ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Secured Proxy Based Collaboration in Multi Cloud

Maitshaphrang Lyngdoh Mawnai[1], A.Selvakumar[2]

P.G. Student, Department of Computer Science Engineering, S.R.M. University, Kattankulathur, Chennai, India[1]

Associate Professor, Department of Computer Science Engineering, S.R.M. University, Kattankulathur, Chennai, India[2]

ABSTRACT: Cloud Computing has emerged as a popular delivery of computing services over the internet. Having the superior power and influence, the cloud computing providers faces the problem of scalability. The need of individual interaction among each cloud service provider to process the collective data has become necessary. Besides computing, service providers will have to collaborate to improve resource utilization and provide solutions to the customers. Cloud mashups offers sophisticated services and need pre-established agreements among providers. In this paper, collaboration framework in cloud computing environment is based on cloud proxies. This allows sharing of the cloud based resources services and dynamic collaboration. The policy trust and privacy issues are provided without pre-established collaboration agreements or standardized interfaces.

KEYWORDS*:* cloud computing, cloud collaboration, cloud mashups, cloud proxies, cloud security.

I. INTRODUCTION

The term “cloud” is often used over the internet metaphorically. It refers to “computing on the internet” [1]. Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In another words, Cloud computing is the delivery of computing services over the internet.

Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Online file storage, social networking sites, webmail and online business applications are some of the examples of cloud services [3]. Cloud computing models allows the individual to access the information and computer resources from anywhere when network connection is available.

Moving the information into the cloud makes the clients easy to access and retrieve without knowing the complexities of administration. The client who get access to the cloud administration pick up all these administrations and gets lock-in to utilize the specific cloud. If clients need to access an alternate cloud administration supplier, the client need to validate to a specific administration and utilize multi-administration supplier on unique premise. Thus, the cooperation of multi-cloud plays a role where the client merchant lock-in can be deprived with an assertion between the different cloud providers that an approved client of specific cloud administration supplier can get access to distinctive administration supplier at his expense.

Many organizations employs cloud computing and different service providers are used for developing new trends to enhance the capabilities in clouds. Cloud mashups have a distributed application structure which merge the different services from multiclouds into a single service which is possible in client side data and service. IBM’s MashupCenter, Appirio Cloud Storage and Force.com for the Google App Engine are some of the examples of the Cloud Mashups. But cloud mashups require pre-written agreements among the providers and also need a tightly integration techniques [2].

The research community is beginning to develop architectures, technologies, and standards to support collaboration among multiple cloud systems. However, these research proposals still remain constraining due to their provider-centric approach or limited scope. Provider-centric approaches require CSPs to adopt and implement the standardized interfaces, protocols, formats, and other specifications, as well as new architectural and infrastructure components to facilitate collaboration, such that without these provider-centric changes, current proposals do not provide facilities for client-centric, on-the-fly, and opportunistic combinations of heterogeneous cloud-based services. While cloud

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

standardization will promote collaboration, there are several hurdles to its adoption. For cloud collaboration to be alive, it is needed to developed mechanisms allowing opportunistic collaboration among services without requiring standards and extensive changes to the cloud service delivery model [4].

II. RELATED WORK

This is a survey paper based on the work done by the researchers in the present era of cloud computing environment. This technique makes it possible to transfer from single cloud architecture to multi cloud architectures and provide a solution to the different security issues for cloud optimization. It gives the user the freedom of choosing the cloud based on the user's 'requirements.

The data usage from different vendors, synchronization among clouds providers and free vendor lock-in system are provided in multi cloud computing. Multi cloud computing needs to work in a distributed environment and services from different cloud providers have to collaborate which makes it more difficult. To overcome this, researchers proposed a proxy based framework for the collaboration in multi cloud.

In this framework, proxies are used at different levels of cloud collaboration. These proxies are set by the organizations and made by the cloud service providers to get access. The communication between the clients and service providers are made secured through proxies.

The proxies provide a trusted computing platform to prevent malicious software from attacking the cloud applications. This can protect the data at rest and data in transit in cloud computing issues.

The three categories of cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Keeping in mind of the stated services, the cloud service providers must be able to provide on a distributed environment of multicloud.

