International Journal of Research

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, June 2015
Available at http://internationaljournalofresearch.org

Usage of Proxy Based Framework in Cloud Computing Environment

Kadurla Srikanth Chary[1]& P.Lakshmi Deepthi[2]

[1]PG Scholar ,Dept of CSE, MLR institute of Technology, Hyderabad, Telangana
[2]ASSISTANT PROFESSOR, Dept of CSE, MLR institute of Technology, Hyderabad, Telangana

ABSTRACT

Cloud computing is the product of the synthesis of traditional computing technology and network technology like parallel computing, distributed computing. The main goal of cloud computing is to construct a perfect system with powerful computing capability through a large number of relatively low cost computing entity using the advanced business models like SaaS, PaaS, IaaS to distribute the powerful computing capability to end users. A proposed proxy-based multi cloud framework using Cloud Proxies allows dynamic collaborations without pre established collaboration agreements or standardized interfaces. The recent surge in cloud computing arises from its capability to provide software, infrastructure, and platform assistance without requiring large investments or outlay to manage and operate them. Clouds typically require service providers, infrastructure/resource providers, and service users (or clients). They incorporate applications delivered as services, as well as the hardware and software systems presuming these services.

Keywords—cloud computing; Cloud Proxies; infrastructure; platform assistance

I. INTRODUCTION

Cloud computing has become a necessity today when the company plans to increase capacity "or capabilities on the fly without getting to invest new infrastructure, training new individual purchase new license application, etc. based service encompasses any subscription or pay per use which extends the existing IT capabilities of the company, current time through Online.

Cloud computing brings a new development in the field of Information Technology that gives a model where a user who wants to gain access to the software without licensing it, and need a platform to run this software and the infrastructure can access these services on pay-per-use basis [1]. It also provides a large amount of data storage to the user who can utilize it and moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. We have approaches that encourage the owner to store the data, it offer some sort of guarantee related to the reliability, privacy and access control of the outsourced data. The u ser 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. By individual basis and pay separately for the service to each provider. Proposed scenario of multi-cloud presents a model called collaboration of multi-cloud where the user vendor lock-in can be abolished with an agreement between the various cloud service provider that an authorized user of a particular cloud service provider can gain access to different service provider as per his requirement and cost management [6]. Cloud mash ups want pre-established agreements among providers as well as the use of custom built, proprietary tools that combine services through low-level, tightly controlled and constraining integration techniques.

This approach to building new collaborative services does not support agility, flexibility, and openness. Realizing multi-cloud collaboration's full potential will require implicit, transparent, universal, and on-the-fly interaction involving different services reach across multiple clouds that lack pre established agreements and proprietary collaboration tools. While cloud standardization will support collaboration, there are number of hurdles to its adoption. From a market perspective, it is doubtful that multiple CSPs will agree on an easy and standardized way to access services, as this would give clients total freedom in changing providers, leading to increased open and direct competition with other providers. Cloud-based computing also introduces new security concerns that affect collaboration across multi cloud applications they are, increase in the attack surface due to system complexity, loss of client's control over resources and migration, threats that target exposed interfaces due to data storage in public domains, and data privacy concerns due to multi-tenancy. So there is need of developing multi cloud system which provides trust, security and safety for applications and data [12]. Keeping all these drawbacks my work is to develop a generic cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. There are restrictions in the current cloud computing model prevent direct collaboration among applications hosted by different clouds. Data due to asset migration, threats that target exposed interfaces due to data storage in public domains, and data privacy concerns due to multi-tenancy. So there is need of developing multi cloud system which provides trust, security and safety for applications and data. Keeping all these drawbacks my work is to develop a generic cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds [6]. There are restrictions in the current cloud computing model prevent direct collaboration among applications hosted by different clouds.

A proposed proxy-based multi-cloud framework using Cloud Proxies allows dynamic collaborations without preestablished collaboration agreements or standardized interfaces.

