IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Multicloud Collaboration: The Cloud Mush up and Security Issues

Ghodake P.R[1], Nagode M.S. [2], Fatale P.R.[3], Menkudale K.S.[4]

Students, Department of Computer Science & Engineering, B.I.T. Barshi, India[1, 2, 3, 4]

Abstract: Cloud computing has now became a vital technology in IT sector. Its impact on the current and future technologies can be seen as the most powerful and flexible technology ever. This is due to the on-demand services offered by the cloud computing. The cloud computing model allows the provisioning of virtual resources according to the requirement, thus offering the "Pay As You Go" model. The term Multicloud computing refers to the mash up of different clouds together. A proposed multicloud computing environment let us to share the resources dynamically among cloud based systems. In general, multicloud involves service provider (admin), infrastructure providers and clients. In this proposed system, the service provider responds to the client by providing the file requested by it. The Proxy Service Provider (PSP) establishes the path for communication between different clouds.

Keywords: Multicloud computing, cloud service provider (CSP or admin or data owner), proxy service provider (PSP), Secure Hash Function (SHA).

I. INTRODUCTION

Cloud computing is an emerging technology in current era. The cloud computing framework provides a pool of resources where the services to the user are offered through Internet. These shared resources may include data storage space, networks, computer processing power, and specialized corporate and user applications. Cost saving, high availability and easy scalability are main advantages of cloud computing. Cloud computing has three most common services which are Software as a Service (SaaS), Platform as a Service (PaaS), and infrastructure as a service (IaaS). In Software as a Service model, a pre-made application is provided. In PaaS, an operating system, hardware, and network are provided, and in IaaS, the customer installs or develop its own software and applications. The virtualization of resources promotes the scalability and high availability of data and computing power. Hence, its leading to the growth in adoption of cloud computing by many organizations and businesses. But, the cloud computing framework restricts the access to data only by the client registered on the specific cloud. To tackle this issue, a multicloud framework was introduced. Collaboration among multiple clouds allows convenient sharing of data among many users.

Cloud mush up means services from multiple clouds are combined into a single service or application. This service composition makes cloud service providers (CSPs) to propose new functionalities to clients at lower development costs. Nowadays, cloud mashups need pre-established agreements among providers and proprietary tools that combine services through low-level, tightly controlled and constraining integration techniques. Some examples of cloud mush up include the following:

IBMs Mash up place:
This is a platform to rapidly create and share application building blocks and provides tools to put them into new web applications.

Appirio Cloud Storage:
With this Salesforce.com clouds users store information about accounts, opportunities, and so on in the Amazon S3 cloud.

Force.com:
a set of libraries for the Google App Engine that enable development of Web and business applications using resources in the Salesforce.com and Google clouds.

But realization of collaboration of multiple clouds requires consistent, transparent and universal interaction among multiple clouds. The greatest benefit of multicloud framework is that it would give users a choice among service providers, thus, resulting in the better services offered by the service providers. There are some security issues that occur while using the multicloud services. These are as follows:

- 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.
- Data privacy concerns due to multitenancy. Other specific security issues associated with multicloud collaboration includes:
- 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.
- Data privacy concerns.

II. ARCHITECTURAL DESIGN STRATEGY

Clouds consist of multiple network-connected resources such as servers, data warehouses, and storage components that ensure scalability, reliability, and high availability. A

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

multicloud system employing the proxy based framework for collaboration contains three architectural components: multiple cloud computing systems, networks of proxies, and clients (or service users).Such systems can use several possible strategies for placing proxies in the proxy network.

- Cloud-hosted proxy
- Proxy as a service
- Peer-to-peer proxy
- On-premise proxy

III. PROPOSED WORK:CLOUD MUSHUPS

The proposed system is based on the cloud-hosted proxy approach.Figure3.1 shows architecture of the proposed system using cloud-hosted proxy. The admin regulates the working of the clouds .Admin is having full control over file upload and downloads and provides services to authenticated users. The client can download the required files from any of the cloud present in the mush up of clouds. Whenever a client requests for specific information, the admin (service provider) look for the particular information in all the clouds. If the information is available and the requestor is authorized then the access to that client is provided. If the requested file is not available then the cloud service provider (admin)contacts to the proxy service provider to connect to other clouds in the mush up. As shown in Figure3.1, each CSP can host proxies within its cloud infrastructure, and manage all of them simultaneously handling service requests from clients that wish to use those proxies for collaboration.

The proxy instances can be CSP-specific. For example, in Figure 3.1, both C1 and C2 might mutually and dynamically provision sharing and collaboration logic as proxy virtual instances within their respective administrative domains.

