ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 6, June 2015

Collaboration between Various Clouds' and Client Using Proxy Framework

Sandeep Muktinath Chitalkar[1], Ashok M. Kanthe[2]

Student, Computer Department, SIT, Lonavala, India [1]

Assoc. Prof., Computer Department, SIT, Lonavala, India [2]

Abstract: Cloud computing is a method of providing resources over the Internet. Security challenges are still foremost concern when we considering collaboration between multiple cloud's service providers (CSP). In cloud, user's information or data is stored in multiple CSP. To access those information or data to other CSP user they need to pay amount or preestablished agreement between all CSP's. Having this issue in mind, this paper focus on the development of Proxy Framework Controller/ Environment (PFW), to determine the uploading and downloading the data or information from multiple CSP. More ever this research aims towards new framework to share data between multiple CSP. This framework also provides heterogeneous data storage on their respective cloud (Amazon, Rackspace and Cloud Sigma).

Keywords: cloud mash-ups, cloud service provider (CSP), Proxy Framework Controller (PFW), trust and privacy issue, Cloud Service Buyer (CSB).

I. Introduction

Cloud computing deals with computational resources as a services and providing storage to the multiple Cloud Service Buyers (CSB) in the form as Database as a Service (DaaS), Software as a Service (SaaS) etc. Software as a Service [1] ensure to provide services to the Cloud Service Buyers (CSB) based on pay as per usages schema where customer or CSB need preestablished agreements among all the Cloud Service Providers (CSP), but they does not need to installed or configure any application on their local computers or nodes.

The primary focus of this paper is to introduce Proxy Framework Controller / Environment (PSW) for sharing the resources between multiple cloud service providers (CSP) [2][3]. The rest of the paper is organized as follows:

Section II: Provides a state of art.
Section III: Issues in current system.
Section IV: Describes the proposed model in details.
Section V: Performance of the proposed framework in simulated testing of data.
Section VI: Conclusion.

II. State Of Art

In cloud computing mash ups environment enamors threats are raised. One of the threats is Data sharing between multiple CSP. A lot of researcher focuses on the trust issues or user authentication using encryption and decryption methodologies in cloud and introduced many solutions to decrease the threats of the trust and authentication. Security challenges in the cloud may be classified as an:

a) Protection of information or data towards CSB side.
b) Protection of information or data towards CSP end.
c) Protection of information or data in storage server or Cloud Data Center (CDC).

An optimized authentication procedure (using encryption algorithms) is used for accessing database of trusted Cloud Service Provides (CSP) for any Cloud Service Buyers (CSB) from another cloud environment.

The system proposed in this paper offer a secure Proxy Framework which allows data security of the user as well as protects the cloud mashup against other external customers [4]. This system also offers a wide usability model which helps the CSB to communicate with the multiple CSP through Proxy Service Provider. The proposed model offers a extra level of the security in which records (like text file, audio, video etc.) are uploaded in any CSP like Amazon, Rackspace and Cloud Sigma after undergoing encryption mechanism.

III. Related Work

Cloud computing has been cited as an "5th utility along with the electricity, water, gas, and mobile phones" whereas computing services are available on customer or buyer demands, like other services available in the human society. Cloud computing have limited support for resource management and provide support: negotiation between Quality of service and service level agreements. Several issues are addressed like service providers and clients, market registry for publishing and discovering CSP and their providing services, QoS, mode of payment as per services provided by CSP's [1].

Cloud computing is a way of providing better utilization of the resources using the virtualization methods. Cloud computing use different service delivery models by which different services are provided to the service buyers. Cloud services provides an services to the multiple users by many ways i.e. Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Desktop as a Service (DaaS) on pay per use basis or on demand self service. SaaS is a software deployment model where application is hosted remotely or by CSP and made available to the users on demand over the internet by paying charge as per uses. Data sharing between clouds is major issue in multiple clouds. The best security solution is implement web application framework [2].