This paper is based on the survey of the techniques which are needed for transferring a single cloud architecture to multi cloud architecture. Considering the cost effectiveness on the client side, a new framework including the issues are included in this paper.

III. PROPOSED METHOD AND TECHNIQUES

The proposed method is based on a proxy cloud, which is an edge node hosted software instance that a client or CSP can delegate to carry out the operations on its behalf. The framework allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. A network of proxies consisting of many number of edge nodes are used to increase the performance and reliability of distributed applications. For the interaction with multiple cloud, a proxy may route data to another proxy as a part of an application workflow. Depending on the situation, the system can employ a network of proxies as a collection of virtual software instances logically connected through a virtual network or underlying nodes.

The architecture model of the proposed framework are categorised into the following:

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

1. **Cloud hosted proxy:** As figure 1 shows, each CSP can host proxies within its cloud infrastructure, manage all proxies within the domain and handle the requests from clients that wish to use those proxies for collaboration. The proxy instances might need to be CSP specific [2]. For example, in Figure 1, both C1 and C2 might mutually and dynamically provision sharing and collaboration logic as proxy virtual instances within their respective administrative domains. In this case client sends a request to C1, which dynamically detects the need to use services from other clouds C2 and C3. The proxies will be employed by C1 to administer these interactions.

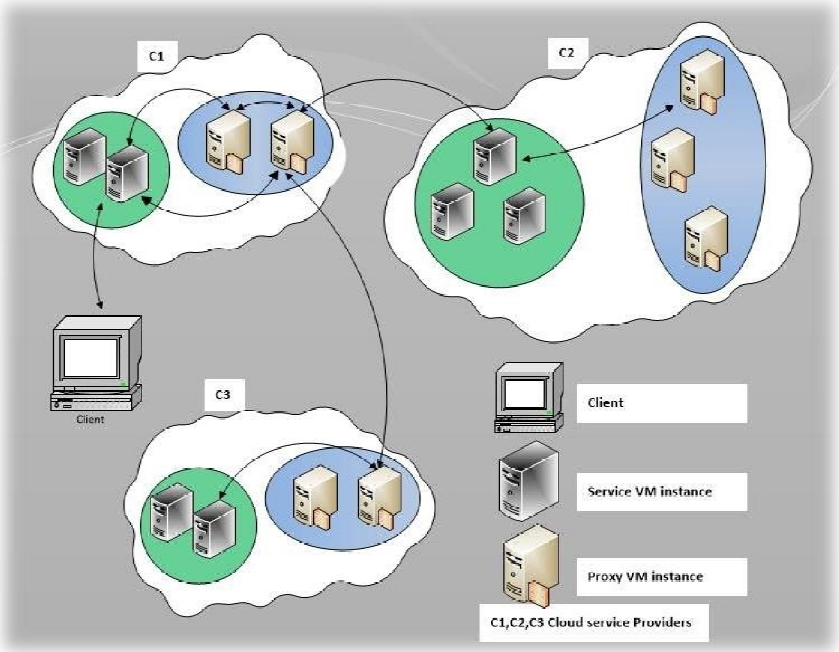


Fig: 1 Client sends a request to cloud C1, which dynamically discovers the needs to use services from clouds C2 and C3.C1 employs proxies to manage these interactions

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

2. **Proxy as a service:** This case involves using proxies as an autonomous cloud that provides collaborative services to cloud service providers as well as clients ;as shown in figure 2 [2]. A group of CSPs that are ready to collaborate can administer this proxy-as-a-service cloud, or a proxy service provider (PSP), can provide administration. Clients directly interact with proxy cloud service and employ them for inter-cloud collaboration. In this case, Proxy as a service, CSPs set up proxies as an autonomous cloud system and offers it as a service to client.