II. RELATED WORK

Multi-Cloud computing has many advantages such as it provides usage of data from various clouds, the ability of choice for the user, stops vendor lock-in and synchronization between different cloud service providers with cost optimization. The main issue in implementing multi-cloud is its working in a distributed environment as the services are to be collaborated with different cloud service providers to make it possible a framework is laid in the research work of “Collaboration Framework for Multi-cloud Systems” which specify the use of proxies at different level of collaboration. These proxies can be implemented by the cloud service provider or can be set by the institutions\organization so as to gain service from collaborated service providers [7]. These proxies can also be used to have a secure communication between the client and the service provider. 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. This also deals with the security aspect of the cloud computing. The cloud services have been classified as software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a Service (IaaS) it becomes important that the cloud service providers must be able to provide these services on distributed environment of multi-cloud for that purpose research work of “A

Federated Multi-Cloud PaaS Infrastructure" can be effective as it provides a platform for various services to be provides in a collaborated paradigm. It is also important that the cost effectiveness of multi-cloud must be considered before shifting towards a new paradigm to solve this issue research work of "Cloud Brokering Algorithm" has given an algorithm based on the Virtual infrastructure in cloud environment which will effectively determine the allocation of VM both on static and dynamic basis [8]. This paper is based on review of the technique that will proof to be efficient while shifting towards the multi-cloud environment.

In the proposed system cloud collaboration is achieved by prior business agreements among the cloud providers and this limits the security to the individual cloud. Moreover our proposed cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. This framework supports universal and dynamic collaboration in a multi-cloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications [12]. This provides security to the data by providing access control to the clients.

Cloud computing is a new design example for large, distributed datacenters [2]. In cloud computing users can store their data using cloud infrastructure and even they can access the applications like email, search, and social networks, Service providers offer these all services . Newly authors have increased offering services to users like, compute related capabilities such as virtual machines, storage, and complete operating system services. The cloud computing design yields breakthroughs in geographical distribution, resource utilization efficiency, and infrastructure mechanization. We have public clouds and private clouds. These public clouds have been used by IT vendors for corporations to construct "private clouds" of their own. The concept or model called "pay as you go" is used to compute resources usage by end users [8]. Public and private clouds use this model as well like the electricity system, telephone and internet systems. However, so far clouds cannot be interoperating. Such federation or interoperating is called the Inter-cloud. Building the Inter-cloud needs more knowledge of their platform because of their different providers. It is important to prepare inter-cloud economy with a technically strong foundation and topology. In general this paper deals with the security considerations of the inter-cloud.

Cloud computing offers a prominent service for data storage known as cloud storage. The flow and storage of data on the cloud environment in plain text format may be main security threat. So, it is the responsibility of cloud service providers to ensure privacy and security of data on storage as well as network level. The following three parameters confidentiality, integrity and availability decide whether security and privacy of data stored on cloud environment is maintained or not [10]. Cloud computing is a distributed computing style which offer integration of web services and data centers. There are several major cloud computing providers including Amazon, Google, Yahoo, Microsoft and others that are providing cloud computing services [4].

The idea of making use of multiple clouds has been proposed by Bernstein and Celesti. However, this previous work did not focus on security. Since then, other approaches considering the security effects have been proposed. These approaches are operating on different cloud service levels, are partly combined with cryptographic methods, and targeting different usage scenarios.

III. PROPOSED SCHEME

A proposed proxy based multi cloud computing framework enable dynamic, on the fly collaborations and resource sharing among cloud depended services, addressing trust, policy, and privacy issues without pre established collaboration agreements or assimilate interfaces.

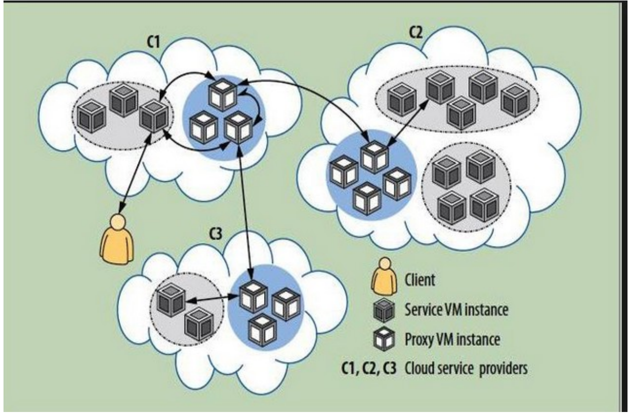

Fig: Proxy based frame work architecture

It include the use of proxy in multi cloud environment in various forms these are

Cloud-Hosted Proxy:

In this framework the cloud service provider host proxies within its infrastructure administer and manage the proxies and will handle the service request from the client who wants to access these proxies.

Proxy as a Service:

Here the proxy is been deployed as an individual cloud. Multiple cloud service providers with collaboration can manage this proxy or a third party proxy service provider can manage it for the cloud service providers.