Client need to established Service Level Agreement (SLA) with cloud service provides. Policies or agreements are differing as per the clients of the CSP each time. The CSP are bounded with only SLA signed between different CSB's. Author advice to encrypt a data before transferring to CSP. Author introduced multiple trust model which help for establishing secure communication between CSB and CSP. Hence the suitability of all these models for use in cloud computing environment needs extensive evaluation work [3].

Table 2 shows the survey for security algorithm and data integrity support in cloud environment**.**

Table 2: Security algorithm and Data integrity support in cloud.

Year	Cost	Security Mechanism	Environment	Support data integrity
2010[1],[2]	Low	-	SC	Yes
2011[3]	High	Depsky Algorithm	SC + MC	Yes
2011[4]	Medium	File Division method	SC + MC	Yes
2012[5]	Medium	Token method	MC	Yes
2013[6]	Medium	Proxy Framework	MC	Yes

There are so many challenges that are pulling back the expansion of the single cloud to multi cloud environment (Cloud mash –ups).

Current cloud mash-ups required pre- established agreement among the service providers as well as the cloud service buyer (CSB) [6]. CSP and CSB are both replay on the pay per use model. One of the well-known service are offered by the CSP is Data Storage, in which CSB don't want to store their data or information on their servers, instead of that they store their data on CSP side servers. These types of services don't provide flexibility for data storage but they provide the benefit for the amount of data they are going store for particular amount of time. In addition to that CSB can access those data from any location as long as they connected with the internet. In cloud mesh-ups data move remotely in cloud servers [7]. Cloud remotely share this data as per client request but CSB have to pay some charges to the CSP.

We focus on the new methodology i.e. Data as a Service (DaaS) which provides a data on demand to CSB across various platforms over the internet using proxy framework. DaaS support data sharing from remote locations at anytime due to this it reduced the cost of data management. The main issue for implementing proxy framework is its introduction of proxies at different levels of the cloud service providers (CSP). These all Proxy Service Providers (PSP) or Proxy Service Controller (PSW) implemented by the CSP or the managed by the organization so they gained the information from multiple CSP. These PSP are used to establish secured communication of transaction between CSB and CSP. To protect the stored information on the CSP's side, PSP provides a trusted platform for CSP and CSB.

The system proposed in this paper offer a secure Proxy Framework which allows data security of the user as well as protects the cloud mashup against other external customers. This system also offers a wide usability model which helps the CSB to communicate with the multiple CSP through Proxy Service Provider. The proposed model offers an extra level of the security in which records (like text file, audio, video etc.) are uploaded in any CSP like Amazon, Rackspace and Cloud Sigma after undergoing encryption mechanism.

IV. PROPOSED FRAMEWORK FOR MULTIPLE CLOUD SYSTEM

We focus to overcome preestablished agreement between CSB and CSP and pay as peruse limitation in current cloud mash-ups we introduced new framework that used as a generic collaboration between clients, mobile user and cloud application for simultaneously use of services from framework controller and route the data from multiple CSP to the CSB.

In the market information providers may be registers with multiple CSP and they promote their existing data to multiple CSP. CSB provide a request with his/her specification to CSP, Then CSP search required data in his database if required data is available then it provided to the CSB otherwise requested CSP dynamically determine the data from other CSP whose data fulfill the CSB request with consideration of data availability. Figure 1 shows the proposed architecture of proxy framework for accessing the data from multiple clouds without establishing an agreement between them. CSB appeal for data to cloud1, which dynamically determine the need to use services from another cloud2 or cloud3. Cloud1 send request to proxies to manage this interaction between multiple clouds.

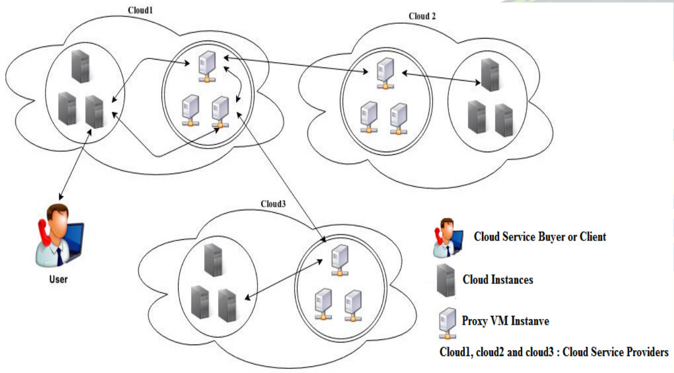

Cloud1
Cloud 2
Cloud3
User
Cloud Service Buyer or Client
Cloud Instances
Proxy VM Instanve
Cloud1, cloud2 and cloud3 : Cloud Service Providers

Figure 1: CSB request to CSP for data.

