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

A NEW APPROACH TO DYNAMIC DATA OUTSOURCING IN MULTICLOUDS USING PROXIES

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 a new computing paradigm offering infrastructure, software and platform services to the internet users. Nowadays most of the services required for an IT organization or an Individual user are obtained through cloud computing. World's top most IT organizations are entering into cloud computing and become as a cloud service providers (CSP). Cloud service providers offer services to the users as "*pay per use*" basis. If a user wants to use a service from a CSP, he has to accept the service level agreements. Then he gets vendor lock-in and avail all services from that cloud only. It's not possible for a user to get multiple services from multiple CSPs. To avoid this scenario, collaboration among multiple cloud environments is required. Nowadays cloud service providers are also eyeing on collaboration services. So by using Proxies collaboration in multiple clouds is possible. Proxies make it easier by communicating with each other. For this proxy based architecture is to be implemented. At initial stage we focused on how to share data among multiple clouds and then it can be implemented to services and applications.

Keywords*:* Multi cloud, Cloud Collaboration, Proxy, Data storage

1. Introduction

Cloud computing is the biggest thing in the world of IT. It is a new computing paradigm providing virtual servers that users, IT departments and organizations can access on demand over the internet. The biggest contribution made by cloud computing is the globalization of the computing assets.

Cloud computing offers various services which include infrastructure services, software services, applications services and much more. The advantages of cloud computing are low expenditure, independent of device and mobile, high efficiency, improved utilization, high scalability and high computational power [1].

The characteristics of cloud computing are massive scalability, multitenancy, elasticity, self provisioning of resources and pay per use basis. Multitenancy makes sharing of resources among multiple users. According to the organizations hundreds or thousands of systems, Massive scalability allows to scale resources tens of thousands of systems along with bandwidth and storage space. Elasticity provides the users rapidly increase or decrease the usage of resources and release of resources to other users when it is no longer required.

Cloud services are mainly classified into three categories. They are

- Software as a Service
- Platform as a Service
- Infrastructure as a Service

1.1 Software as a Service

Software as a Service (SaaS) delivers applications through a browser to thousands of end users over the internet. For the users there is no need to put any cost for licensing the software or in servers. Among multiple enterprise applications, the best-known example for SaaS is Salesforce.com. Nowadays SaaS is also used for human resource applications and enterprise planning. Google Apps. is the another example for SaaS, which provides a wide range of office and business applications access through online via a web browser.

1.2 Platform as a Service

Platform as a Service (SaaS) is another variation of Software as a Service (SaaS), which provides web services, various platforms rather than applications. It provides application programming interfaces (APIs) to develop various applications instead of delivering a full-blown application. Google App Engine is best-known example for Platform as a Service (PaaS) provider. It provides dynamic web serving, automatic load balancing and scaling, APIs and local development environments.

1.3 Infrastructure as a service

Infrastructure as a Service (IaaS) provides various infrastructure to build an organization. It provides servers, storage, network and computer hardware.

All the above services are billed based on the usage of the services on monthly basis or as their wish how they pay monthly bills.

