INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

PERSPECTIVES ON MULTICLOUD COMPUTING ENVIRONMENTS FRAMEWORK AND SECURITY ISSUES

[1]Hadiya Sameen, [2]Mohd Ayazuddin
[1]Nawab Shah College of Engineering & Technology (Affiliated to JNTUH)

[2]Nawab Shah College of Engineering & Technology (Affiliated to JNTUH)

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: Proxy-based Multicloud Computing Framework Resource Pooling, Multitenancy, Dynamic Reconfiguration, Infrastucture.

INTRODUCTION

Cloud instances must be able to dialog with each other. One cloud must be able to find one or more other clouds, which for a particular interoperability scenario is ready, willing, and able to accept an interoperability transaction with and furthermore, exchanging whatever subscription or usage related information which might have been needed as a pre-cursor to the transaction. Thus, an Intercloud Protocol for presence and messaging needs to exist which can support the 1-to-1, 1-to-many, and many-to-many use cases. The discussion between clouds needs to encompass a variety of content, storage and computing resources. The vision and topology for the Intercloud we will refer to is an analogy with the Internet itself: in a world of TCP/IP and the WWW, data is ubiquitous and interoperable in a network of networks known as the “Internet”; in a world of Cloud Computing, content, storage and computing is ubiquitous and interoperable in a network of Clouds known as the “Intercloud”. The reference topology for realizing this vision is modeled after the public Internet infrastructure. Various providers will emerge in the enablement of the Intercloud. We first envision a community governed set of Intercloud Root providers

Who will act as brokers and host the Cloud Computing Resource Catalogs for the Intercloud computing resources, similar to DNS [20] would be utilized. One important difference for the cloud capabilities is that the root systems would be replicating and hierarchical, but would not replicate in a hierarchical fashion.

The Intercloud Vision We propose that the roots replicate “sideways” and “upwards” using Peer to Peer technology [21] in order to scale. The sideways replication would be “master node” replication, as is common in P2P topologies, whereas the upwards replication would be to multiply interconnected peer replication, also as is common in P2P topologies.

The Intercloud Root instances will work with Intercloud Exchanges to solve the n2 problem by facilitating as mediators for enabling connectivity among disparate cloud environments. This is a much preferred alternative to each cloud vendor establishing connectivity and collaboration among themselves (point-to-point), which would not scale physically or in a business sense. Intercloud Exchange providers will facilitate the negotiation dialog and collaboration among disparate heterogeneous cloud environments, working in concert with Intercloud Root instances as described previously. Intercloud Root instances will host the root servers containing all presence information for Intercloud Root instances, Intercloud Exchange Instances, and Internet visible Intercloud capable Cloud instances. Intercloud Exchanges will host second-tier servers. Individual Intercloud capable Clouds will communicate with each other, as clients, via the server environment hosted by Intercloud Roots and Intercloud Exchanges. In order for the Intercloud capable Cloud instances to federate or otherwise interoperate resources, a Cloud Computing Resources Catalog system is necessary infrastructure. This catalog is the holistic and abstracted view of the computing resources across disparate cloud environments. Individual clouds will, in turn, will utilize this catalog in order to identify matching cloud resources by applying certain Preferences and Constraints to the resources in the computing resources catalog. The technologies to use for this are based on the Semantic Web which provides for a way to add “meaning and relatedness” to objects on the Web. To accomplish this, one defines a system for normalizing meaning across terminology, or Properties. This normalization is called Ontology.

LITERATURE SURVEY

The diversity and flexibility of the capabilities envisioned by Intercloud enabled federated Cloud computing model, combined with the magnitudes and uncertainties of its components, pose difficult problems and challenges in effective provisioning and delivery of application services in an efficient and secured manner.

Security is one of the most important and paramount elements of such a computing environment. In an Intercloud cross-clouds federated environment, security concerns are even more important and complex. Intercloud paradigm or cloud computing paradigm, in

General, will only be adopted by the users, if they are confident that their data and privacy are secured. Trust is one of the most fundamental means for improving security across heterogeneous independent cloud environments. Currently, Public Key Infrastructure (PKI) based trust model is the most prevalent one. PKI trust model depends on a few leader nodes to secure the whole system. The leaders' validity certifications are signed by well established Certificate Authorities ("CA"s). At a basic level, proposed Intercloud topology subscribes to the PKI based trust model. In accordance to the PKI trust model, the Intercloud Root systems will serve as a Trust Authority. In the currently proposed trust architecture, a Certificate issued by a Certificate Authority (CA), must be utilized in the process to establish a trust chain. The CAs which provides certificates must provide them in specific formats, undergo annual security audits by certain types of accountancy corporations, and conform to a host of best practices known as Public Key Infrastructure.