Cloud collaboration allows CSB and cloud application to concurrently use the services from multiple CSP and route the information from multiple CSP. The framework support collective and dynamic collaboration between multiple CSP. CSB simultaneously utilize the services provided from multiple CSPs without any prior business agreement between multiple CSPs.

This framework allows dynamic data resourcing from multiple CSP and resources sharing between different clouds based services. It also addresses the security issues regarding privacy of CSB, trust and policy issues without pre-established agreement or standard in collaboration between multiple CSPs. It uses proxies in different level in multiple cloud surroundings. They are as follows:

1. Proxy as a Service

Here group of proxies are developed as an independent cloud and it is managed by the multiple CSP those are in collaboration.

2. Cloud Hosted Proxies

Here proxies are managed by CSP within same infrastructure or administrative area. CSP manage these proxies and manage the services requested by the CSB who want to access the data from other CSP. Proxy instance must be provided by the CSP.

A. Algorithms

In this section, we introduced two proposed algorithm are discussed to determined uploading of data based on CSP and downloading of data as per service or request of CSB and getting information if the request made by CSB is based on trust requirement of CSP's.

Algorithm for uploading information operates for the CSP user "N" that upload their data request "DT" to CSP database "DS" for an information "UD" and key value is passed as an argument to the algorithm to provide encryption for the data. This algorithm is work for three types of CSP i.e. Amazon, RackSpace and CloudSigma.

Algorithm for Uploading Data/ Information:

Input: *CSP user I; User password pwd; user trust key value k; select upload document DS; upload application Name DN; cloud type CT*

Output: *DS to be uploaded or rejected*

```
Begin:
Step1: validate login from CSP by providing valid user id "I" and password "pwd"
If validation succeeds {
    Show the new GUI page to upload CT data and go to step2
}
else {
Go to step 3;
}
Step 2:
If validation succeeds {
    1. CT selects the document "DS" need to be uploading.
    2. Provide appropriate and unique application name i.e. DN to the uploading file or data.
/*these name is referring by all CSB and CSP while satisfying the CSB request for downloading data.*/
    3. Random 5bit key is generated for encryption using
K< %=( int) (math. Random ( )*10000) formula.
/*generate random number of type integer in range 0 to N-1 where N is scaling factor*/
    4. On submit button upload the application on CT database and generate message.
}
else {
  Give error message if uploading failed
}
Step 3:
  Ask for valid user name and password.
 End
```

Second algorithm is for downloading information based on CSB request. This would be operational when a successful request DS reaches to CSP for a DN from CSP. Trust value of the user is validated based on User id "I" and password "pwd".

Algorithm for downloading Data/ Information:

```
Input: CSB login based on their CT, Cloud service Request DS
Output: Deliver information DS to the user I or reject request.
Begin Algorithm:
Step 1: client login with appropriate cloud type CT
If validation succeeds {
   1.  Go to step 2 or (Client requesting for data page visible
       to user)
}
else {
       Go to step 3.
}
Step 2:
   1.  Send a request of DS  to the CSP
   2.  If DS available with current CSP{
Send download link to CSB
}
          else {
                Send DS to another CSP via Proxy Server P;
                CSP updates the database for trusted CSB and check for the DS made by CSB
                Repeat step 2 until we check all CSP for DS
          }
Step 3:
  Ask for valid user name and password.
End
```

B. Flowchart

In this section, we introduce flow of system to upload and download the data from CSP's. Figure 2 shows flow authentication for CSB to get the required information from any cloud service providers.

