COLLABORATION IN MULTICLOUD COMPUTING ENVIRONMENTS: FRAMEWORK AND SECURITY ISSUES

Reshma Valishettar[1], Rameshkumar H K[2]

[1]M.Tech, [2]Assistant Professor, Dept. of Computer Science and Engineering,
STJIT, Ranebennur (India)

ABSTRACT

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

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.

Keywords: CSP (Cloud Service Provider), PSP (Proxy Service Provider, Multicloud, Multitenancy

I. INTRODUCTION

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 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. 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.

Today, cloud mashups require preestablished 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 spread across multiple clouds that lack pre-established agreements and proprietary collaboration tools.

Cloud-based computing also introduces new security concerns that affect collaboration across multi-cloud applications, including the following:

- 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.

Some specific security issues associated with collaboration among heterogeneous clouds include:

- Establishing trust among different cloud providers to encourage collaboration.
- Addressing policy heterogeneity among multiple clouds so that composite services will include effective
- Monitoring of policy anomalies to minimize security breaches.
- Maintaining privacy of data and identity during collaboration.

II. ARCHITECTURAL DESIGN

Clouds consist of multiple network-connected resource clusters such as server farms, data warehouses, and so on that host geographically distributed virtual machines and storage components that ensure scalability, reliability, and high availability. A multicloud system that employs proxies for collaboration consists of 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
- Hybrid proxy infrastructure

In this paper we have taken cloud-hosted proxy strategy.

2.1 Cloud-Hosted Proxy

As Figure1 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 Figure1, both C1 and C2 might mutually and dynamically provision sharing and collaboration logic as proxy virtual instances within their respective administrative domains.

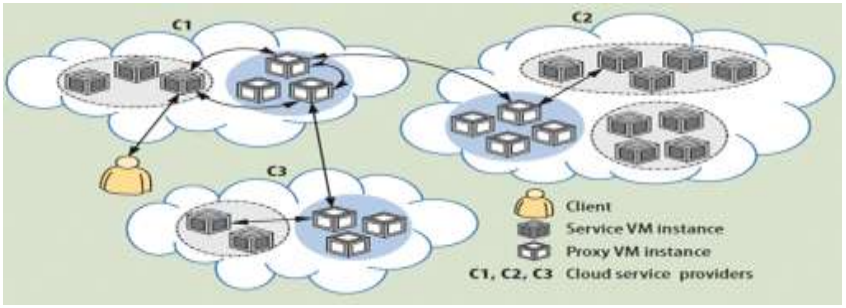

Figure 1: Client Sends a Request to Cloud C1, Which Dynamically Discovers the Need to Use Services from Clouds C2 And C3. C1 Employs Proxies to Manage these Interactions.

III. SECURITY ISSUES IN MULTICLOUD COLLABORATION

Researchers and industry specialists have highlighted several security issues in cloud computing, including isolation management, data exposure and confidentiality, virtual OS security, trust and compliance, and mission assurance. Specific security issues emerge during dynamic sharing and collaboration across multiple clouds. In particular, issues pertaining to trust, policy, and privacy are a concern in multicloud computing environments.

3.1 Establishing Trust and Secure Delegation

Using proxies moves the trust boundary one step further: clients and CSPs now must establish trust relationships with proxies, which includes accepting a proxy's security, reliability, availability, and business continuity guarantees. Moreover, CSPs responding to service requests that a proxy makes on behalf of a client or another CSP must trust the proxy to legitimately act on behalf of requesting entity. 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.

3.2 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, and policy evolution management. The design of access control policies for multicloud collaboration must permit careful management by proxies while ensuring that policy integration does not lead to security breaches.

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. 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. Favorable solutions to ensure data privacy must employ flexible data perturbation methods that provide control over the tradeoff between the privacy guarantee and the utility of the query results.\

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.

V. ACKNOWLEDGEMENT

I consider it is a privilege to express my gratitude and respect to all those who guiding me in the progress of my paper.

I wish my grateful thanks to ***Mr. Rameshkumar H K*** *M.Tech*, project guide, for his invaluable support and guidance.

Reshma Valishettar

REFERENCES

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing, special publication 800-145, Nat'l Inst. Standards and Technology, 2011, p. iii + 3.

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

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

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

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

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

BIOGRAPHY

Reshma Valishettar, is a student pursuing her Master degree in Computer Science and Engineering department at STJ Institute of Technology, Ranebennur(INDIA). Her research interests are Computer Science related aspects such as cloud computing technology, Java programming language and web 2.0.

Rameshkumar H K, is an assistant professor in the department of Computer Science and Engineering at STJ Institute of Technology, Ranebennur(INDIA). He received his Master degree in Computer Networks. His research interests are related to computer networks.