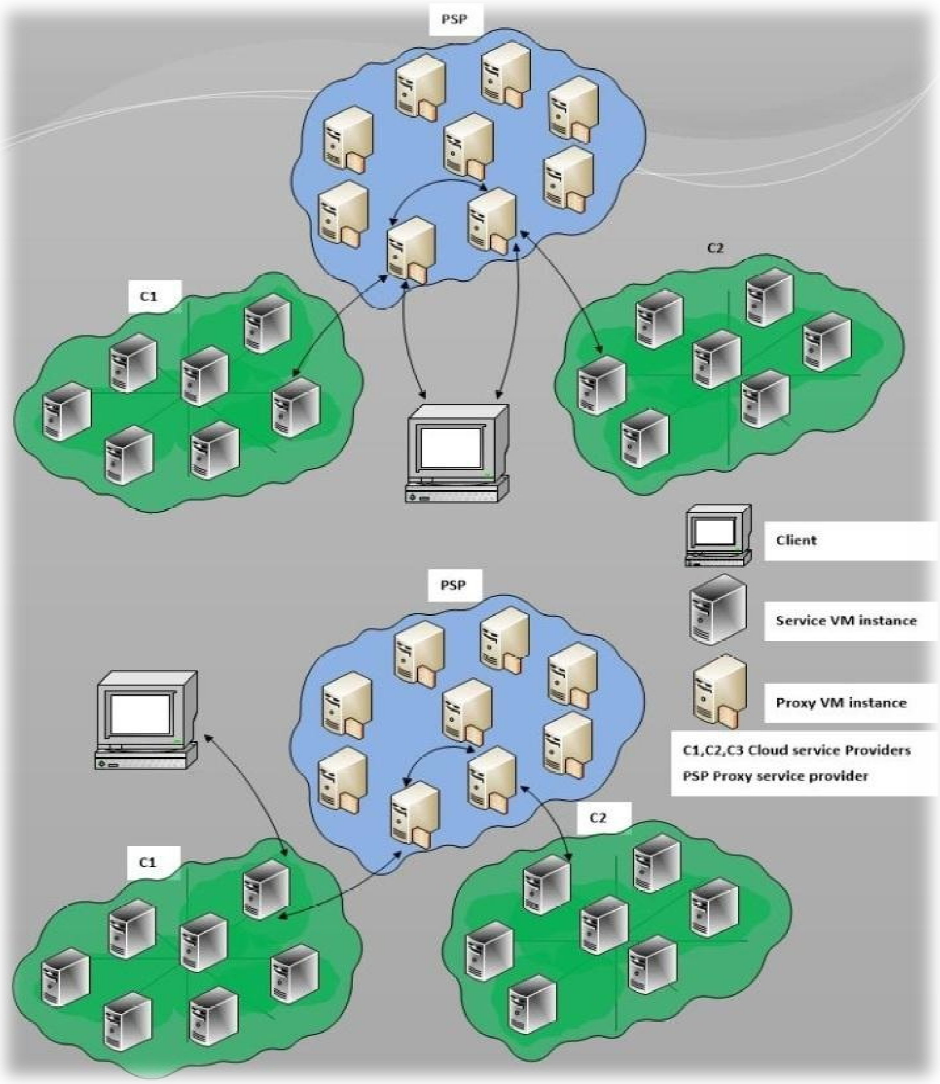


Fig: 2 Proxy as a service. In this scenario, cloud service providers (CSPs) deploy proxies as an Autonomous cloud system and offer it as a service to clients. (a) A client employs two proxies to Interact with CSPs C1 and C2. (b) Alternatively, a client initiates a service request with C1, which then discovers the need for a service from C2.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

3. **Peer to Peer Proxy:**Proxies can also interact in a peer-to-peer network managed by either a PSP or a group of CSPs that wish to collaborate. Another possibility is for proxies to have no collective management: each proxy in the peer-to-peer network is an independent entity that manages itself [3].In this case, the proxy itself must handle requests to use the services. As shown in figure 3, Proxies are deployed within the infrastructure of client's organization.

