International Journal of Computer Science and Engineering Communications,
Vol.3, Issue.4, Page.1216-1219, (2015)
www.scientistlink.com

Secure Collaboration Framework for Multicloud Systems

[1]G.Radha Devi, [2]M.C.Babu
[1] *PG Scholar - Department of Computer Science, St. Peter's University, Chennai, India.*
[2]*Assistant Professor- Department of Computer Science, St. Peter's University, Chennai, India.*
[1]*deviradhag@gmail.com*, [2]mcbabu@yahoo.co.in

Abstract:
A proposed proxy-based multicloud computing framework allows dynamic, on the fly collaborations and resource sharing among cloud-based services, addressing trust, policy, and privacy issues without pre-established 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, PSP, Apps Upload, Unauthorized user, Check/send request, cloud mashup, universal/dynamic collaboration, data privacy, contract, resource management*

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 mashups 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. Examples of cloud mashups and technologies to support them include the following:

• IBM's Mashup Center, a platform for rapid creation, sharing, and discovery of reusable application building blocks (like widgets and feeds) with tools to easily assemble them into new Web applications.
• Appirio Cloud Storage, a cloud-based storage service that lets Salesforce.com cloud customers store information about accounts, opportunities, and so on in the Amazon S3 cloud.
• Force.com for the Google App Engine, a set of libraries that enable development of Web and business applications using resources in the Salesforce.com and Google clouds.

2. Literature Review

Introduction and related works

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are then to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above considerations are taken into account for developing the proposed system.

The NIST Definition of Cloud Computing

After years in the works and 15 drafts, the National Institute of Standards and Technology's (NIST) working definition of cloud computing, th**e** 16th and final definition has been published as The NIST Definition of Cloud Computing (NIST Special Publication 800-145). Cloud computing is a relatively new business model in the computing world. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three "service models" (software, platform and infrastructure), and four "deployment models" (private, community, public and hybrid) that together categorize ways to deliver cloud services. The definition is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. [1]

Intercloud Security Considerations

Cloud computing is a new design pattern for large, distributed data centers. Service providers offering applications including search, email, and social networks have pioneered this specific to their application. Recently they have expanded offerings to include 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 automation. These “public clouds” have been replicated by IT vendors for corporations to build “private clouds” of their own. Public and private clouds offer their end consumers a “pay as you go” model - a powerful shift for computing, towards a utility model like the electricity system, the telephone system, or more recently the Internet. However, unlike those utilities, clouds cannot yet federate and interoperate. Such federation is called the “Intercloud”. Building the Intercloud is more than technical protocols. A blueprint for an Intercloud economy must be architected with a technically sound foundation and topology. As part of the overall Intercloud Topology, this paper builds on the technology foundation emerging for the Intercloud and specifically delves into details of Intercloud security considerations such as Trust Model, Identity and Access Management, governance considerations and so on. [2]

Market-Oriented Cloud Computing

This keynote paper: presents a 21st century vision of computing; identifies various computing paradigms promising to deliver the vision of computing utilities; defines Cloud computing and provides the architecture for creating market-oriented Clouds by leveraging technologies such as VMs; provides thoughts on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain SLA-oriented resource allocation; presents some representative. Cloud platforms especially those developed in industries along with our current work towards realising market-oriented resource allocation of Clouds by leveraging the 3rd generation Aneka enterprise Grid technology; reveals our early thoughts on interconnecting Clouds for dynamically creating an atmospheric computing environment along with pointers to future community research; and concludes with the need for convergence of competing IT paradigms for delivering our 21st century vision. [3]

Blueprinting the Cloud

Current cloud solutions are fraught with problems. They introduce a monolithic cloud stack that imposes vendor lock-in and don't let developers mix and match services freely from diverse cloud service tiers to configure them dynamically to address application needs. Cloud blueprinting is a novel approach that lets developers easily syndicate, configure, and deploy virtual service-based application payloads on virtual machine and resource pools in the cloud. [5]

3. Existing System

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.

4. Proposed System

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 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 best cloud collaboration tools:

Use real-time commenting and messaging features to enhance speed of project delivery. Leverage presence indicators to identify when others are active on documents owned by another person. Allow users to set permissions and manage other users' activity profiles. Allow users to set personal activity feeds and email alert profiles to keep abreast of latest activities per file or user. Allow users to collaborate and share files with users outside the company firewall. Comply with company security and compliance framework. Ensure full auditability of files and documents shared within and outside the organization. Reduce workarounds for sharing and collaboration on large files

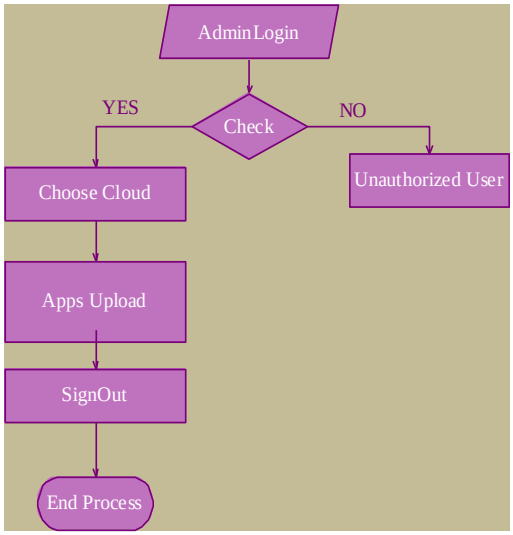

Fig. 1. Data Flow Diagram

5. Results and Discussion

Cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds.

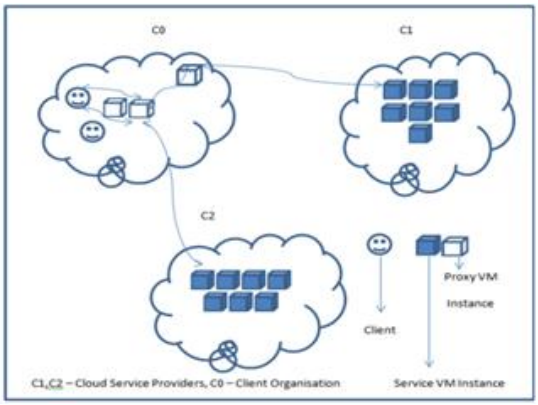

Fig. 2. Cloud Diagram

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 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 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. 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.

6. 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. 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. Currently, we are 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] 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 and the Grid (CCGRID 09), IEEE CS, 2009, pp. 599-616.

[4] GSM-Bluetooth based Remote Monitoring and Control 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. Chandrasekhar et al., "Efficient Proxy Signatures Based on Trapdoor Hash Functions," IET Information Security, Dec. 2010, pp. 322-332.

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

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

[10] P. Mell and T. Grance, "Perspectives on Cloud Computing and Standards,NIST Information Technology Laboratory," Nat'l Inst. Standards and Technology, 2008.