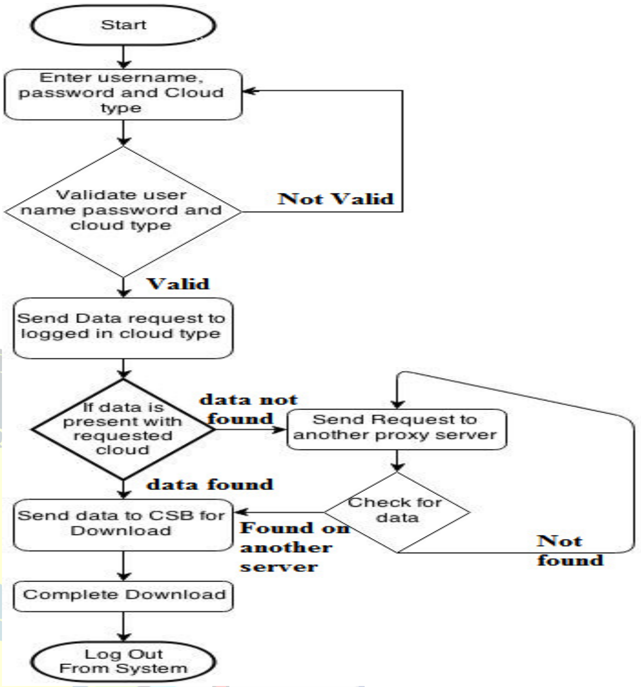

Start
Enter username, password and Cloud type
Validate user name password and cloud type
Not Valid
Valid
Send Data request to logged in cloud type
If data is present with requested cloud
data not found
Send Request to another proxy server
data found
Check for data
Send data to CSB for Download
Found on another server
Not found
Complete Download
Log Out From System

Figure 2: validation processes for CSB to get the required data from CSP.

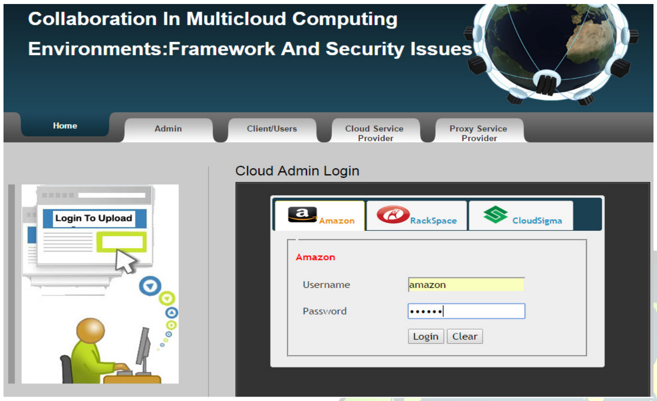
When any CSB who want to download data from CSP send any request to the CSP, CSB have to pass correct data like user id, password and required data. When request reaches to the CSP, It passes the request to trusted agent suited in the same domain to verify the CSB. If trust agent validates the CSB then CSP send the data to CSB with data required to CSB. If trust agent denied the verification then trust agent instantly informed to CSP and tell user to provide valid information.

C. Result

Collaboration allows CSB and cloud application to concurrently use the services from multiple CSP and route the information from multiple CSP. The framework support collective and dynamic collaboration between multiple CSP. CSB simultaneously utilize the services provided from multiple CSPs without any prior business agreement between multiple CSPs. The sub system of the multiple clouds and client using proxy framework is as follows:

1. Multiple Clouds/ Admin:

The multiple clouds may be created centrally under the SaaS (Software as a Service) category. Multiple clouds have a cluster of system which is organized through LAN. User can upload and download data after proper authentication is met. This is done by the administrator and hence user or CSB is allowed to get access his data or other user data. Figure 3 shows multiple cloud login window or cloud admin login window.



