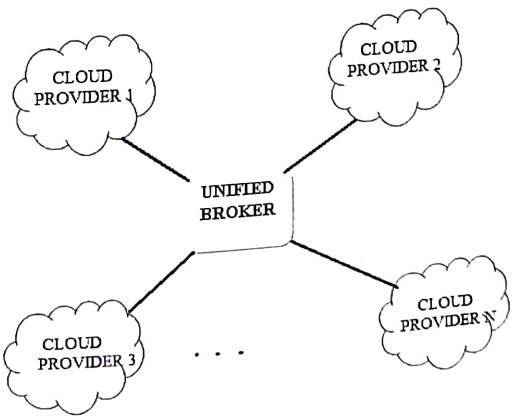


**Figure-1: Centralized Federation of Clouds**

## ISSUES UNDER APPREHENSION IN CENTRALIZED CLOUD FEDERATION

The success of any federation of cloud providers depends on its management and control over its components at different layers of cloud architecture. There are two entities in the centralized federated system namely cloud broker and the cloud providers to do this. To raise the confidence of customers in centralized cloud federation, the broker and a cloud provider need to overcome all technical issues that are critical to resource prediction, allocation and the maintenance of transparency of accounting, location and identity etc.

### Resource allocation

The Centralized cloud federation depends on unified resource broker for resource allocation since at the heart of centralized federation lies the broker. The broker intercepts the requests from cloud consumers along with their service level requirements (e.g. response time, Bandwidth requirements, cost etc.). Scheduling algorithms need to be developed to match the consumer requests with the SLAs published by various cloud providers [5].

### Accounting

As many applications run in parallel, broker has to maintain the complex accounting of each provider and customer in a federated cloud environment. Some of them are transferred from one cloud provider to another amidst their execution (VM images and associated data structures are transferred from one cloud provider to another). Data structures and procedures for accounting of these applications (partly or completely executed) need to be developed at the broker level.

### Transparency

In a centralized federated environment, broker introduces the cloud consumer to its suitable cloud provider after SLAs comparisons. Maintaining the transparency to the user about his effective provider lies on the shoulders of broker and it has to maintain the continuous transparency even if there is a shift in cloud provider before the job completion/execution [6]. The location is visible to cloud provider and not to the consumer. This problem of location awareness increases many fold in federated cloud environment since data is transferred to multiple cloud providers during service compliance. Since data is most vital asset to the owner data location awareness procedures for this purpose must be developed at the broker level [8].

### VM Migratio

VM Migration scenario too requires due diligence that occurs quite frequently in federated environment due to depletion of resources at one cloud provider or due to a cloud outage (of a member cloud). Partially executed services may have to be transferred from one provider to another. Virtual machine images need to be handed over to recipient cloud provider so that cloud consumer doesn't get undue delays. The arrival pattern of the requests for cloud services can serve as an important metric, if analyzed properly. In order to avoid under-provisioning of resources, the broker has to develop some behavior prediction metrics to predict the no. of required resources for each request. These metrics may be developed after a careful study of the consumer requests for a certain period of time [4].

### Identity management

In order to effectively utilize the power of federated cloud environment, the efficient management of identities has to be established. The federated identity provider should employ a single, common

but secure identity to the access the applications between different providers. The federated identity manager should have flexible but extensible architecture to enforce identity security policies and yet be light weight [7].

## Uniform and automated authorization mechanisms

A cloud provider has to authorize the cloud consumer before any actual usage of the cloud service begins. In a federation, such authorization mechanisms need to be enforced which are identical with every cloud provider. Automated authentication methods must be contained which rarely intervene the execution of the service being rendered to the consumer [9].

## Integrity and confidentiality of the data

Undoubtedly, the hesitation in adoption of federated cloud environment can only be fully alleviated or minimized if each participating member cloud provider properly attends the issues pertaining to its efficient service delivery and integrity. A single cloud provider serves many cloud consumers. It is the foremost responsibility of cloud provider to ensure integrity and confidentiality of the data of each cloud consumer whether at disk or "on wire". Consumer must be made aware of the data location and assured about its integrity [9].

Each cloud provider always wishes to avail the maximum of profit by delivering the full services to its customer. But this may not happen in case the available resources are under-provisioned and this may entail the decomposition of the request into smaller requests by the provider. Then only the required small portions of requests may be outsourced and fulfilling the larger request itself. This process of disintegration of request and transferring the workload to other cloud for completion requires vigilant and rational algorithms which actually enhance the throughput and reduces the response time [10]. While service decomposition process a cloud provider has to ensure implementing concurrency control.

