INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A REVIEW ON PROXY BASED DYNAMIC DATA OUTSOURCING MULTICLOUDS

Subramanya Chari Meesaragandla[1], Dr. G.Venkata Rami Reddy[2]

[1]Computer Networks Information Security, msubramanyachari@gmail.com
[2] Computer Science Engineering, gvr_reddi@yahoo.co.in
School of IT, JNTU Hyderabad, India

Abstract

Cloud computing is one of the new emerging technology that provides platform, infrastructure and software services for the internet users. Nowadays clouds are getting huge attention due to its ease of services and characteristics and enables users on pay per use basis. If a user wants service from a cloud, he gets vendor lock-in and has to avail all services from that cloud only. In recent times, many organizations are adapting cloud environments, the cloud service providers are also moving towards new concepts i.e. collaboration in multiclouds. Cloud collaboration services enable the internet evolution into a global market. It uses the concept of multi cloud where a user can get services from different clouds at one place. Proxies make cloud collaboration easier and dynamic data outsourcing is possible with different proxy based architectures. In this paper we mainly focused on different methodologies in proxy based dynamic data outsourcing and related security issues in multicloud computing

Keywords*:* cloud collaboration, multi cloud, proxy service provider

1. Introduction

The term *the cloud* is often used as a metaphor over the internet historically. However, when the term "the cloud" is combined with the "computing" makes as a new type of utility computing that uses virtual servers that have been made available for the third parties over the internet. Another view of cloud computing considers it the delivery of the computational resources from a location to your computing location.

Cloud computing delivers a wide variety of services for example, support services, mail filtering services, storages services, platform services, infrastructure services and a lot of full-blown applications. The benefits of the cloud computing includes high computing power, location independence, efficiency and utilization improvement, minimized capital expenditure, device independence and finally very high scalability [1].

Cloud computing brings a new model in the field of IT where a client can gain access to a software without licensing it, a platform to run this software and infrastructure and infrastructure services on *pay per use* basis. Cloud computing also provides a large amount of data storage to the clients. Moving data into the cloud is easy to users since they don't care about the complexities of hardware management and platform requirements. The well-known examples for cloud computing vendors are Amazon Simple Storage Service (S3), Google App Engine and Amazon Elastic Compute Cloud (EC2)[2].

Different methodologies have been investigated to protect the integrity, confidentiality and access control of the outsourced data. The user who gain access to the cloud service gain all these services but the user gets vendor lock-in and has to use all the service by this particular 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 [3].

In multi cloud scenario the user vendor lock-in can be avoidable with an agreement among multiple cloud service providers such that an authorized user of particular cloud service provider can get access to other cloud service providers as per his requirement. To avoid this vendor lock-in problem "software as a service" could be portable on various platform service providers and infrastructure service providers. This portability makes use of the migration from one cloud service provider to another cloud service provider in order to take the advantage of better quality of service and cheaper prices.

Cloud mashups are the recent trend in multi cloud collaboration. Various cloud mashup centre are Force.com for Google App Engine, Appirio cloud storage and IBM's mashup centre. But the architectures, protocols and other platforms required for establishment of such collaborations are on research level. Here, another point is that it may be difficult for different cloud service providers get into collaboration so that an authorized user of a one cloud service provider can gain access to another cloud service provider.

In multicloud provider concept the service provider is responsible for provisioning of various cloud services. Thus the service provider contacts possible IaaS providers, get the details of their terms of use and negotiate if necessary, then deploy services and monitor their operation and migrates their services potentially from various infrastructural service providers. Placement of services on different infrastructural providers is treated as multiple instances of deployment and they are managed independently.

Apart from these things the main role of the researchers is to develop a mechanism for this mashup centre or collaboration into real time for the cost effective and standardized use of cloud computing. Here while implementing these mashup centre, security issues also generate when these mashup centre starts working. So the service provider must look around it to not make it as a threat. This paper will present all the scenarios related to the cloud collaboration and use of proxies for dynamic data outsourcing.