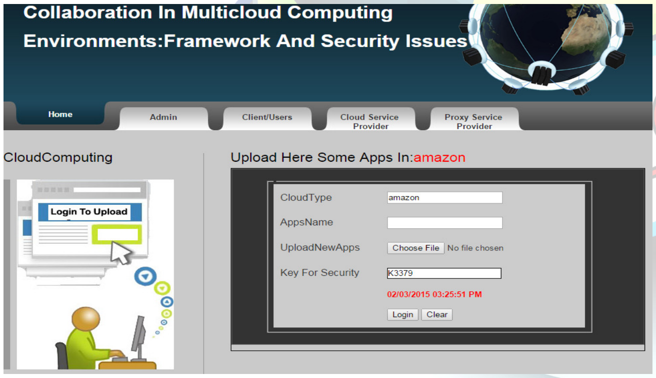
Cloud Admin Login

Amazon

Username: amazon
Password: ••••••

Figure 3: Cloud Admin Login Page for multiple CSP like Amazon, Rackspace and CloudSigma.

After proper authentication of Cloud Service Provider (CSP). CSP User can upload any using Encryption mechanism Advanced Encryption Standard (AES) and Random Key Generation (RKG) algorithm. Figure 4 shows the CSP user can upload data after validation and Figure 5 shows successful data upload message.

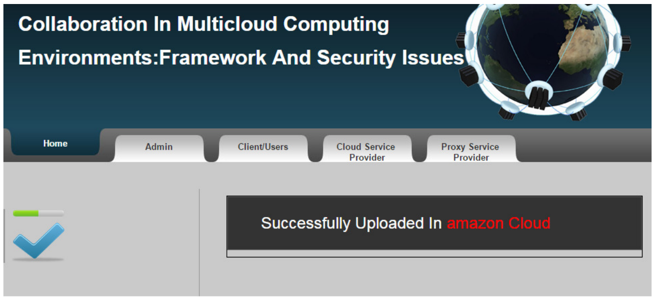


CloudComputing

Upload Here Some Apps In:amazon

CloudType: amazon
AppsName:
UploadNewApps: No file chosen
Key For Security: K3379
02/03/2015 03:25:51 PM

Figure 4: Upload data on specific CSP.

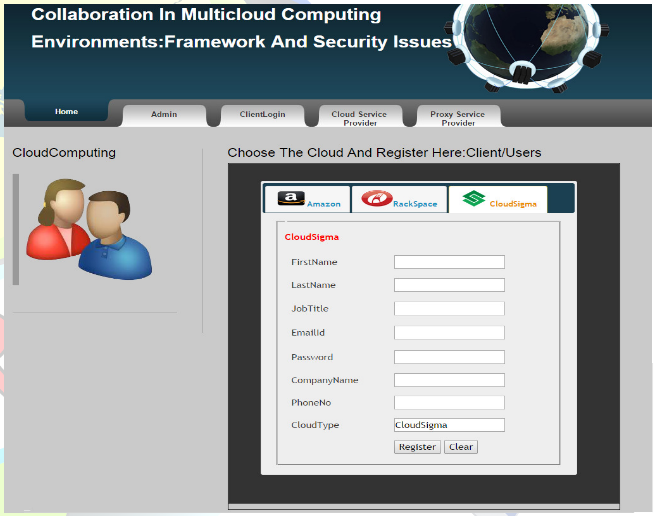

Collaboration In Multicloud Computing
Environments:Framework And Security Issues
Home
Admin
Client/Users
Cloud Service Provider
Proxy Service Provider

Successfully Uploaded In amazon Cloud

Figure 5: Data uploaded successfully.

2. Client/ User:

Cloud Service Buyers (CSB) is register with their respective Cloud Service Provider (CSP). Figure 6 shows Client registration for particular CSP and Figure 7 shows the client or user login page.