These requirements can vary by country. The PKI best practices, the CA process, and the accountancy rules, need to be re-examined for cloud computing. Certificates not only need to identify the clouds, but the resources the clouds offer, and the workloads that the cloud wishes federation with other clouds, to work upon. Where web sites are somewhat static, and a certificate can be generated to trust the identity of that web site, cloud objects such as resources and workloads are dynamic, and the certificates will have to be generated by a CA. As per the architecture of the CA, the Intercloud Exchange will need to be the intermediate CA, acting in a just-in-time fashion to provide limited lifetime trust to the transaction at hand.

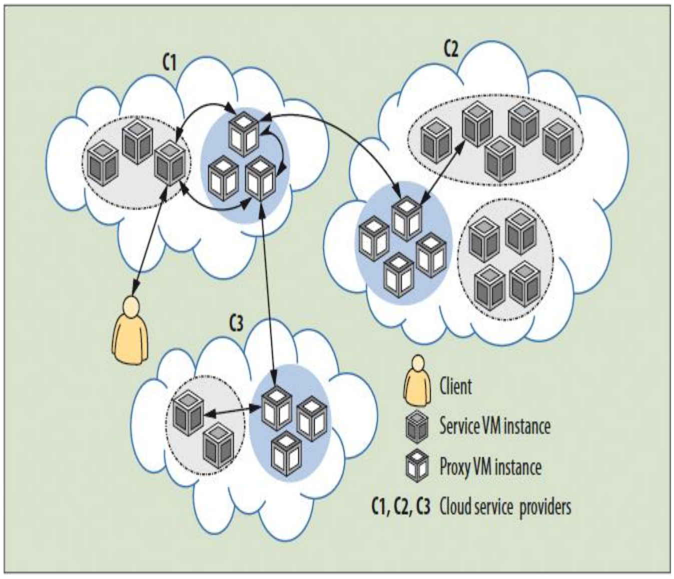
The current PKI certificates based trust model is primarily all or nothing trust model and is unsuitable for Intercloud environment. According to the current PKI based trust model, once the CA authorizes the certificate for an entity, the entity is either trusted or non-trusted. This is more like a Boolean relationship. However, in the cloud computing environment, especially in the Intercloud environment, this model needs to be extended to have "Trust Index" to go along with the existing PKI based trust model. "Trust Index" is essentially a level of trust demonstrated by cloud providers. Depending on the level of trust (40%50%, 60%, or 100%), for example, one Intercloud provider might trust another provider to use its storage resources but not to execute programs using these resources. The trust level is specified within a given time because the trust level today between two entities is not necessarily the same trust level a year ago. Trust Level is something dynamic in nature as opposed to static PKI certificates.

From Intercloud topology perspectives, Intercloud Roots will provide static PKI CA root like functionality. On the other hand, Intercloud exchanges will be responsible for the dynamic "Trust Level" model layered on top of the PKI certificate based trust model. The overall trust model is more of a "Domain based Trust" model. It divides the cloud provider computing environment into several trust domains. Nodes in the same domain usually are much more familiar with each other; they have a higher degree of trust for each other. Exchanges are the custodians/brokers of "Domain based Trust" systems environment for their affiliated cloud providers. Cloud providers rely on the Intercloud exchanges to manage trust. As Domain trust agents, Intercloud exchanges store other domains' trust information for inter-domain cooperation. Essentially, the trust information stored reflects trust value for a particular resource type (compute, storage etc.) for each domain. Exchanges also recommend other domains trust levels for the first time inter-domain interaction. At a high level, we are working towards a trust algorithm framework in order to derive the “Trust Index” for a cloud provider. Essentially, the Intercloud Trust algorithm will evaluate the underlying security attributes of a cloud provider such as “Firewall Capabilities”, “Intrusion Detection and Anti-Virus.

PROBLEM DEFINITION

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.

SYSTEM ARCHITECTURE



METHODOLOGIES

1. Collaboration Framework for Multicloud System Module:

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.

2. Client/Users Module:

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.

3. Cloud Service Provider Module:

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.

4. Proxy Service Provider Module:

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.

CONCLUSION AND FUTURE WORK

In this paper, 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 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, 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

Vol.2 Issue.10, Pg.: 20-25
October 2014

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 case.

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* (CloudCom10), 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.

Authors

1. Hadiya Sameen pursuing M. Tech (CS) in Nawab Shah College of Engineering & Technology.

2. Mohd Ayazuddin working as Assistant Professor in C.S.I.T department in Nawab Shah College of Engineering & Technology.