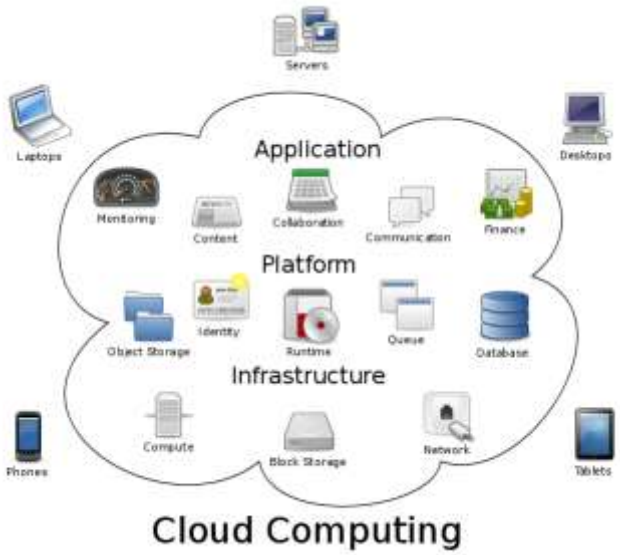

Figure 1: Cloud Computing Overview

2. Literature Survey

This is a survey paper based on the work done by the researchers in the new era of cloud computing i.e. "collaboration in multicloud environments". This will give the present techniques which are used for the collaboration of multiple cloud environments i.e. to transfer from single cloud architecture to multicloud architecture, solutions to security issues and cost effectiveness of multicloud compared with a single cloud. Multicloud computing gives more freedom to the user to choose the cloud which is suitable for him.

Multicloud computing provides usage of the data from different cloud vendors, synchronization among multiple cloud providers for cost effectiveness and free from vendor lock-in system. The main problem with the multicloud computing is its working i.e. since it has to work in distributed environments and services from different service providers have to be collaborated. To do this, researchers working on "collaboration framework for multicloud environments [4]" proposed a proxy based framework.

In this framework proxies are used at different levels of collaboration. These proxies can be set by the organizations or institutions and developed by the cloud service providers to get access for different clouds. These proxies also used for the secure communication between the service providers and the clients.

To protect data at rest and data in transit, proxies must provide a trusted computing platform that prevents malicious software from taking control and compromising sensitive client and cloud application data [4]. This can also manage the security issues of the cloud computing.

The cloud computing services have been classified into three categories mainly. They are Software as a service (SaaS), Plat form as a service (PaaS) and Infrastructure as a service (IaaS). The important point here is that the cloud service providers must be able to provide the above stated services on a distributed environment of multicloud. For this purpose the research work done on "A Federated Multi-cloud PaaS Infrastructure [5]" is used since it gives platforms for various services in a multicloud environment paradigm.

From the research work of "Cloud Brokering Algorithm[6]"(it is an algorithm given based on the virtual infrastructure of clouds for the allocation of Virtual Machines(VM) on static and dynamic basis)the cost effectiveness of multicloud problem can be solved before shifting to the collaboration framework.

This paper is based on the survey of the techniques which are helpful in moving from single cloud system to multicloud system. Whenever a new technology is emerging a new platform is required and a framework is needed, all these factors are included in this paper with the consideration of cost effectiveness on the side of users\clients.

3. Methodology

This section explains the methodologies proposed by the researchers which are described in the literature review.

3.1 Proxy based framework

Researchers are proposed a proxy based framework for multicloud computing. This framework allows dynamic data outsourcing in multiple cloud vendors and resource sharing among different cloud based services. It also addresses security issues relating to privacy, trust and policy issues without pre-established standards or agreements in collaboration. It uses proxies at various levels in multicloud environments. They are

3.1.1 Proxy as a Service

In this scenario a group of proxies are deployed as an autonomous cloud and it is managed by a third party service provider or multiple cloud service providers who are in the collaboration.

3.1.2 Cloud hosted Proxy

In this scenario the proxies are hosted by the cloud service provider within its infrastructure administer. Cloud service provider manages these proxies and also manages the service requests from the clients who want to access these proxies.

3.1.3 Peer-to-Peer Proxy

Proxies can also be used to interact in peer-to-peer network. Here also these proxies are managed by a third party service provider or cloud service providers who are in the collaboration.

3.1.4 On-premise Proxy

Here, the client himself can host proxies in his infrastructural domain and manage these proxies. The cloud service provider who wishes to collaborate with other cloud service provider will have to implement these proxies on the client infrastructure who requested the service and use them.

3.2 Security Issues

Security is the major factor since applications having critical information are shared with different cloud service providers. So lack of security isolations, security service level agreements (SLAs) leads to lack of trust and loss of control problems [7]. By using proxies the trust limit increases further. i.e. cloud service providers and clients must establish trust relations like proxy's availability, reliability and security with proxies[6].