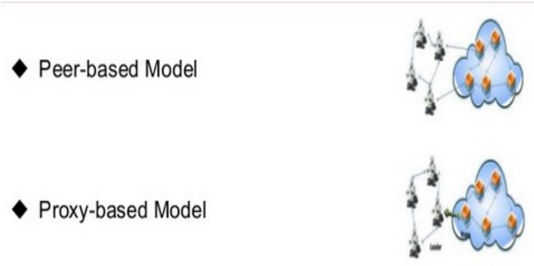

Fig: Proxy and Peer based models

Peer-To-Peer Proxy:

Proxy can also be communicated on peer-to-peer network which is managed by the proxy service provider or cloud service provider those who have an agreement of collaboration.

On-Premise Proxy:

The client himself can host proxies within infrastructural domain and manage it in administrative domain. The person who wishes to use proxies will have to deploy it on premise proxies and the service providers that wish to collaborate with other service provider will have to implement it within the service requesting client domain.

Advantages:

Partition of application System into tiers allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic.

Partition of application logic into fragments allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality. Partition of application data into fragments allows distributing fine -grained fragments of the data to distinct clouds. None of the involved cloud providers gains access to all the data, which safeguards the data’s confidentiality

IV. CONCLUSION

To facilitate dynamic collaboration between clouds, we proposed a framework that uses proxies to act as mediators between applications in multiple clouds that must share data. Our proposed framework has the potential to overcome several restrictions in the current cloud computing model that can prevent system’s functionality and limitations, and make further refinements. Currently, our research team is working toward a single viable proxy deployment strategy based on use cases, trust, and security requirements. We are also developing specifications to instantiate, deploy, maintain, and release proxy virtual machines reliably and securely, along with a suite of proxy services to support various collaboration use cases. Our incremental approach to the development of proxy services for collaboration initially provides support for simple use cases, later progressing to more complex use cases.

REFERENCES

[1] R. Buyya et al., “Market-Oriented Cloud Computing: Vision, Hype, and Reality of Delivering Computing as the 5th Utility,” Proc. 9th IEEE/ACM Int’l Symp. Cluster Computing andthe Grid (CCGRID 09), IEEE CS, 2009, pp. 599-616.

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

[3] S. Ortiz Jr., “The Problem with Cloud Computing Standardization,” Computer, July 2011, pp. 13-16.

[4] J. Jin et al., “Patient-Centric Authorization Framework for Electronic Healthcare Services,” Computers & Security, Mar.-May 2011, pp. 116-127.

[5] 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.

[6] Collaboration Chandrasekhar S and Singhal M *Collaboration in Multicloud Computing Environments: Framework and Security Issues,* IEEE Transactions on Cloud Computing Vol.46 No.2 Year 2013.

[7] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, special publication 800-145, National Inst. Standards and Technology, 2011, p. iii+3 .

[8] R Buyya et al., *Market-Oriented Cloud Computing: Vision, Hype, and Reality of Delivering Computing as the 5thUtility* Proc. 9th IEEE/ACMInt’l Symp, *Cluster Computing and the Grid (CCGRID 09)*, IEEE CS 2009, pp. 599-616.

[9] M.P. Papazogulu and W. Vanden Heuvel, *Blueprinting the Cloud*, IEEE Internet Computing, No 2011, pp. 74-79. [10] S. Chandrasekhar et al., *Efficient Proxy Signatures Based on Trapdoor Hash Functions IET Information Security,* Dec. 2010, pp. 322-332.

[11] N.R. Adam and J.C. Wortmann, *Security-Control Methods for Statistical Databases: A Comparative Study*, ACM Computing Surveys, Mar. 1089, pp. 515-556.

[12] L. Xiong S. Chitti and L.Liu, *Preserving Data Privacy in Outsourcing Data Aggregations Services* ACM Trans. Internet Technology, Aug. 2007, p. 17.

[13] E. Hammer-Lahav, ed., *The OAuth 1.0 Protocol*, IETF RFC 5849, Apr. 2010; http://tools.ietf.org/html/rfc5849.

Author’s Profile:

KADURLA SRIKANTH CHARY,
PG SCHOLAR

Department of CSE,
MLR INSTITUTE OF TECHNOLOGY,
Hyderabad, Telangana

P.LAKSHMI DEEPTHI,
ASSISTANT PROFESSOR,
Department of CSE,
MLR INSTITUTE OF TECHNOLOGY,
Hyderabad, Telangana