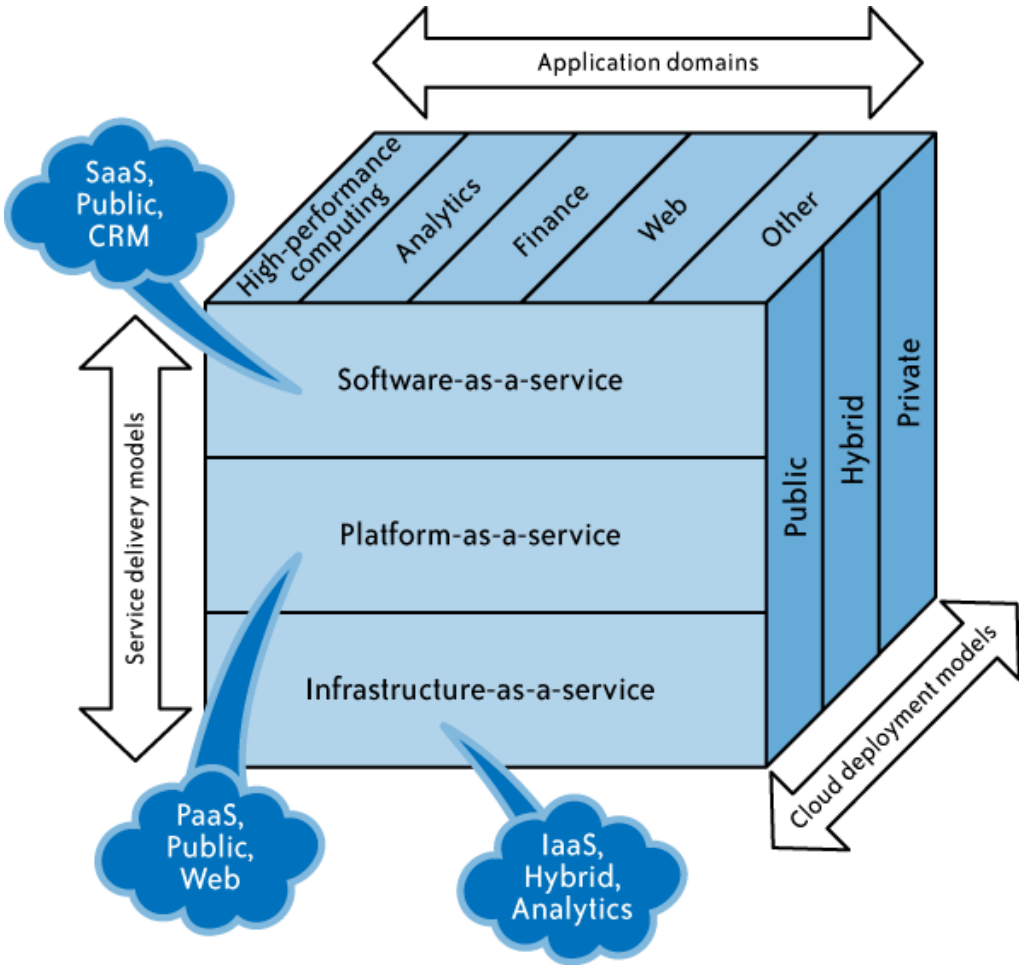

Figure 1: Cloud computing service model

Clouds are mainly classified into three types of clouds. They are public clouds, private clouds and hybrid clouds. Public clouds are the clouds which are available for all the users over the internet. Everyone can use them. Private clouds are the clouds which are specific to some organizations and which are maintained by organization itself. Hybrid clouds are the combination of both public and private cloud. *i.e.* a cloud service provider who is providing public cloud may also provide a private cloud for some other organization.

2. Literature survey

Cloud computing is a new era in the field of computing and IT. Here, user can access all types of services as pay per use basis and he can use software without licensing it and platforms and infrastructures to run applications. Moving data into the cloud is easy and it provides a huge amount of storage to the users.

In general, a user gets vendor lock-in and allowed to use services from a single cloud. But to get lower costs and high performance of services he has to use multiclouds. For this he needs to authenticate multiple times while accessing the services from multiclouds and he has to accept the service level agreements which are different for different clouds. To avoid this problem, collaboration in multiple cloud computing environments is required.

The key factors which are involved while moving data among multiple clouds are data integrity, confidentiality and access control. Apart from these, security issues relating to user data and inside the cloud are also has to be addressed. The recent trends in collaboration are cloud mashups. Examples for cloud mashups are IBM mashup center, Appirio cloud storage and Force.com for Google App Engine. Protocols, architectures and various platforms are required to extend the cloud mashups. But they are at the research level and one more difficulty is the authorization of a user (belongs to one cloud) to multiple clouds.

Different methodologies have been suggested for collaboration in multiple clouds in the paper titled "Collaboration in Multicloud Computing Environments: Frameworks and Security Issues [2]". They are

- Cloud hosted proxy
- Peer-to-peer proxy
- Proxy as a service
- Proxy based framework

But the entire above are suggested to use the applications of one cloud by the user of another cloud. But practically, this doesn't work since every cloud service provider has his proprietary applications which are not at all available in other cloud service providers. Second thing is, it increases the competition among multiple clouds and it may leads to drop of their own clients also. A lot of security issues may come since they are giving complete access to their applications. So step into this type of collaboration directly is not possible. So, to avoid these issues we are trying to use step by step process initially starting with the sharing of data in multiclouds.

