1 Cloud Computing Overview

Cloud computing technology is not new! The technology is ubiquitous, the service offering concepts and service models are newer concepts. It is a common terminology that can be applied to various service provider network models that deliver host-based services to customers (mostly Internet-based access).

Cloud consumers can benefit from:

- *Significant IT cost savings based on economies of scale;*
- *Service flexibility (on-demand); and*
- *Increased IT capabilities*

To differentiate cloud computing from traditional IT hosting services, cloud computing offers:

- *Customer purchased on-demand;*
- *Service elasticity by up-scaling or down-scaling using automated transparent processes; and*
- *Generally managed by Service Provider (depending on the deployment model, see below).*

From a technology perspective, one can related to Virtual Machines (VM) as a component of cloud computing; however, it is but a component and not the focal point of cloud computing depending on the service model.

1.1 Defining Cloud Computing

Cloud computing can best be defined by its main characteristics which are recognized in industry as being pervasive for all cloud computing service offering models:

- ***On-demand self-service**: A customer can unilaterally provision computing capabilities such as server time and network storage as needed automatically, without requiring human interaction with a service provider.*
- ***Broad network access**: Services are provided over the network and accessed through standard interfaces (VPN, web-based etc.) to facilitate use by cellular-based phones, portable computing devices (laptops, net books etc.), and PDAs. as well as other traditional or cloud-based software services.*
- ***Resource pooling**: A Service Provider (SP) pools its computing resources to serve several customers (usually based on a multi-tenant model) with varying resources dynamically assigned and based on customer demand. Generally, the customer is not made aware of the physical or logical location of the resources being consumed.*

- ***Rapid elasticity****: Service offerings can be ramped up or reduced based on various scaling requirements and customer demands. Scaling is mostly automated and transparent to the customer based on ability to consume…and pay.*
- ***Measured service****: Resource usage is controlled by metering and reporting usage to customers on a per contract (Service level Agreement).*

1.2 Typical Cloud Service Offerings

Cloud services are usually offered to customer based on any of the three service models[1]:

- ***Cloud Software as a Service (SaaS):*** *The capability provided to the customer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited use-specific application configuration settings.*
- ***Cloud Platform as a Service (PaaS):*** *The capability provided to the customer is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.*
- ***Cloud Infrastructure as a Service (IaaS):*** *The capability provided to the customer is to provision processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).*

There are security benefits and risks associated with each service and can be mitigated through risk assessments and risk mitigation strategies.

[1] Based on definitions provided by NIST Special Publication 800-145, September 2011.

1.3 Cloud Deployment Models

Various deployment models are available that facilitate management and consumption of the services to customers:

Public Cloud: A public cloud is one in which the infrastructure and computational resources that it comprises are made available to the general public over the Internet. It is owned and operated by a cloud provider delivering cloud services to customers and, by definition, is external to the customers' organizations.

Private Cloud: A private cloud is one in which the computing environment is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization's data center or outside of it. A private cloud has the potential to give the organization greater control over the infrastructure, computational resources, and cloud customers than can a public cloud.

Community Cloud: A community cloud falls between public and private clouds with respect to the target set of customers. It is somewhat similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization.

Hybrid Cloud: Hybrid clouds are more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public). Each member remains a unique entity, but is bound to the others through standardized or proprietary technology that enables application and data portability among them.

2 Security Considerations

Cloud computing can be a significant cost saver for many IT applications and definitely a business enabler. The common security issues associated with cloud computing are not trivial; however, once understood, customer and SP risk mitigation strategies can be applied to satisfy business objectives. Some of the common security issues include:

- *Security Governance;*
- *Portability (i.e. changing SP);*
- *Multi-tenancy and component failures;*
- *Legal, Regulatory and Customer Policy-specific Compliance;*
- *Customer Management Interface Compromises;*
- *Data Protection (Confidentiality, Integrity and Availability);*
- *Secure Data Retention and Disposal; and*
- *Service Provide Malicious activity (insider access)*

All of these issues can be addressed and security strategies developed, including transferring certain risks to the SP.

Both consumers and Service providers should address the following aspects of security to establish adequate assurances for suitable information protection:

- *Personnel security requirements, including roles, and responsibilities*
- *Regulatory requirements (Privacy Act, PIPEDA*
- *Service availability*
- *Problem reporting, review, and resolution*
- *Information handling and disclosure agreements and procedures (Information sharing)*
- *Physical and logical access controls*
- *Network access control*
- *Data protection (Confidentiality Integrity Availability)*
- *System configuration and patch management*
- *Backup and recovery*
- *Data retention and Disposal (sanitization)*
- *Vulnerability scanning*

- *Risk management (includes TRA)*
- *Incident reporting, handling, and response*
- *Continuity of operations (BCP)*
- *Resource management*
- *Certification and Accreditation (C&A, ISO27001)*
- *Assurance levels*
- *Independent auditing of services.*

Avalon Security certified professionals can assist with any or all of the security issues and facilitate adequate business objective achievements by working with both customers and Service Providers.