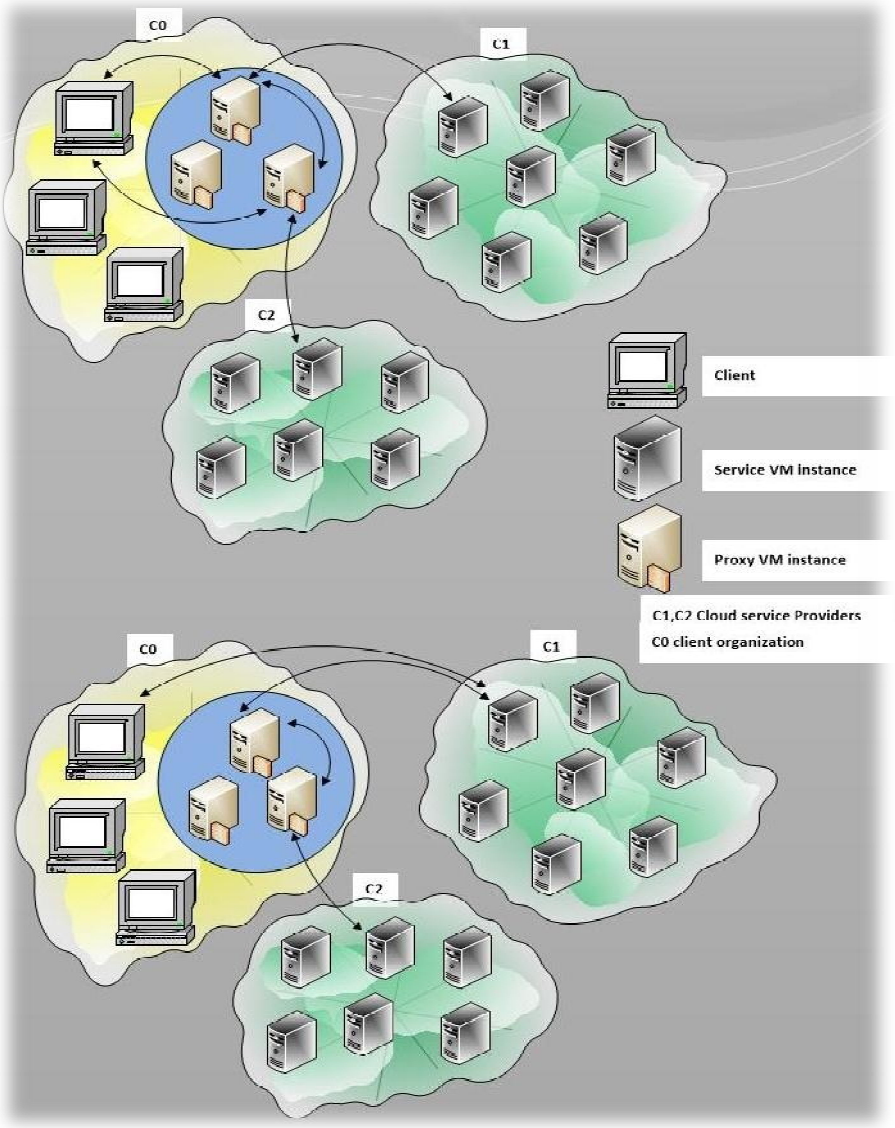


Fig: (a) A client employs two proxies to collaborate with CPS"s C1 and C2 (b) A client starts requesting services with cloud C1, which then detects the need for a service from C2.

4. **On premise Proxy:** A client that wishes to use proxies for collaboration will employ its on-premises proxies, whereas CSPs that wish to collaborate with other CSPs must employ proxies that are within the domain of the