3. Analysis and Design

A third party administrator (TPA) is required to outsource the dynamic data in multiclouds. TPA is responsible for provisioning of services from multiclouds. TPA contacts with the clouds which are in the collaboration and establish service level agreements with them. He manages the services provided by them and utilization of resources cost and negotiates if possible.

This framework mainly contains three modules. They are

- Client/User module
- Third party administrator (TPA) module
- Cloud service providers module

3.1 Client/User module

This module mainly fulfills the activities of the client. This module contains the implementation of the user interface. It includes the user activities like uploading the files to the cloud, updating the files and downloading the files. To do all the activities he needs to be the client of the cloud service provider. Once he becomes the client of the framework then he use the services of the multiclouds in the collaboration.

3.2 Third party administrator (TPA) module

Third party administrator (TPA) maintains the track of all the users in the framework. He has the entire information and he can authenticate the users. He has to maintain service level agreements and standards with all the clouds in the collaboration and also acts as a mediator between user and cloud service providers. He gets the requests from the clients and forwards it or shares it to all the clouds.

The following figure illustrates the entire mechanism of dynamic data outsourcing in multiclouds using proxies.

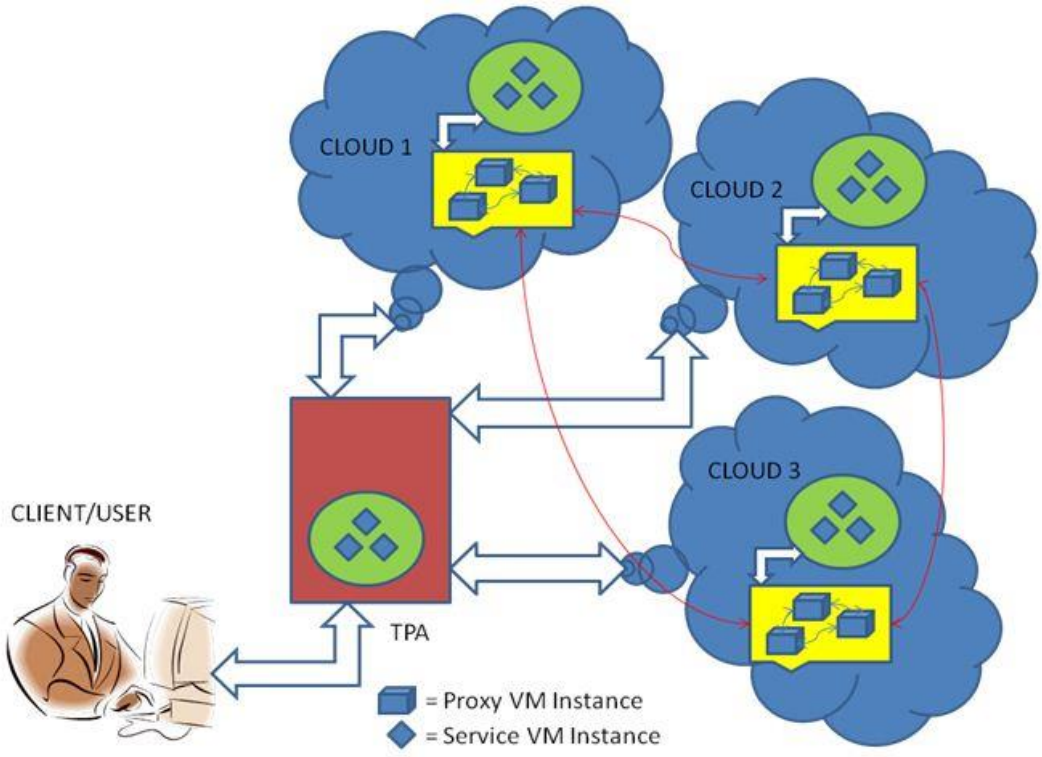

Figure 2: Proxy based dynamic data outsourcing Multiclouds

3.3 cloud service provider module

Cloud service provider provides various services to the clients. CSP receives the service requests from other proxies and verifies the proxy identity and then store the data in the cloud. It maintains all the file records including user name, identity, service id, proxy service provider etc..