Apart from these it also provides business continuity guarantees. A trust worthy collaboration is needed in management and administration between the cloud service provider and the client with proper communication. In this framework, different types of proxy's networks are established. Some are established on client side and some established on cloud service providers side and so on. It clearly says that the control over the proxies and assets are in the cloud service providers administration. Proxy networks are the best platforms to develop proxy based architectures. TLS (Transport layer security) protocol is used to provide confidentiality for the transmitted data in proxy networks. Some other techniques are Simple public key infrastructure to provide secure access and Warrant-based proxy signature for delegation singing rights technique to provide authentication to the proxies.

3.3 A Federated multi-cloud PaaS Infrastructure

This offers solutions to security problems like geo-diversity, interoperability and portability for the management of both SaaS and PaaS. Different layers of cloud (SaaS,PaaS,IaaS) provide various dedicated services. As their granularity and complexity varying, a principled definition of these services is required to promote the federation and inter-operability among heterogeneous cloud environments. This is based on three models. They are

3.3.1 Open service model

To run the service oriented applications, service component architecture is required. It contains the notion of binding which supports interaction among multiple protocols. Hence, it is user for the definition of services in both SaaS and PaaS.

3.3.2 Configurable federated multi-PaaS Infrastructure

A federated multi-PaaS infrastructure is depended on configurable kernel implemented in concrete cloud environment. A SPL (software product line) is described as a set of software intensive system which share a managed set of common features developed from core assets. The basic idea of SPL is to grasp the variability among multiple clouds and also to use it as a component in Software Configurable Architecture.

3.3.3 Infrastructure Services

In this, initially a service list is scheduled according to the service requests from the clients and then it allocates the nodes and supplies the services and applications and deploy the configurable kernel. In second step, it deploys the instances of the kernel. And finally, SaaS and PaaS can be deployed on either application level or on kernel level.

4. Conclusion

This paper reviewed all the techniques relating to the multicloud collaboration, a new paradigm emerging in cloud computing. This multicloud framework allows consumers to use services for fewer prices as compared to the single cloud. This multi-cloud environment ends the vendor lock-in system which is presented in the single cloud and gives freedom to the consumer. The major concern in this field is that the agreement between the CSPs (cloud service providers) for collaboration of their services. Finally, at the end the consumer will get highly benefited in this multicloud collaboration and consumers will get services according to their requirement and preference.

References

[1] 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

[2] Cong Wang, Student Member, Qian Wang, Student Member, Kui Ren, Senior Member, Ning Cao, and Wenjing Lou, “Toward Secure and Dependable Storage Services in Cloud Computing”, IEEE transactions on services computing, V, (2), 2012.

[3] Swaraj P. Thakre, Prof. Nitin R. Chopde, “ A Review of collaboration of multicloud – An Effective use of cloud computing ”, IJAIEM V(2), I(3)

[4] 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.

[5] Fawaz Paraiso, Nicolas Haderer, Philippe Merle, Romain Rouvoy, Lionel Seinturier, “A Federated Multi-Cloud PaaS Infrastructure”, 5th IEEE International Conference on Cloud Computing pp.392 – 399, 2012.

[6] Jose Luis Lucas-Simarro, Rafael Moreno-Vozmediano, Ruben S. Montero and Ignacio M. Llorent, “Cost optimization of virtual infrastructures in dynamic multi-cloud scenarios”, Concurrency and Computation: practice and experience Concurrency Computat.: Pract. Exper. Published online in Wiley Online Library (wileyonlinelibrary.com). 2012.

[7] Mohamed Almorsy, John Grundy, and Amani S. Ibrahim, “TOSSMA: A Tenant-Oriented SaaS Security Management Architecture”, 5th IEEE Conference on Cloud computing IEEE, 2012.

A Brief Author Biography

M. SUBRAMANYA CHARI – M.S.Chari is pursuing his Post Graduation in Computer Networks Information Security from School of Information Technology, JNTU Hyderabad. His research areas of interest include Computer Networks, Cloud Computing and Information Security.

Dr. G Venkata Rami Reddy – He is presently working as an Associate Professor in Computer Science and Engineering Dept. at school of Information Technology, JNTU Hyderabad and course Co-ordinator for Software Engineering Dept. He has more than 11 years of experience in Teaching, and Software Development. His areas of interests are: image Processing, Computer Networks, Analysis of Algorithms, Data mining, Operating Systems and Web technologies.