Dynamic Collaboration of Multi cloud- An Efficient use of Cloud Computing

Swetha D.
M.Tech Scholar (CS&E)
VTU PG Centre, Regional office, Mysore

Dr.Thippeswamy K
Professor (CS&E)
VTU PG Centre, Regional office, Mysore

ABSTRACT

Cloud computing is emerging trend of IT delivery in which application data and IT resources are rapidly and elastically provisioned and provided as standardized subscription to users over the internet in a flexible pricing model and effort by interacting with the service provider. . Security of cloud computing is a major factor in the cloud computing platform, as users often store sensitive information and critical application with cloud service providers but these providers may be not trusted. Moreover, the interoperability among the endowment and the flexibility of services from one provider to another is very crucial for the customer to maximize the expected from the cloud. Dealing with the solo cloud providers is predicted to become less popular with customers due to risks of service availability failure , the possibility of malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud thus affecting many user and user gets stick on to the single cloud(vendor lock-in) and has to get all the services from this infected single cloud. A shift towards multi-clouds assists the user to utilize services from multiple cloud service providers in case of failure from single cloud. The efficient dynamic collaboration of multiple clouds provide several potential benefits, such as high availability, scalability, fault tolerance and reduced infrastructural cost.

Keywords

Multi-cloud ,Proxy, Cost effective, Security, Cloud service provider, High Availability

1. INTRODUCTION

Cloud computing gets its name as a metaphor for today’s internet world. Cloud typically contains an outstanding pool of resources, which can be reallocated to different purposes within short span of frames. The process is typically automated and takes minute. Through this technology the providers computing resources are pooled to serve multiple customers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to the demand and they can consume services at any time by their particular needs and pay for what they use. The formation of cloud exchanges is a logical development to provide cost-effective, efficient, and well-managed delivery of services, before cloud computing technologies, the optimization process would require the company or the users to buy and operate a dedicated high-performance cluster of computers but now it become easy to access the application on demand over the network. The agility, efficiency, collaboration and data insights enabled by the cloud are driving the innovation faster than ever before. The cloud platform also provides a huge amount of data storage to the user who can utilize it. Moving data into the cloud offers great convenience to users since they don’t have to care about the complexities of direct hardware management and users need not have to buy individual or costly software, and hardware resources. As more organizations adopt cloud computing, cloud service providers (CSPs) are developing new technologies to enhance the cloud’s capabilities.

The user who wants to access to the cloud service gain all services from the single cloud but the user gets vendor lock-in. The fear of vendor lock-in is often cited as a major problem to cloud service adoption .i.e. user has to use all the service by this solo cloud service provider if users want to gain access to another cloud service provider for more effective and low cost management user has to authenticate to a particular service provider in this way user has to use multi-service provider on individual basis and pay separately for the service to each provider. The concept of multi-cloud has emerged where Multi-cloud approach is the use of two or more cloud services to minimize the risk of service loss of data stored in different location or downtime due to a failure of component in a cloud computing environment. Failure can occur in hardware, software, or infrastructure. So, multi-cloud approach can also improve overall performance by avoiding failure of hardware or software and vendor lock-in and using different infrastructures to meet the demand of the customers. A multi-cloud approach can offer not only the hardware, software and infrastructure redundancy necessary to optimize fault tolerance. Some clouds are better suited for particular services than others for a particular task.

The scenario of multi-cloud presents a model called collaboration of multi-cloud where the user vendor lock-in can be eliminated with an agreement between the various cloud service providers that an authorized user of a particular cloud service provider can gain access to different service provider as per his requirement with low cost management. Cloud mashups are a recent trend[6]. The term mash-up refers to a new breed of Web-based applications to mix at least two different services from disparate, and even competing, Web sites. This service composition offer new functionalities to clients at lower development costs..Cloud data storage redefines the issues targeted on customer’s out-sourced data (data that is not stored/retrieved from the costumers own servers). From a user’s point of view, relying upon a single CSP(Cloud Service Provider) for his outsourced data is not very promising or trusted. In addition, providing reliability and ensuring a high availability of the data can be achieved by maintaining the user’s data block into Multi- cloud so that user will get services at any time even if one cloud is down.

To identify new threats and concerns resulting from these collaboration mechanisms for dynamic collaboration must undergo a rigorous, in depth security analysis across multiple clouds. They must have the support of innovative, systematic, and usable mechanisms that provide effective security for data and applications. Such security mechanisms are essential for gaining the trust of the general public and organizations in adopting this new collaboration of multi-cloud..

