Volume: 6 Issue: 3 Pages: 2338-2341 (2014) ISSN : 0975-0290

A Framework for Multicloud Environment Services

Dr. C S. Pillai
Associate .Professor & HOD,ACS College OF Engineering, Bangalore.
Email : Pillai.cs5@gmail.com

ABSTRACT

The recent surge in cloud computing arises from its ability to provide software, infrastructure, and platform services without requiring large investments or expenses to manage and operate them. Clouds typically involve service providers, Infrastructure / resource providers, and service users (or clients). They include applications delivered as services, as well as the hardware and software systems providing these services. Our proposed framework for generic 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 multicloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among (CSP) cloud service providers, and without adopting common standards and specifications.

KEYWORDS: cloud clients, cloud service provider, applications delivered as services.

Date of Submission: October 18, 2014 Date of Acceptance: December 01, 2014

1. INTRODUCTION

Cloud computing characteristics include a ubiquitous (network-based) access channel; resource pooling; multitenancy, automatic and elastic provisioning and release of computing capabilities; and metering of resource usage (typically on a pay-per-use basis).

Virtualization of resources such as processors, network, memory, and storage ensures scalability and high availability of computing capabilities. Clouds can dynamically provision these virtual resources to hosted applications or to clients that use them to develop their own applications or to store data. Rapid provisioning and dynamic reconfiguration of resources help cope with variable demand and ensure optimum resource utilization.

As more organizations adopt cloud computing, cloud service providers (CSPs) are developing new technologies to enhance the cloud's capabilities. Cloud mash-ups are a recent trend; mashups combine services from multiple clouds into a single service or application, possibly with on-premises (client-side) data and services. This service composition lets CSPs offer new functionalities to clients at lower development costs.

Collaboration among multiple cloud-based services, like cloud mashups, opens up opportunities for CSPs to offer more-sophisticated services that will benefit the next generation of clients.

A proposed proxy-based multicloud computing framework allows dynamic, on-the-fly collaborations and resource sharing among cloud-based services, A proposed proxy-based multicloud computing framework allows dynamic, on the-addressing trust, policy, and privacy issues without preestablished collaboration agreements or standardized interfaces.

With cloud computing initiatives, the scope of insider threats, a major source of data theft and privacy breaches, is no longer limited to the organizational perimeter

2. PRESENT SYSTEM AND PROBLEMS

Many existing cloud data services provide similar access control models, in which individual and organizational privacy, a key requirement for digital identity management, is unprotected. Also, with cloud computing initiatives, the scope of insider threats, a major source of data theft and privacy breaches, is no longer limited to the organizational perimeter. Multicloud environments exacerbate these issues because proxies can access data (which the environment might dynamically move or partition across different clouds) on behalf of clients. Revealing sensitive information in identity attributes to proxies that grant them authorization to access the data on behalf of clients is not an attractive solution. Thus, assuring the private and consistent management of information relevant to ABAC becomes more complex in multicloud systems.

- Increase in the attack surface due to system complexity,
- Loss of client's control over resources and data due to asset migration,
- Threats that target exposed interfaces due to data storage in public domains, and
- Data privacy concerns due to multitenancy

3. MULTICLOUD COMPUTING FRAMEWORK

Multi-Cloud computing has many advantages such as it provides usage of data from various clouds, the ability of

Volume: 6 Issue: 3 Pages: 2338-2341 (2014) ISSN : 0975-0290

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" [6] 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. 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 [6]. 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" [4] 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" [10] 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. This paper is based on review of the technique that will proof to be efficient while shifting towards the multi-cloud environment. All the factor included in this paper are the research work done in the fields which are the major concern whenever a new technology is to be implemented it includes the framework, platform for new technology to be implemented and the cost effectiveness on the side of the consumer.

3.1 Cloud hosted proxy

As Figure 1.1 shows, each CSP can host proxies within its cloud infrastructure, manage all proxies within its administrative domain, and handle service requests from clients that wish to use those proxies for collaboration. The proxy instances might need to be

CSP specific. For example, in Figure 1.1, both C1 and C2 might mutually and dynamically provision sharing and collaboration logic as proxy virtual instances within their respective administrative domains.