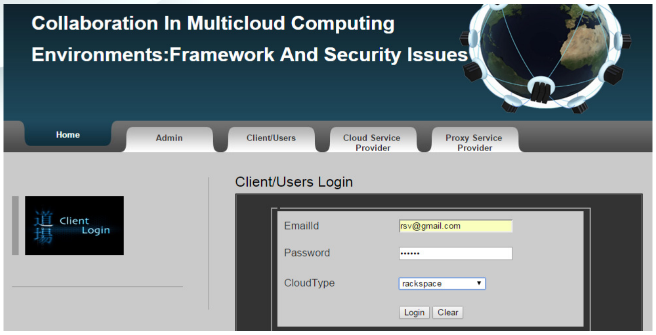
CloudComputing

Choose The Cloud And Register Here:Client/Users

CloudSigma

FirstName:
LastName:
JobTitle:
EmailId:
Password:
CompanyName:
PhoneNo:
CloudType: CloudSigma

Figure 6: Client Registration page for CSP



Client/Users Login

EmailId: rsv@gmail.com
Password: ••••••
CloudType: rackspace

Figure 7: Client login page for CSB

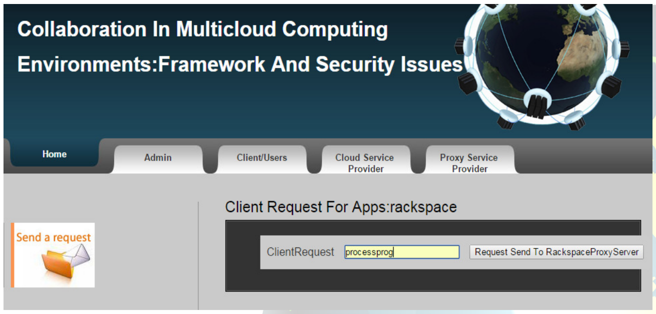
Framework Solution for CSB

2. A. Solution overview

The objective of our proposed solution is to provide Proxy mashup framework with Service Oriented Architecture (SOA) that enable CSP to securely integrate their information with other CSPs such that privacy of the data is preserved, while request coming from CSB is satisfied.

The framework for answering CSB consists following steps:

Step 1 – Send a request to CSP: Figure 8 shows CSB send a request with specification to the CSP.


Collaboration In Multicloud Computing
Environments:Framework And Security Issues
Home
Admin
Client/Users
Cloud Service Provider
Proxy Service Provider
Send a request
Request Send To RackspaceProxyServer

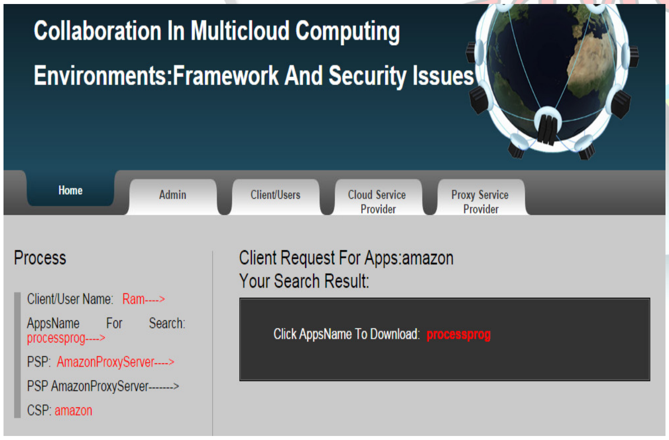
Client Request For Apps:rackspace

ClientRequest processprog

Figure 8: shows CSB send a request with specification to the CSP.

Step 2 – CSP Determine the data dynamically: CSP accept the client request and search desired information in self database. If required information is available then data send to the CSB. Here CSB can download required data.

Figure 9 shows CSP accept the client request and search desired information in self database.


Collaboration In Multicloud Computing
Environments:Framework And Security Issues
Home
Admin
Client/Users
Cloud Service Provider
Proxy Service Provider