2. RELATED WORK

S.Oritz Jr. [1] has review that most of industry observers have limit the future adoption of cloud computing technology. They say that without standard cloud making use of cloud computing is not easy to use and without standardization interoperability of specific application and service functionality from one cloud to another is impossible and it restrict the implementation causing instability in area such as security and interoperability .This standardization involve virtualization which play very important role in cloud platform. Moreover without interoperability would make the user being vendor lock-in. Interoperability of one cloud service provider to another cloud is very important to make customer to except more from cloud computing

M.P.Papazoglou etc. all [2] has review that vendor lock-in is major drawback in cloud computing technology and cloud solution is fraught with many problem that don't allow the developers to mix and match services freely from one cloud service to another. They introduce cloud blueprinting approach so that the developers can easily mix and match the application ,configure, and pool the resources into the cloud . In this approach applications dynamically run on fully virtualized clouds. It outlines the simplified method for provisioning and automating cloud services.

B. Rochwerger et al.[3], has review that, one cloud is not enough as cloud computing becomes more predominant, the problem of scalability has become critical issues for cloud computing providers. The paradigm is more attractive for the consumer because it offers great reduction in capital and operation expenses. But ,as demand for cloud services increasing rapidly in many industry, this result in increases in cost and complexity for the cloud provider may become intolerable. They implemented RESERVOIR European research project to make the cloud providers to deal with complexity and scalability issues. They also introduce the federated cloud that consist of several cloud services providers by making mutual collaboration agreements. A federated cloud can deal with scalability and complexity problems in a cost- effective manner. So it helps the user to use the cloud services in low cost. Providers in the federation cloud can share their infrastructure who have large storage capacity to provide additional resources

Shaik.Aafreen Naaz etc. all [4] has review that, the need of cloud computing has increased rapidly in many organizations. This Cloud computing features provides more benefits to the users in terms of low cost and availability of data. providing security to cloud computing is a major factor in the cloud platform, as users often store very important or sensitive data (information) with cloud service providers but these providers may be untrusted. From a customer's point of view, stick on to a solo Service provider for his outsourced data is not very trusted .Handling with single cloud providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A shift towards multi-clouds, or in other words, interclouds or cloud-of-clouds has emerged where research related to single cloud problem can be addressed by using multi-cloud. Security concerned to the use of multi-cloud has received less attention from the research community than has the use of single clouds. It promote the user to use multi-clouds due to its ability to reduce security risks that can be affected from the single cloud computing user. In addition, data availability and reliability can be achieved by dividing the user's data block into data pieces and distributing them among the available Service providers.

R.Thandeeswaran et al., [5] has review that, along with benefit of using cloud computing with the minimal cost, security concern also need to be addressed for handling sensitive information and critical application. He proposed Multi-cloud infrastructure that can be exposed to the public as utility computing. The use of multiple clouds has the following advantages:

- Import and export data from various clouds;
- Enables choice ability to move clouds easily based on price and services

Level Agreement

- Stops vendor lock-in;
- Automated synchronization of different clouds;
- Fault tolerance with primary back and high availability of data;
- Infrastructure cost reduction.

3. PROBLEM STATEMENT THREAT MODEL AND PROPOSED SCHEME

3.1 Issues in the Existing Methodology

Some of the issues in multi-cloud deployments, regarding cloud interfacing, network management and fault tolerance

Cloud Interfacing: Collaboration of multi-cloud is probably one of the aspects that are receiving more attention by industry. The need for interoperable clouds is two folded: first, the ability to easily move a virtualized infrastructure among different providers would prevent a vendor or proprietary lock-in and secondly, the concurrent use of multi-clouds that are geographically distributed can also improve the cost effectiveness, high availability and reduced the infrastructural cost.

Network Management: The resources running on various cloud providers are located in different networks and may use different addressing schemes (public, private, NAT). But some services need all their components to have a uniform IP address so it is necessary to build an overlay network above a physical network for the communication purpose with different service components.

Fault Tolerance and High availability: Managing the fault tolerance in the cloud is difficult factor. . Also the cloud cannot be accessed easily and some time is needed due to the network traffic and other issues.

Security: There is no secured interaction between the local grid and the cloud.

3.2 Proposed Method

Clouds consist of multiple network-connected resource clusters such as server farms, data warehouses, and so on that host geographically distributed virtual machines and storage components that ensure scalability, reliability, and high availability.

A multi-cloud system that employs proxy for collaboration to provide more security to the cloud. It consists of three architectural components: multiple cloud computing systems, proxy , and clients (or service users).