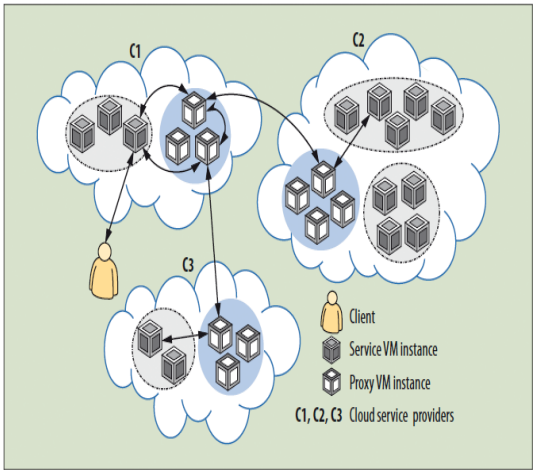

Figure1.1:Cloud-hosted-proxy

3.2 Proxy as a service

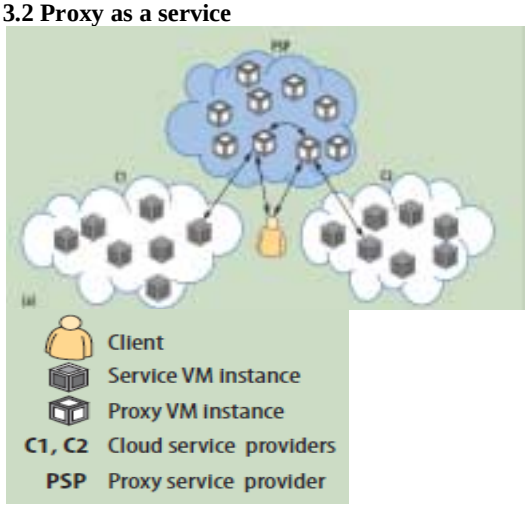

Figure1.2: Proxy as a service

As Figure 1.2 shows, this scenario involves deploying proxies as an autonomous cloud that offers collaborative services to clients and CSPs. A group of CSPs that are willing to collaborate can manage this proxy-as-a-service cloud, or a third-party entity, a proxy service provider (PSP), can provide management. Clients directly subscribe to the proxy cloud service and employ them for inter cloud collaboration.

4. GENERIC CLOUD COLLABORATION

Our proposed framework for generic 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 multicloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications. As more organizations adopt cloud computing, cloud service providers (CSPs) are developing new technologies to enhance the cloud's capabilities. Cloud mashups are a

Volume: 6 Issue: 3 Pages: 2338-2341 (2014) ISSN : 0975-0290

recent trend; mashups combine services from multiple clouds into a single service or application, possibly with on-premises (client-side) data and services. This service composition lets CSPs offer new functionalities to clients at lower development costs.

The proposed framework includes 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. Enhance id management protocol framework for more authentication. user centric identity management and is being considered as a complete \all-round solution addressing all possible issues of cloud IDMs.

5. IMPLEMENTATION

After careful analysis the system has been identified to have the following

- Collaboration Framework For Multicloud System
- Client/Users
- Cloud Service Provider
- Proxy Service Provider
- Collaboration Framework For Multicloud System :

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 multicloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications.

- **Client/Users :**

Client sends a request to cloud C1, which dynamically discovers the need to use services from clouds C2 and C3. C1 employs proxies to manage these interactions. A client that wishes to simultaneously use services from multiple clouds must individually interact with each cloud service, gather intermediate results, process the collective data, and generate final results. Proxies can facilitate collaboration without requiring prior agreements between the cloud service providers. First, the requesting entity chooses proxies to act on its behalf and to interact with cloud applications. A client or a CSP might employ multiple proxies to interact with multiple CSPs. It can select proxies based on, for example, latencies between proxies and clouds or workload conditions at various proxies.

- **Cloud Service Provider :**

Cloud service providers (CSPs) deploy proxies as an autonomous cloud system and offer it as a service to clients. A client employs two proxies to interact with CSPs C1 and C2. Alternatively, a client initiates a service request with C1, which then discovers the need for a service from C2. PSP: proxy service provider. Clients deploy proxies within the infrastructure of their organization. A client employs two proxies to interact with CSPs C1 and C2. A client initiates a service request with C1, which then discovers the need for a service from C2.

- **Proxy Service Provider :**

It involves deploying proxies as an autonomous cloud that offers collaborative services to clients and CSPs. A group of CSPs that are willing to collaborate can manage this proxy-as-a-service cloud, or a third-party entity, a proxy service provider (PSP), can provide management. Clients directly subscribe to the proxy cloud service and employ them for intercloud collaboration. 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.

