Federal Government Application of the Cloud Computing Application Integration Model

John P. Sahlin
The George Washington University, USA

INTRODUCTION

As Amazon, Earthlink, Rackspace, and IBM vie for supremacy in the commercial cloud computing marketplace, government agencies are investigating whether this model, geared toward improving profitability can apply to government.

This article challenges the notion that cloud computing cannot add value to government agencies. Despite arguments that cloud computing is only appropriate for commercial enterprises, appropriate aspects of cloud computing can and should be applied to government agency efforts to reduce costs while others may be an imperfect fit (Buyya, Yeo, Vengupal, Broberg, & Brandic, 2009; Armbrust et al., 2009). The Systems Engineer's primary role in this case is to balance the needs of business-oriented features of cloud computing with the needs and constraints of the government organization, which is different from those of commercial organizations.

BACKGROUND

In 2011, the U.S. Chief Information Officer (CIO) Vivek Kundra announced that all federal agencies must evaluate cloud computing options for integrating applications with infrastructure before making any capital investments. A recent study indicated that U.S. Federal Government spending on cloud computing will reach $1.7 billion in 2014 and is likely to exceed $7 billion by 2017 (McCarthy, 2013). While government agencies are not required to adopt cloud computing as their application integration approach, they are required to consider adoption before making capital investments (Kundra, 2011). While some decisions are clear (e.g., not adopting a public cloud infrastructure for classified systems), the federal government is at a distinct disadvantage when evaluating commercial cloud computing options. Because cloud computing architectures were designed originally for improving the profitability of commercial organizations, it becomes difficult to determine whether cloud computing presents an appropriate and valuable model of application integration for government organizations.

This disadvantage may be contributing to slow adoption of cloud computing by government agencies. Federal spending on cloud computing architectures is projected to decline in 2013 and beyond in favor of more limited server consolidation models (McCarthy, 2013, 2013a). While server consolidation is considered a form of cloud computing, the adoption of more limited cloud computing models appears to indicate that the original models of on-demand scalability, self-service, and applications on a "pay-for-play" model is not extensible to Federal Government agencies.

Literature Review: The Emergence of Cloud Computing

To reduce sustainment costs, service providers sought to provide applications in a predictable and automated manner. Automatic provisioning technology helped ASPs reduce maintenance costs and provide a stable baseline across a heterogeneous client enterprise, increasing the overall effectiveness of the client support organization (Chouhan, 2006). Security of data was of paramount concern for hosting service providers as they provided business-critical/proprietary data for multiple clients in the same infrastructure environment. Security is critical for the cloud computing model, as platforms and infrastructure are virtualized on a single pool of resources across the entire enterprise. As technology for data segregation improved, use of physically

DOI: 10.4018/978-1-4666-5888-2.ch267

separate data stores evolved to Community of Interest (COI) segregation with encryption (Motahari-Nezhad, Stephenson, & Singhal, 2009).

The cloud computing industry emerged in order to address the rising costs and security concerns associated with hosting environments. The complexity of ensuring security and separation of sensitive data has driven service providers to consider alternative infrastructure designs. The need for additional business agility and cost reduction has driven a need for additional automation and self-service for deployment.

Service monitoring is critical in a cloud computing environment (Mell & Grance, 2009). The Service on Demand Architecture (SODA) model of dynamic service metering enables a pay-as-you-go approach based on subscription and demand (Jiang and Xu, 2003).

CLOUD COMPUTING: A MODEL FOR GOVERNMENT IT ACQUISITION

Concepts of Cloud Computing

Since 2008, several definitions have been offered for the term "cloud computing." The term seems as nebulous as the imagery it conjures. These definitions have varied from those who argue that cloud computing is limited to commercial ventures to far more generic definitions that could apply to any form of virtualized/abstracted system design (Buyya et al., 2009; Armbrust et al., 2009). The U.S. National Institute of Standards and Technology (NIST) provides the most useful definition of cloud computing, as it defines the characteristics in terms of models for deployment, allowing for applications beyond the commercial industry without rendering it indistinguishable from earlier computer architectures.

Cloud computing draws upon the lessons learned from the Application Service Provider (ASP) and Internet Service Provider (ISP) industries. Cloud computing takes advantage of evolving technology to realize the original vision of distributed computing from the days of mainframe computing. While distributed computing is not new, cloud computing represents the convergence of advances in abstraction technology with the original vision of distributing the computational load across multiple nodes (Sahlin, 2013).

In the NIST definition of cloud computing, Mell and Grance discuss the technology enablers that comprise a cloud computing architecture (2011), including virtualization, storage networking, automated provisioning, network monitoring, and Quality of Service (QoS) management. Any infrastructure consolidation program must provide most of these capabilities. However, NIST defines cloud computing as distinct from other models by identifying five essential characteristics (Mell & Grance, 2011):

- **On-Demand Service:** The end-user/consumer can unilaterally (and automatically) provision computing capabilities such as server time, storage, and applications
- **Broad Network Access:** Capabilities are available over a network and accessed by heterogeneous client base
- **Resource Pooling:** Computer resources are abstracted and pooled to serve multiple consumers
- **Rapid Elasticity:** Capabilities can be rapidly provisioned to scale up, out, or down to meet changing business needs
- **Measured Service:** Metering service to monitor and control resources automatically for optimized resource allocation

Cloud computing is generally a commercial architecture. By delivering scalable services and automated self-service to end users, a Cloud Service Provider (CSP) allows for rapid delivery of services and is a force multiplier for small business lacking investment capital. The NIST definition of cloud computing does not preclude non-commercial ventures as do other definitions provided in literature (Buyya et al., 2009; Armbrust et al., 2009). The NIST definition includes a tiered model of graduated services (a "stairway" to the clouds) that allows a cloud consumer to define which aspects of the cloud it needs and is represented (see Figure 1).

The foundation tier is called Infrastructure as a Service (IaaS) and provides hardware and software infrastructure (e.g., server and storage hardware, network, facilities, Operating System) and systems management (e.g., network monitoring, patch management). The CSP can provide additional services by managing core applications and a development environment (e.g., widget frameworks, Google Apps) for consumers in the Platform as a Service (PaaS) offering. In the most