3.2.1 Collaboration of Multi Cloud System

Collaboration allow client to allow concurrently use services from and route data among multi cloud. There will pre-established agreement between different service provider. This frame work support universal and dynamic collaboration in a multi cloud system

3.2.2 Cloud Hosted Proxy.

Cloud Service Provider(CSP) can host proxy within its cloud infrastructure, it manage all proxy within its administrative domain, and handle service requests from clients for more security. Cloud employs proxy to interact with different services provider. For example, in Figure 1, both CSP 1 and CSP 2 might mutually and dynamically provision sharing and collaboration logic as proxy virtual instances within their respective administrative domains

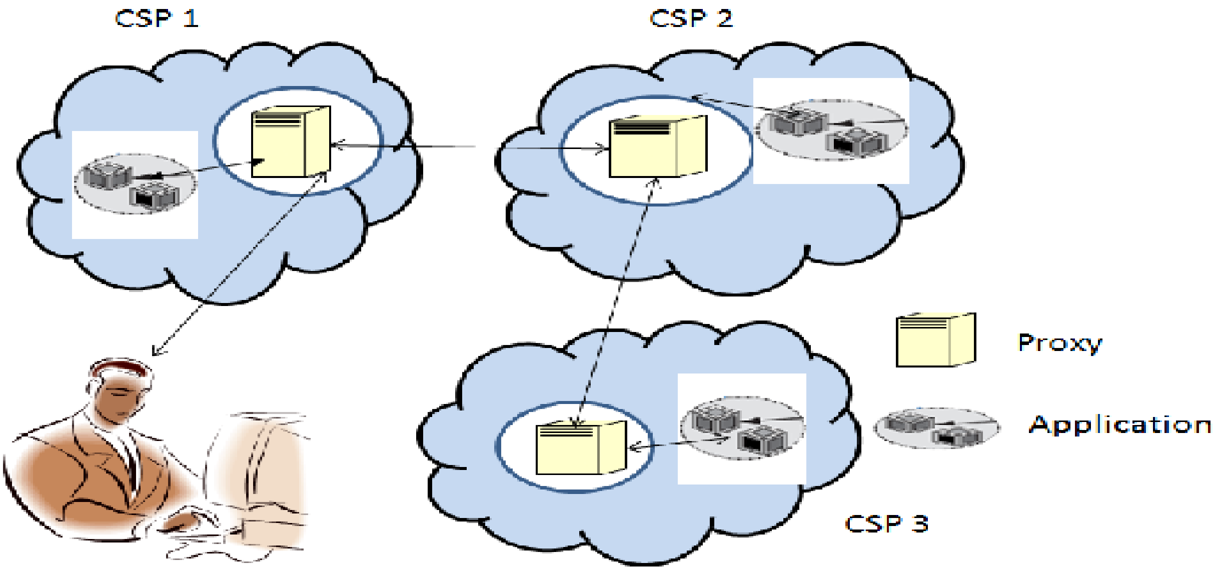

Fig 1 : Architecture Of Multi-Cloud In Collaboration

3.2.3 User Module

Client send request to CSP 1, which dynamically discover the need to use the service from cloud service provider 2 and 3. CSP 1 provides proxy to manage these interactions. A client that wishes to simultaneously use the service from multiple cloud must made an agreement with the different cloud service provider if requested services is not available with agreement cloud, the CSP will provide that services from another CSP if they are in collaboration . In this way user will get the services from multi-cloud.

3.2.3 Proxy as a Service

It involves hosting proxy as an autonomous cloud that offers collaborative services to clients and CSPs. A group of CSPs that are wishes to collaborate can manage this proxy for providing more security. It is an mediator between the CSP and the user. Clients directly subscribe to the proxy cloud service and employ them for interclouds collaboration.

3.2.4 Peer-to-Peer Proxy.

If group of CSPs managed by the proxy can also interact with the peer to peer network that wishes to collaborate. Another possibility is for proxy to have no collective management: each proxy in the peer-to-peer network is an independent entity that manages itself. In this case, the proxy itself must handle requests to use its services and what were the application that comes from the CSP must checked by proxy and then it sent to the user or the client for providing more security.

3.3 Security Issues in Multi-Cloud Collaboration

Security in multi-cloud computing is more and more importance as organizations often store sensitive data on the cloud .Sharing applications that process critical information with different tenants without sufficient proven security isolation, security SLAs or tenant control, results in "loss-of-control" and “lack of trust” problem. Using proxy moves the trust boundary one step further: clients and CSPs now must establish trust relationships with proxy server, which includes accepting a proxy’s security, reliability, availability, and business continuity guarantees . User requesting and receiving the services must be encrypted using AES algorithm for providing high security and password protection key for privileged user’s access. A trustworthy collaboration must be set between the client and Cloud service provider at the initial stage that is during SLA which will help in management and administering proper communication between service provider and the user. Proxy network is a potential platform for developing proxy based security architecture. Data confidentiality on transmission in proxy based network can be achieved using Transport Layer Security Protocol. If the particular application is no longer used by the client or the user then that application can be deleted in the cloud by Cloud services provider .Clean process can be done and so that it save the storage of the cloud.