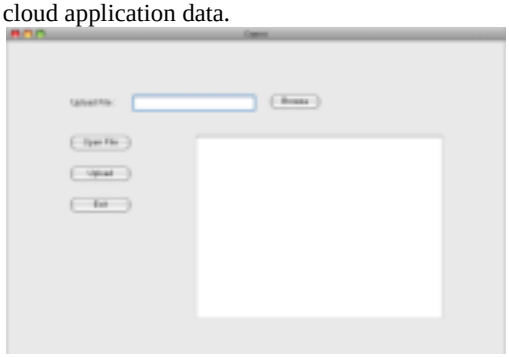

Fig 1.3 Owner uploads file

Fig 1.4 Uploaded file can be viewed

Fig 1.5 New service level agreement

Fig 1.6 New service level agreement successful

Volume: 6 Issue: 3 Pages: 2338-2341 (2014) ISSN : 0975-0290

Fig 1.7 File requested by user 'b' is successful

Fig 1.8 File requested by user 'a' is successful

6. CONCLUSION

The platform on which the services are to be shared and at last the market point of view that is its cost effectiveness compared to the available. The multi-cloud environment can end the vendor lock-in of the consumer which is attained in the single cloud. The major area of concern in this field is the agreement between the cloud service providers for collaboration of their services in multi-cloud. The consumer will get highly benefited with multi-cloud environment and obtain service based on his preferences and requirement and not based on his cloud service provider.

A secure multicloud computing which provides collaboration between clouds and gives the user opportunity to download the files from different cloud that is present. This also provides the security to the user's password and also to the files and data present in the cloud.

7. FUTURE ENHANCEMENT

Cloud computing is new and growing very quickly, but because security issues are still delaying its adoption, we need to provide security mechanisms to ensure that cloud computing benefits are fully realized and utilized.

Although there are many advantages to using a cloud-based system, practical problems remain that have to be solved before the technology can be more fully deployed, particularly those problems related to service level agreements, security, privacy, and power efficiency.

8. BIBLIOGRAPHY

[1]. P. Mell and T. Grance, The NIST Definition of Cloud Computing,special publication 800-145, Nat'l Inst. Standards and Technology, 2011

[2]. D. Bernstein and D. Vij, "Intercloud Security Considerations,"Proc. 2nd Int'l Conf. Cloud Computing (CloudCom 10), IEEE Press, 2010, pp. 537-544.

[3]. 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 and the Grid (CCGRID 09), IEEE CS, 2009, pp. 599-616.

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

[5]. M.P. Papazoglou and W. van den Heuvel, "Blueprinting the Cloud," IEEE Internet Computing, Nov./Dec 2011, pp. 74-79.

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

[7]. P. Mell and T. Grance, "Perspectives on Cloud Computing and Standards, NIST Information Technology Laboratory,"Nat'l Inst. Standards and Technology, 2008; http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloudcomputing-standards_ISPAB-Dec2008_P-Mell.pdf.

[8]. 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.

[9]. S. Chandrasekhar et al., "Efficient Proxy Signatures Based on Trapdoor Hash Functions," IET Information Security,Dec. 2010, pp. 322-332.

[10]. C.M. Ellison et al., SPKI Certificate Theory, IETF RFC 2693,Sept. 1999; www.ietf.org/rfc/rfc2693.txt.

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

[12]. Y. Zhang and J.B.D. Joshi, "Access Control and Trust Management for Emerging Multidomain Environments," An .Emerging Research in Information Assurance, Security and Privacy Services, Emerald Group Publishing, 2009, pp.421-452.

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

[14]. R. Wu, G.J. Ahn, and H. Hu, "Towards HIPAA-Compliant Healthcare Systems," Proc. 2nd ACM Int'l Symp. Health Informatics (IHI 12), ACM, 2012, pp. 593-602.

[15]. N.R. Adam and J.C. Wortmann, "Security-Control Methods for Statistical Databases: A Comparative Study," ACM ComputingSurveys, Mar. 1989, pp. 515-556.

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

[17]. D.J. Abadi, S. Madden, and M. Ferreira, "Integrating Compression and Execution in Column-Oriented Database Systems," Proc. ACM SIGMOD Int'l Conf. Management ofData (SIGMOD 06), ACM, 2006, pp. 671-682.