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

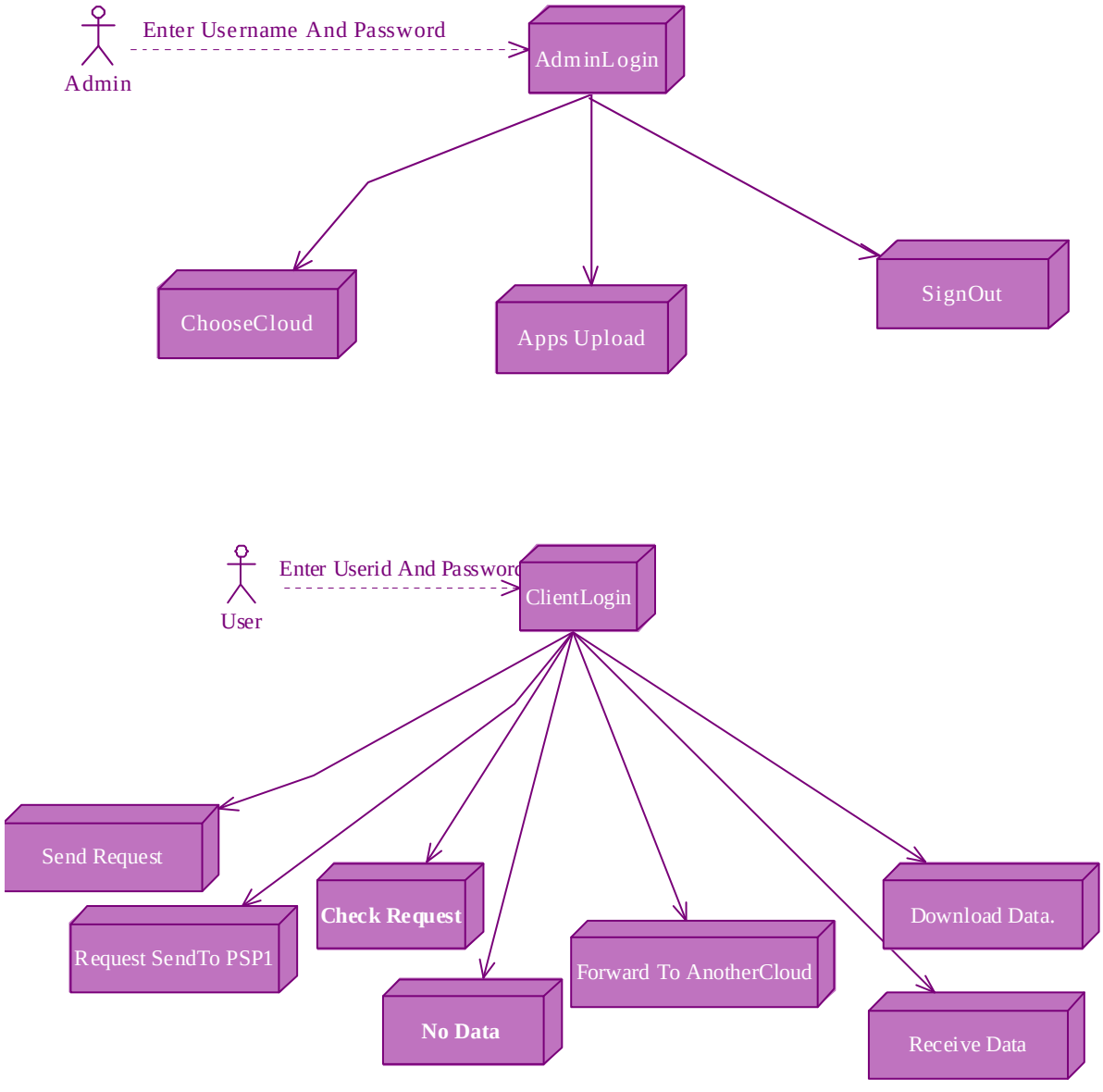
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

service-requesting client. In the scenario shown in Figure3, a client can host proxies within its organization's infrastructure (or on premises) and manage all proxies within its administrative domain [2].

5. **Hybrid Proxy:** A hybrid infrastructure can include on-premises, CSP- and PSP-maintained, and peer to- peer proxies. Selecting proxies for collaboration will depend on the type of service being requested and the entity that initiates collaboration, among other factors.

The Component diagram of the proposed framework is shown as follows:



ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

IV. SECURITY

Having all the critical information being shared with different cloud providers, the level of security has to be maintained. The cloud service providers and clients must establish trust relations and this can be done by using proxies [4]. The trust relations also guarantee the business continuity and management of the different cloud providers. In this framework, Proxies are established on the client side as well as on the cloud provider side. The control over the proxies and assets are always in the cloud service provider's administration. Transport Layer Protocol is used to provide confidentiality for transmitted data in proxy networks. The public key infrastructure provides secure access and Warrant-based proxy signature for delegation signing rights to provide authentication to the proxies. Proxies analyse the relationship between policies to resolve the anomalies and made easy to adapt and handle the evaluated policies as a whole [5-10].