3.4 High Availability or Service Availability

Another major concern in cloud services is high availability. Google Search is effectively the dial tone of the Internet if people went to Google for search and it wasn't available, they would think the Internet was down. Users expect similar availability from new services. Cloud must provide the services on all the time. For this to achieve services must be replicated. This replica copy must be maintained in Multi-cloud if one particular CSP or proxy is down . It should get services or the application from another cloud if they are in collaboration. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy.

For example if Companies seeking to protect services from any failure need measures such as backups or use of multiple providers. Both Google Mail and Hotmail experienced service down- time recently. If a delay affects payments from users for cloud storage, the users may not be able to access their data. Table 1 show the top 3 obstacles and can solved in collaboration of multi-Cloud

TABLE 1: Obstacles and Opportunity for the growth of Collaboration of Multi-Cloud

Obstacles	**Opportunity for the growth of multi-cloud**
Availability of service	Use Multiple Cloud Providers;
Vendor lock -in	Collaboration of Multi-cloud
Data Confidentiality and Integrity	Deploy encryption and decryption by using AES algorithm

4. RESULTS AND DISCUUSSION

This paper provide dynamic collaboration of multi-cloud where user can receive the services from more than one cloud where two or more cloud are in collaboration such that different cloud services provider will be agreements before providing services to the user . User will get services on all the time(high availability). and user vendor-lock-in can be eliminated and it will be more cost effective to the user. Performances of cloud can be increased if user get the services from multi-cloud that are in collaboration. More security can be provided during SLA. The resulting solution must scale to use for large amounts of data and many CSPs. A client's request for data can result in a large communication overhead in the proxy network. Compression methods such as dictionary encoding can reduce both communication and query processing costs for example, CSPs and proxies can perform much of the query processing over the encoded format.

Data authentication which assures that the returned data is the same as the stored data is extremely important. As customer demand for the internet and device types grow increasingly diverse, industries face a complex set of challenges to satisfy the demands of all end users. so In particular, the speed with which a given Website loads has a huge impact on customer satisfaction. Because faster page loading results in more frequent and longer visits to a given Website. the making use of multi-cloud help the organization to minimize page loading times for all types of services. Finally, multi-cloud scenarios require new privacy definitions that will allow formal proofs of privacy guarantees for protection schemes. so that the user can trust this multi-cloud for outsourcing their data into the cloud

To facilitate dynamic collaboration between clouds. This paper proposes a framework that uses proxy to act as mediators between cloud service provider and the user that must share data and it provides a very high security.. This proposed framework has the potential to overcome several restrictions in the current cloud computing model that can prevent dynamic collaboration among applications hosted by different cloud systems.

5. CONCLUSIONS

Today internet is major need for the all the user they expect services from the cloud all the time. This paper focuses on all the major domains of multi-cloud environment and its efficient interoperability among the users. Where multi-cloud are organized by an agreement between the different service provider to provide low cost functionality to the client in which it end the vendor lock-in of the user which is attained in the single cloud . The user will get highly benefited with multi-cloud environment such as high availability, fault tolerance and reduced infrastructural cost. Here the proxy to act as a mediator between application in multi cloud that must share the data and provide very high security when collaborating the multi-cloud.

6. ACKNOWLEDGEMENT

I would like to thank the Department of computer science & Engineering, VTU University, VTU PG centre, Regional Office, Mysore for providing support to conduct this research work.

7. REFERENCE

[1] S. Ortiz Jr., "The Problem with Cloud Computing Standardization," *Computer*, July 2011, pp. 13-16.

[2] M.P. Papazoglou and W. van den Heuvel, "Blueprinting the Cloud," IEEE Internet Computing, Nov. /Dec 2011, pp. 74-79

[3] B. Rochwerger et al., "Reservoir—When One Cloud Is Not Enough," Computer, Mar. 2011, pp. 44-51.

[4] Shaik.AafreenNaaz, Pothireddygari.Ramya, P.Vishunu Vardhan Reddy., **"**Cloud Computing: Use of Multi-Clouds" pp. 295-304

[5] R. Thandeeswaran, S. Subhashini, N. Jeyanthi1, M. A. Saleem Durai, "Secured Multi- Cloud Virtual Infrastructure with Improved Performance", cybernetics and information technologies XII, (2), pp. 11-22, 2012

[6] Mukesh Singhal and Santosh Chandrasekhar, Tingjian Ge, Ravi Sandhu and Ram Krishnan, Gail-Joon Ahn, and Elisa Bertino "Collaboration in Multicloud Computing Environments: Framework and Security Issues", Published by the IEEE Computer Society IEEE, 2013