2011 IEEE World Congress on Services

# NIST Cloud Computing Reference Architecture

Robert B. Bohn, John Messina
Information Technology Laboratory
NIST
Gaithersburg, MD, USA
robert.bohn@nist.gov
john.messina@nist.gov

Fang Liu, Jin Tong, Jian Mao
Knowcean Consulting, Inc.
Potomac, MD, USA
liuf@knowceanconsulting.com
tongj@knowceanconsulting.com
maoj@knowceanconsulting.com

***Abstract*— This paper presents the first version of the NIST Cloud Computing Reference Architecture (RA). This is a vendor neutral conceptual model that concentrates on the role and interactions of the identified actors in the cloud computing sphere. Five primary actors were identified - Cloud Service Consumer, Cloud Service Provider, Cloud Broker, Cloud Auditor and Cloud Carrier. Their roles and activities are discussed in this report. A primary goal for generating this model was to give the United States Government (USG) a method for understanding and communicating the components of a cloud computing system for Federal IT executives, Program Managers and IT procurement officials.**

***Keywords-component; cloud computing, reference architecture, Federal Government***

## I. Introduction

In 2010, NIST was charged by Federal CIO Vivek Kundra with facilitating and leading the development of standards for security, interoperability and portability for cloud computing in the Federal Government as it makes its way into cloud adoption [1]. These standards will be driven by operational requirements of the agencies and through collaboration with Agency CIOs, private sector experts, and international bodies to identify, prioritize, and reach consensus on standardization priorities. In 2010, NIST conducted engagement workshops to identify and prioritize needs. NIST has already helped to establish broadly adopted definitions for the four commonly recognized cloud deployment models (i.e., private, public, hybrid, and community) and three service models (SaaS, PaaS, and IaaS). To be useful when describing and discussing cloud computing, a necessary condition is to have a common framework from which to start. This could only be achieved by developing a Reference Architecture and Taxonomy for cloud computing that will be the foundation for opening the discussion. This article describes the work of the NIST Cloud Computing Reference Architecture and Taxonomy Working Group (NCCRAT-WG) over the period Jan-Mar 2011 and presents the first version of the NIST Cloud Computing Reference Architecture and Taxonomy.

## II. Description of Model

The NIST Cloud Computing Reference Architecture (RA) is a neutral, actor role-based conceptual model and this is reflected in the accompanying taxonomy. The principle of neutrality in the vendor and technical solutions is strictly enforced in the model in order to prevent lock-in or stifle innovation in the marketplace. It was our objective to develop a RA that describes the *what* of cloud computing instead of the *how* and avoid a technical and solution based RA. By keeping this focused to a role based structure, we alleviate the need for developing a technically-based architecture at this time. The literature has many examples of technically-based cloud computing RA's [2-13]. The principle users for this RA will be IT leadership in the Federal Government, e.g. CIO's, IT program managers and procurement individuals.

The NCCRAT-WG identified 5 major actors who carry out unique and specific cloud computing activities which are depicted in Figure 1. Although not obvious from the figure, it is assumed that the Cloud Service Consumer's principle activities are purchasing and using services from a Cloud Service Provider or a Cloud Broker. From the USG viewpoint, the Cloud Service Consumer would be a federal agency that is interested in moving to a cloud-based solution, e.g. an SaaS solution, such as e-mail.