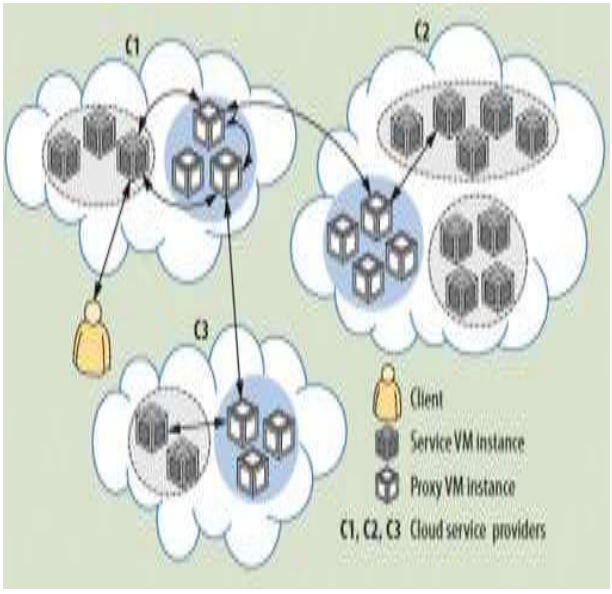

Figure 3.1 Client Sends a Request to Cloud C1, Which in turn uses Services from Clouds C2 and C3. C1 Employs Proxies to Manage these Interactions.

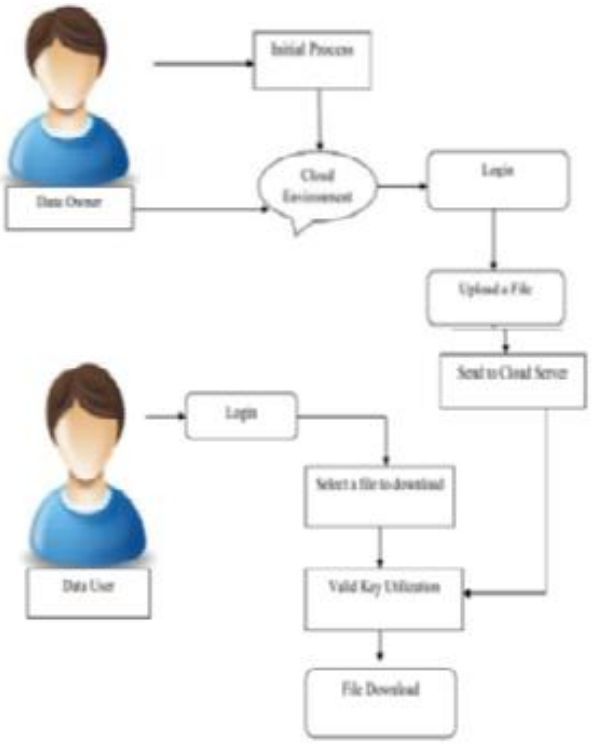

Figure3.2 Data flow Diagram

IV. SECURITY ISSUES IN MULTICLOUD COLLABORATION

Establishing Trust:

Security in the cloud relies heavily on the establishment of trust relationships among involved entities. The need for trust arises due to direct control of the security and privacy of its assets to a CSP. This reveals a client's assets to new risks that are preventable or decreased in internal organization. These risks consist of internal security threats, weakening the rights of ownership of data, trust issues with third party providers of cloud services. Establishing a trust relationship with proxies depends on the strategy used to establish, manage, and administer the proxy network. The entity managing the proxies must provide guarantees of its own trustworthy operation and also provide assurances of the proxies' security, reliability, and availability.

Policy Heterogeneity and Conflicts

When proxies enable dynamic collaboration between multiple CSPs, heterogeneous security policies can be the source of policy conflicts that result in security breaches. Proxies must monitor for and defend against such breaches. Even though existing policy evaluation mechanisms can verify individual domain policies, security violations can easily occur during integration. In multicloud collaborations using proxies, service requirements can drive dynamic, transient, and intensive interactions among different administrative domains. Thus, a proxy's policy integration tasks must address challenges such as semantic heterogeneity, secure interoperability' sand policy evolution management. The design of access control policies for multicloud

DOI 10.17148/IJARCCE.2016.52148

collaboration must permit careful management by proxies while ensuring that policy integration does not lead to security breaches.

V. CONCLUSION

To facilitate the dynamic collaboration between clouds, proposed work provides a framework that uses proxies to act as mediators between applications in multiple clouds that must share data. 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.

REFERENCES

[1] P. Meill 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 (Cloud Com 10), IEEE Press, 2010, pp. 537-544.
[3] P. Meill and T. Grance, "Perspectives on Cloud Computing and Standards, NIST Information Technology Laboratory," Nat'l Inst. Standards and Technology, 2008.
[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.
[4]. C.M. Ellison et al., SPKI Certificate Theory, IETF RFC 2693, Sept.1999; www.ietf.org/rfc/rfc2693.txt
[5]. S. Chandrasekhar et al., "Efficient Proxy Signatures Based on Trapdoor Hash Functions," IET Information Security, Dec. 2010, pp.322-332.

BIOGRAPHY

Ghodake P.R. Pursuing B. E. Computer & Science Engineering in JSPM's B.I.T. Barshi. (Maharashtra)

Nagode M.S . Pursuing B. E. Computer & Science Engineering in JSPM's B.I.T. Barshi. (Maharashtra)

Fatale P.R. Pursuing B. E. Computer & Science Engineering in JSPM's B.I.T. Barshi. (Maharashtra)

Menkudale K. S. Pursuing B. E. Computer & Science Engineering in JSPM's B.I.T. Barshi. (Maharashtra)

DOI 10.17148/IJARCCE.2016.52148