Process

Client/User Name: Ram---->

AppsName For Search: processprog---->

PSP: AmazonProxyServer---->

PSP AmazonProxyServer------->

CSP: amazon

Client Request For Apps:amazon

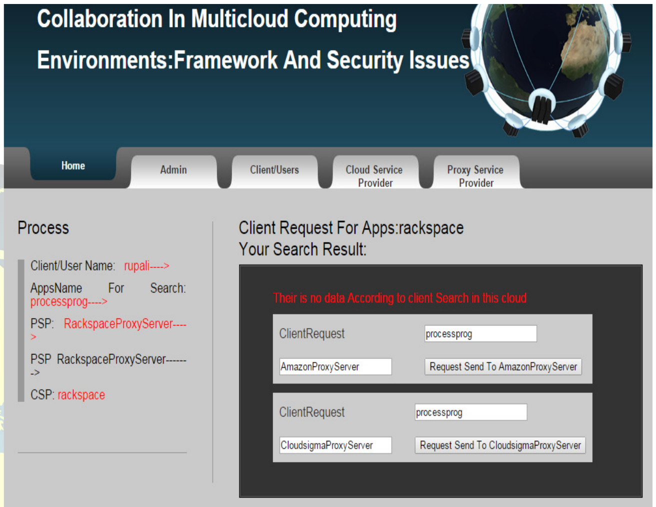
Your Search Result:

Click AppsName To Download: processprog

Figure 9: shows CSP accept the client request and search desired information in self database.

Otherwise CSP send client request to the Proxy Service Provider (PSP) and PSP dynamically discover the information from another CSP and send desired information to the requested CSP and CSP send this data back to client.

Figure 10 shows Otherwise CSP send client request to the Proxy Service Provider (PSP) and PSP dynamically discover the information from another CSP


Collaboration In Multicloud Computing
Environments:Framework And Security Issues
Home
Admin
Client/Users
Cloud Service Provider
Proxy Service Provider
Request Send To AmazonProxyServer
Request Send To CloudsigmaProxyServer

Process

Client/User Name: rupali---->

AppsName For Search: processprog---->

PSP: RackspaceProxyServer---->

PSP RackspaceProxyServer------->

CSP: rackspace

Client Request For Apps:rackspace

Your Search Result:

Their is no data According to client Search in this cloud

ClientRequest processprog

AmazonProxyServer

ClientRequest processprog

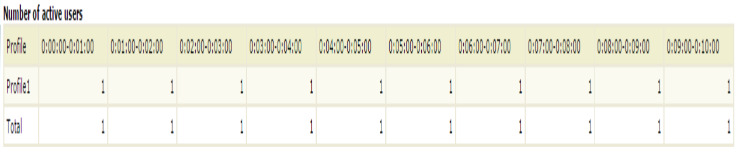
CloudsigmaProxyServer

Figure 10: shows Otherwise CSP send client request to the Proxy Service Provider (PSP) and PSP dynamically discover the information from another CSP

Step 3 – Check the desired information: After getting the response from CSP. CSB must check whether his/her request is fulfill or not.

V. Analysis Of System

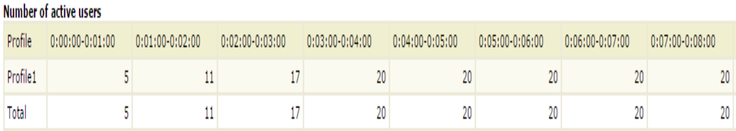
For proposed system proxy framework is used to share the data between multiple CSP's. For testing purpose we used WAPT tool, figure 11 and 12 shows the active users in proposed system.



Number of active users

Profile	0:00:00-0:01:00	0:01:00-0:02:00	0:02:00-0:03:00	0:03:00-0:04:00	0:04:00-0:05:00	0:05:00-0:06:00	0:06:00-0:07:00	0:07:00-0:08:00	0:08:00-0:09:00	0:09:00-0:10:00
Profile1	1	1	1	1	1	1	1	1	1	1
Total	1	1	1	1	1	1	1	1	1	1

Figure 11: Number of active user 1



Number of active users

Profile	0:00:00-0:01:00	0:01:00-0:02:00	0:02:00-0:03:00	0:03:00-0:04:00	0:04:00-0:05:00	0:05:00-0:06:00	0:06:00-0:07:00	0:07:00-0:08:00
Profile1	5	11	17	20	20	20	20	20
Total	5	11	17	20	20	20	20	20

Figure 12: Number of active users is more than 1

Figure 13 shows the overall performance of the system. X axis used for time and Y axis is used to represent number of active users.