For keeping Identity attributes and data privacy in shared computing environments like clouds, protecting the privacy of client assets is critical. The privacy issues pertaining to both data and identity. Privacy protection methods (other than encryption) fall broadly into two categories [6], i.e., Data perturbation (also known as input perturbation), which adds some form of noise to the data itself, and Output perturbation, which adds noise to the otherwise accurate query answers.

V. EXPERIMENTAL RESULT

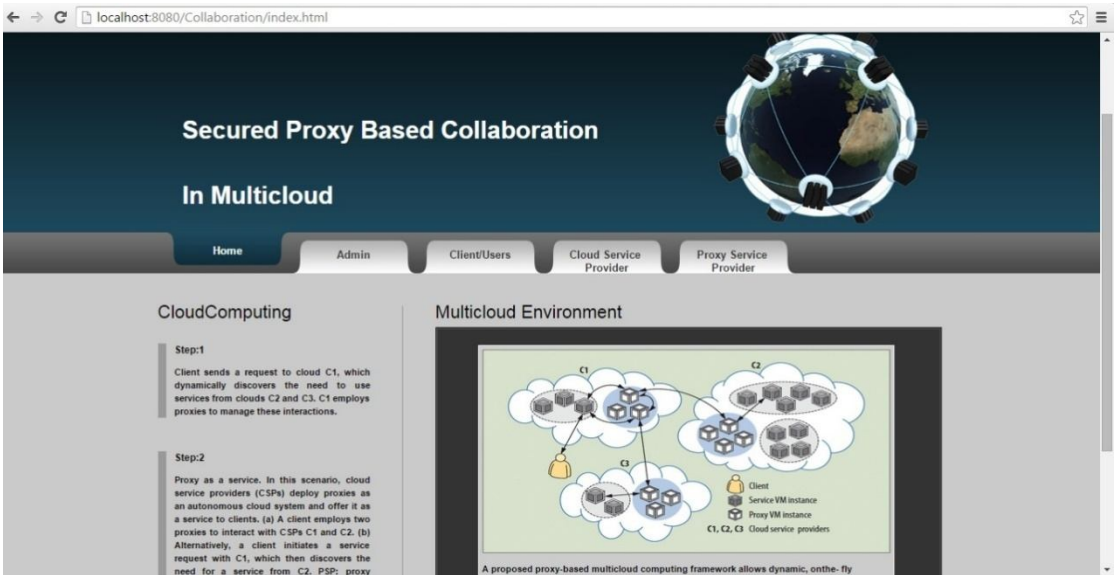


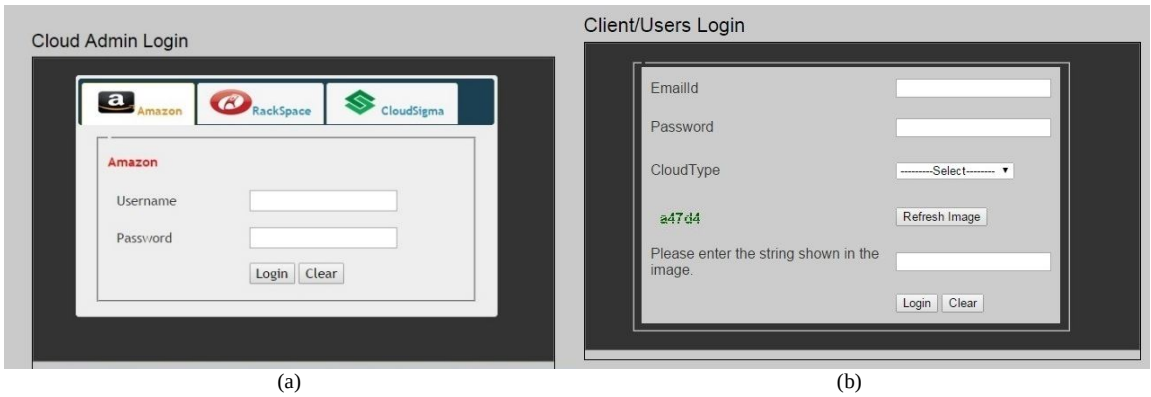
Fig: 7 Collaboration Framework consisting of Admin, Client, Cloud Service Providers and Proxy Service Provider. This is the basic workspace where all the collaboration work is done.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015



(a) (b)

Fig: 8 (a) Cloud Admin Login consisting of three Cloud Providers viz. Amazon, Rack space, Cloud sigma. The admin can login and upload application in the database (b) Client can login into the cloud to access the application as needed. Applications are access based on proxies.