## Concurrency and Recovery

A cloud provider handles many service requests from different cloud consumers simultaneously. These may use same storage area for local storage of data. Thus it becomes indispensable on the part of cloud provider to provide locking measures to ensure concurrency control. A cloud provider has to have sound recovery mechanisms. If any of the member cloud provider faces outage, the decisive question that arises is what will happen to the vital data of cloud consumers. A need arises to replicate the data. A decision needs to be taken by the cloud provider regarding the degree of replication i.e. whether the Cloud provider should opt for full replication or not. Second problem is that of dealing with consumer requests in case of cloud outage. Cloud Broker can reschedule the services provided by such cloud providers till they are up and functional again. The performance of federation is also questionable in case unified broker goes down for any unforeseen reason [11].

## Synchronization

Since the federation is made up of independently managed clouds and infrastructure of different administrative domains. So, the federated Inter-Cloud system must be able to specify such inter-cloud gateway translators which support conversion of requests, pattern or formats of data (at SaaS level) and underlying protocols (at IaaS level) from one to another cloud domain [12]. The federation has to confront and support inter-application synchronization and run time infrastructure optimization which includes migration of Virtual Machines from one provider to another, ability to handle new joining/leaving of VMs and resource scaling in harmony with the job's need.

## CONCLUSION AND FUTURE WORK

This paper examined the idea of centralized federation of cloud providers with a view to provide a deeper look into the requirements of inter-cloud federation. The issues addressed above are of higher relative importance from the broker's point of view and from provider's angle. We believe that outcomes of this research revelation, if properly attended, will give significant strength to the centralized federation of cloud providers. The different issues have been highlighted at various layers of the cloud ( SaaS, PaaS and especially at IaaS level). These issues also provide an insight into the inter-cloud federation to a consumer while selecting the one to meet his/her requirements. It also allows the providers to assess the effort that is required to integrate the legacy systems with a federation of clouds. The federation can work in a collaborative manner only if unified broker carries all of its above mentioned responsibilities with due respect. The timely and regular publishing of SLAs, optimizing the load distribution and run time infrastructure optimization are critical factors for retaining the customer. In this work, only equi-probable events (like cloud outage, resource depletion etc.) are assumed to happen. If the relative weightage of each issue is also considered then scenario may become more complicated and a statistical analysis may also be greatly helpful.

The future objective of this research will be on developing the comprehensive solutions to come across these above mentioned issues. These findings will lead to figure out the robust architecture which may be integrated into the existing model. A deeper look into the inter-cloud security mechanisms, legal understanding, monitoring, fixing the responsibilities are other areas of further interest. Undoubtedly, the strength of the cloud providers is really elevated to new heights if they work in a federation of cloud like architecture but it is also evident that these peaks may be maintained only if the issues highlighted in this paper are addressed properly.

## REFERENCES


- Grance, T., "The NIST Cloud Definition Framework". NIST http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-142_cloud-computing.pdf, 2010.
- Liang-Jie Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture", "IEEE International Conference on Web Services", 607-616, 2009.
- Grozev Nikolay and Buyya Rajkumar, "Inter-Cloud Architectures and Application Brokering: Taxonomy and Survey", "Software – Practices and Experience – Published in Willey InterScience", 1-22, 2012.
- Buyya Rajkumar, Ranjan Rajiv and Calheiros N. Rodrigo, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services"," 10th International Conference on Algorithms and Architectures for Parallel Processing",pp 13-31,2010.
- GICTF (Global Inter-Cloud Technology) Forum, "Use Cases and Functional Requirements for Inter-Cloud Computing", August 2010.
- DMTF (Distributed Management Task force) Inc., White Paper " Interoperable Clouds",2009.
- David Nunez et. al, "Identity Management Challenges for Intercloud Applications", STA 2011 workshop,CCIS 187, pp-198-204,Springer 2011.
- GICTF (Global Inter-Cloud Technology) Forum, White Paper "Technical Requirements for Supporting the Intercloud Networking", 2012.
- W. Li and L. Ping, "Trust model to enhance security and interoperability of cloud environment," in Cloud Computing, pp. 69–79, November 2009.
- Tahereh Nodehi et. al, "On MDA-SOA based Intercloud Interoperability framework", Computational Methods in Social Sciences" Vol. I, Issue 1/2013, ISSN 2344-1232
- Tsuda H., Matsuo A.,Abiru K. and Hasebe T., "Inter-Cloud Data Security for secure Cloud-based Business Collaborations", " FUJISTU Sci. Tech. J., Vol 48,No.2, pp. 169-176,April 2012.
- SNE (System and Network Engineering Group)," Intercloud Architecture for Interoperability and Integration", Release 2, Draft Version 0.6, February 2013.