Whenever the proxies get requests from other proxies to obtain a specific user data, then it gives the permission to get that data.

4. Implementation and Security Issues

4.1 Implementation

To implement this framework we require a third party administrator (TPA). As this framework involves collaboration in multiple clouds, trust among multiple clouds and security issues are the major factors. Here a question may arise who may be the third party administrator. Here the TPA may be the outsider who is not in the collaboration or he may be one of the cloud service provider or all the cloud service providers may act as a TPA.

In general if the TPA is an outsider who provides third party services then all cloud service providers must agree for that TPA. They must form standardized interfaces, protocols and service level agreements which are accepted by all cloud service providers. But this mechanism once again looks like a third layer between user and

cloud service provider. This may increase the complexity and arise new security issues since the user has to register with the new TPA.

Another possibility for this TPA problem is to make any one of the cloud service provider as third party administrator (TPA). For this also all cloud service providers must agree for that cloud as a TPA. But it is a new responsibility for the cloud service provider who comes forward to acts as a TPA. But the positive thing is fewer burdens on the implementation of protocols, interfaces and standards since they are all most same or similar to the security protocols, interfaces and standards used by the cloud service providers.

More reliable and possible solution for this is to make each and every cloud service providers to acts as a TPA. *i.e.* every CSP in the collaboration have the access to accept the requests from the users and then by using proxies they can send the data to other CSPs. By doing this mechanism trust among multiple clouds is improved and security issues also resolved since all the clouds are involving in the collaboration framework.

4.2 Work Flow

User who wants to store his data in multiple clouds, login to the framework and upload his files to the cloud. Then the cloud service provider verifies the credentials of the user and authenticates the user weather valid user or invalid user. To make collaborations proxies are used. Proxies act as a mediator between user and the cloud service provider. Proxies transfer the control among them and provide the services to share in multiclouds. Then he verifies the data and by using proxies he send the data to remaining cloud service providers. After that it is available for the user to download the file which is in the cloud.

4.3 Security

Security is provided at each and every module. User data is protected by using security algorithms. Encryption algorithms (e.g. AES algorithm) are used while uploading the files into cloud. A secret key is also generated by using random key generator and that key is used in the security algorithms. Either the user or the TPA doesn't know the secret key. Key is generated automatically by using random function generator and is used automatically.

Before uploading the file to the clouds, the file data gets portioned into small parts. The number of partitions is depends on the number of clouds in the collaboration. If *n* clouds are in the collaboration then the file is divided into n parts. The partition of file is done by dividing the entire file size with the number of clouds. By doing this each sub part of the file is having the same size. Then proxies are used to send the sub parts to the other clouds in the collaboration.

As the data is encrypted before the partition of the file, even the cloud service providers are also not able to see the original data. They can't modify the data and even they can't decrypt the data since they don't know the key. Likewise security is provided to the user data at CSPs.

To download the user file, user simply login to the framework and he can download it. When user requests for download, then automatically proxies collect the data in various clouds and merge the entire data into the single file. The file then decrypted by using AES decryption algorithm and using the automatic key which is generated earlier. User can update the data which is already uploaded into the cloud. All the updates done by the user are reflects at the cloud service providers also. Here one of the best features provided to the user is, user can know which data is stored in which cloud and he can modify the data in a specific cloud also. Likewise data is stored dynamically in multiple clouds by using proxies.

5. Conclusion and Future work

Cloud computing is the present trend spreading rapidly around the world. In this technology age, a lot of technologies are inventing day by day. In cloud computing also a lot of innovative services are coming by the cloud service provider. Hence it is the correct time to make collaborations among multiple cloud service providers to get the atmost experiences of the services. To make collaborations proxies are used. Proxies act as a mediator between user and the cloud service provider. Proxies transfer the control among them and provide the services to share in multiclouds. As an initial step, here we discussed about the process of storing dynamic data in multiclouds. In future it can be implemented to share the applications, services, software, infrastructure and etc. Hence proxies are used to make dynamic collaboration in multiclouds and these techniques can be enhanced to offer more services.

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] 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.

[3] 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.

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

[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 interests 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.