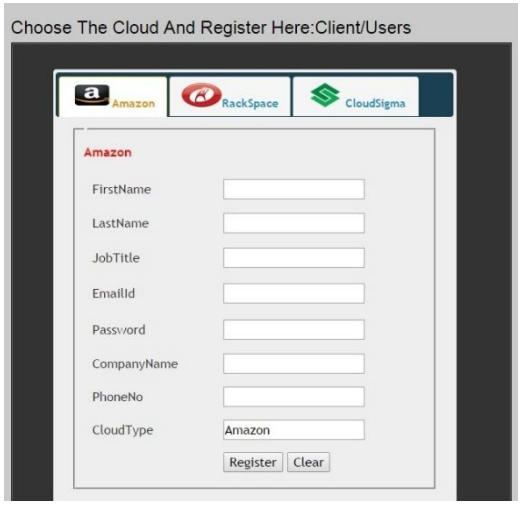


Fig: 9 A client can register in any of the created cloud service providers. A client need to enter the information as required by the cloud providers. When the client are registered, they can access the applications on the cloud and these are managed by proxy service providers.

VI. CONCLUSION

The 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. Future research directions for the proposed framework include refining the proxy deployment scenarios and development of infrastructural and operational components of a multicloud system. This must be accompanied by implementation of an experimental platform using open source tools and libraries that work in combination with real-world cloud services to evaluate the system's functionality and limitations, and make further refinements.

VII. REFERENCES

[1] Cary Landis and Dan Blacharski, "Cloud Computing made easy",Virtual Global Inc.
[2] M. Singhal and S. Chandrasekhar, T. Ge, R.Sandh and R. Krishnan, G. Ahn E. Bertino, "Collaboration in Multicloud Computing Environments: Framework and Security Issues", Published by IEEE Computer Society , Feb. 2013
[3] P. Mell and T. Grance, "The NIST Definition of Cloud Computing",Special publication 800-145, National Inst. Standards and Technology, 2011, p. iii + 3.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

[4] P. Mell and T. Grance, "Perspectives on Cloud Computing and Standards, NIST Information Technology Laboratory", National Inst. Standards and Technology, 2008; http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloudcomputing-standards_ISPAB-Dec2008_P-Mell.pdf.
[5] R. Thandeeswaran, S. Subhashini, N. Jeyanthi1, M. A. SaleemDurai, "Secured Multi-Cloud Virtual Infrastructure with Improved Performance", Cybernetics and Information Technologies, Volume 12, No 2 Sofia, 2012
[6] Jon Weissman "Using proxies to accelerate cloud applications", Proceeding HotCloud'09 Proceedings of the 2009 conference on Hot topics in cloud computing ,Article No. 20
[7] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", special publication 800-144, Nat"l Inst. Standards and Technology, 2011, p. x + 70.
[8] C.M. Ellison et al, "SPKI Certificate Theory", IETF RFC 2693, Sept. 1999; www.ietf.org/rfc/rfc2693.txt.
[9] N.R. Adam and J.C. Wortmann, "Security-Control Methods for Statistical Databases: A Comparative S16", ACM Trans. Internet Technology, Aug. 2007
[10] L. Xiong, S. Chitti, and L. Liu, "Preserving Data Privacy in Outsourcing Data Aggregation Services," ACM Trans. Internet Technology, Aug. 2007, p. 17

BIOGRAPHY

Maitshaphrang Lyngdoh Mawnai is pursuing M.Tech Final Semester, Department of Computer Science Engineering from S.R.M. UNIVERSITY, KATTANKULATHUR, CHENNAI - 603203

Mr. A. Selvakumar is working as an Asst. Professor in The Department of Computer Science Engineering, S.R.M. UNIVERSITY, KATTANKULATHUR, CHENNAI - 603203. His areas of interest includes Computer Networks, Cloud Computing and Information Security.