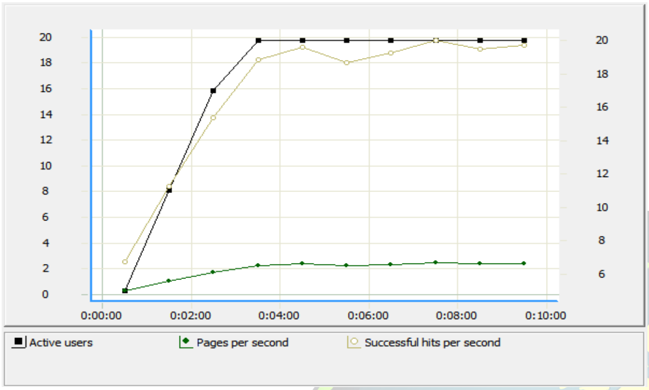


Figure 13: Overall Performance of the system

V.I Comparison with existing system

In this section we introduce comparison between existing system and our proposed solution. Table 1 shows the comparison between existing and proposed solution.

Table 1: Difference between existing and new proposed model.

Sr .no	Parameter	Existing	Proposed
1	Focus on Cloud Service	PaaS	SaaS and DaaS
2	Preestablished Agreement between multiple cloud providers.	Required	Not Required
3	Extra Charges for each service providers	Required	Not Required
4	Use of Proxy Framework	No	Yes
5	Services type	Web	Web and Non web application

VI. Conclusion

This paper review all the techniques related to the multiple cloud collaboration environments. This new proposed framework allows multiple clients or CSB to use services for low prices as compared to the single cloud environment. Major advantage of this framework is that non pre-established agreement between the multiple CSP for collaborating their services. Finally consumer gets their services without paying extra charges to each service providers.

References

[1]. Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg and Ivona Brandic, “Cloud Computing and emerging IT platforms: Vision, hype and reality for delivering computing as the 5th utility,” Journal of Future Generation computer Systems, Vol.25, no. 6, pp.599-616, June 2009.

[2]. Mohamed Firdhous, Osman Ghazali and Suaidi Hassan, “Trust Management in cloud computing; A Critical Revew,” International Journalon Advance in ICT for EmergingRegions 2011 04 (02): 24-36.

[3]. J. Carolan, S. Gaede, J. Baty, G. Brunette, A. Licht, J. Remmell, L. Tucker, J. Weise, “Introduction to cloud computing architecture”, whitepaper 2009.

[4]. Mukesh Singhal and Santosh Chandrasekar, Tingjian Ge, Ravi Sandhu and Ram Krishnan, Gali-Joon Ahn, and Elisa Bertino, “Collaboration in multicloud environments: Framework and Security Issues”, published by IEEE computer Society IEEE, 2013.

[5]. Zacharias Enslin, “Introduction to cloud computing and control objectives for information and related technologies (COBIT) – mapped benefits of cloud computing adoption”, AJBM Vol.6 (41), pp. 10568-10577, Oct 2012. Available at http://academicjournals.org/AJBM

[6]. Saranya Eswaram and Dr. Sunitha Abburu, “Identifying the data integrity in cloud storage”, IJCSI International journal of computer science ISSUES, Vol. 9, Issue 2, No 1, March 2012.

[7]. S. Subashini, V. Kavitha, “A survey on security issues in service delivery model of cloud computing”, Elsevier Ltd, journal of Network and Computer Application, 11th July 2010.

[8]. http://thoughtsoncloud.com/2014/02/what-is-infrastructure-as-a-service-iaas/

[9]. Prodan R, Ostermann S, “A survey and taxonomy of infrastructure as a service and web hosting cloud providers”, Grid computing, 2009 10th IEEE/ACM International Conference on, pp. 17, 25, 13-15 Oct 2009.

[10]. jeff sedayao, steven su, Xiaoao Ma, Minghao Jiang and Kai Miao, “A Simple Technique for securing data at rest stored in a computing cloud”, proc. Of CloudCom 2009, Springer-Verlag Berlin Heodelberg 2009, LNCS 5931, pp. 553-558, 2009.