978-0-7695-4461-8 2011

DOI 10.1109/SERVICES.2011.105

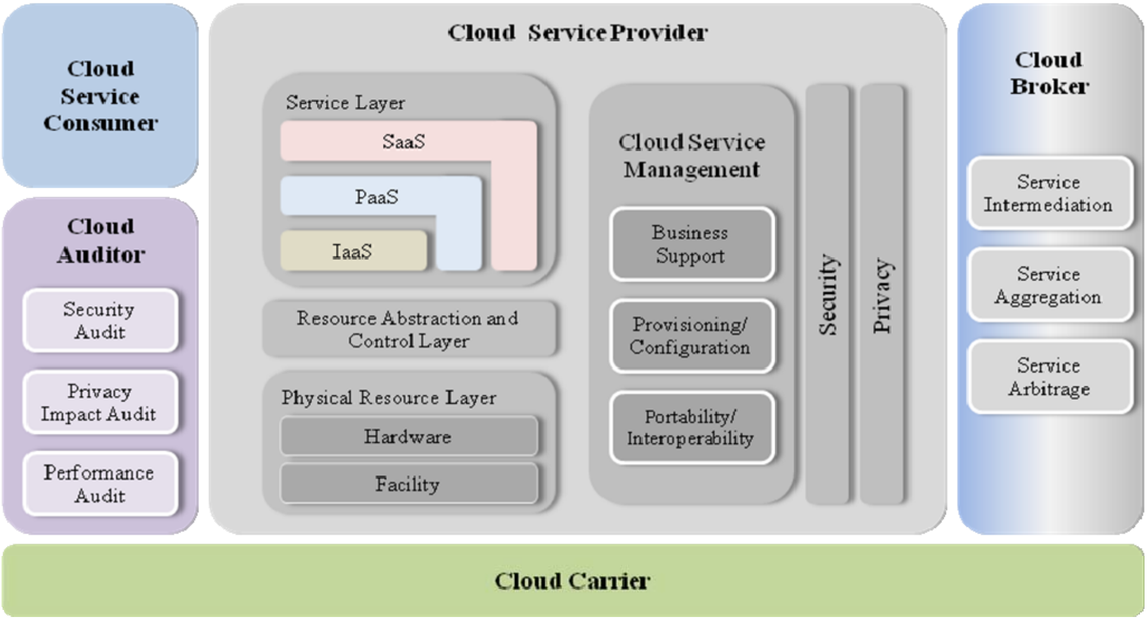

Figure 1. NIST Cloud Computing Reference Model

The Cloud Service Provider is associated with providing services, management of the resource allocation and control and the physical resource layers that make up the cloud. The Service Layers are depicted in such a way to show that it is possible to optimize each service layer down to the Resource Abstraction & Control Layer in addition to building layer upon layer. In addition, they are also responsible for the overall management of the cloud as shown in the Cloud Service Management (CSM) section. The CSM has three components: Business Support that consists of all business-related services with the clients and supporting process; Provisioning and Configuration that handles all aspects of provisioning, resource changing, monitoring, and metering; and Portability and Interoperability that supports the migration of services and data between clouds. The Security & Privacy aspects of the cloud cut across all layers of the cloud backbone. Work continues to proceed on this topic, but aspects related to this are Authentication & Authorization, Identity Management, Integrity, Security Monitoring & Response and Security Policy Management.

The integration of cloud services can be too complex for cloud consumers to manage, and a Cloud Broker eases this and plays a unique dual role in the RA. It behaves as a provider when interacting with a consumer or as a consumer when interacting with a cloud provider. It has three predominant activities: Service Intermediation, Service Aggregation and Service Arbitrage. Service Intermediation occurs when the Cloud Broker *enhances* a service by improving an existing one or providing other value-added services to consumers. Service Aggregation is accomplished when enhances an existing service or combine multiple services together to produce a new service. Service Arbitrage is similar to Service Aggregation except that the services being aggregated are not fixed.

A Cloud Auditor can evaluate the services provided by a cloud provider in terms of *security controls*, *privacy impact*, *performance*, etc. that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. “Auditing is especially important for federal agencies and agencies should include a contractual clause enabling third parties to assess security controls of cloud providers” [14].

The Cloud Carrier is the intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers. Cloud carriers provide access to consumers through network, telecommunication and other access devices. A cloud provider will set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers. Consumers may require the cloud carrier to provide dedicated and encrypted connections.

## REFERENCES

[1] V. Kundra, “25-Point Implemenation Plan To Reform Federal Information Technology Management”, December 2010.

[2] Gartner, “Gartner Says Cloud Consumers Need Brokerages to Unlock the Potential of Cloud Services”, http://www.gartner.com/it/page.jsp?id=1064712

[3] IETF internet-draft, “Cloud Reference Framework”, http://www.ietf.org/id/draft-khasnabish-cloud-reference-framework-00.txt

[4] IBM, “Cloud Computing Reference Architecture v2.0”, http://www.opengroup.org/cloudcomputing/doc.tpl?CALLER=documents.tpl&dcat=15&gdid=23840

[5] OASIS, the charter for the OASIS Privacy Management Reference Model Technical Committee, http://www.oasis-open.org/committees/pmrm/charter.php

[6] Open Security Architecture (OSA), “Cloud Computing Patterns”, http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing

[7] [16] Juniper Networks, “Cloud-ready Data Center Reference Architecture”, www.juniper.net/us/en/local/pdf/reference-architectures/8030001-en.pdf

[8] DMTF, “Interoperable Clouds White Paper”, http://www.dmtf.org/about/cloud-incubator/DSP_IS0101_1.0.0.pdf

[9] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus In Cloud Computing V2.1”, www.cloudsecurityalliance.org/csaguide.pdf

[10] CISCO, “Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions”, http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf

[11] GSA, “Cloud Computing Initiative Vision and Strategy Document (DRAFT)”, http://info.apps.gov/sites/default/files/Cloud_Computing_Strategy_0.ppt

[12] SNIA, “Cloud Storage for Cloud Computing”, www.snia.org/cloud/CloudStorageForCloudComputing.pdf

[13] L.J. Zhang and Q. Zhou, "CCOA: Cloud Computing Open Architecture", Proceedings of 2009 IEEE International Conference on Web Services (ICWS), Jul. 6-10, 2009, Los Angeles, CA, USA, pp. 607-616.

[14] V. Kundra, “Federal Cloud Computing Strategy”, February 2011.