

Table of contents

Cloud Computing Overview

Risks in the Cloud



Cloud Computing Overview



Definition of cloud computing

Cloud computing is a model for enabling 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. This cloud model promotes availability and is composed of five essential **characteristics**, three **service models**, and four **deployment models**.

Essential Characteristics:

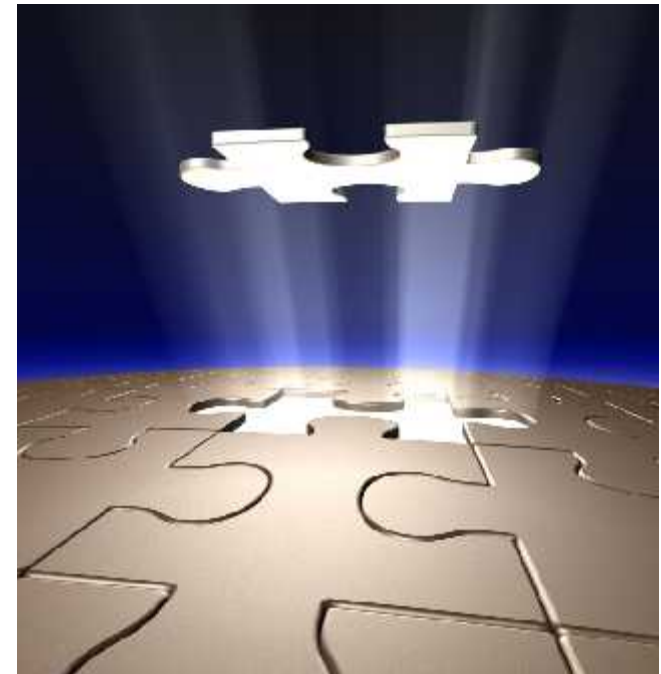
1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured Service

Service Models:

1. Cloud Software as a Service (SaaS)
2. Cloud Platform as a Service (PaaS)
3. Cloud Infrastructure as a Service (IaaS)

Deployment Models:

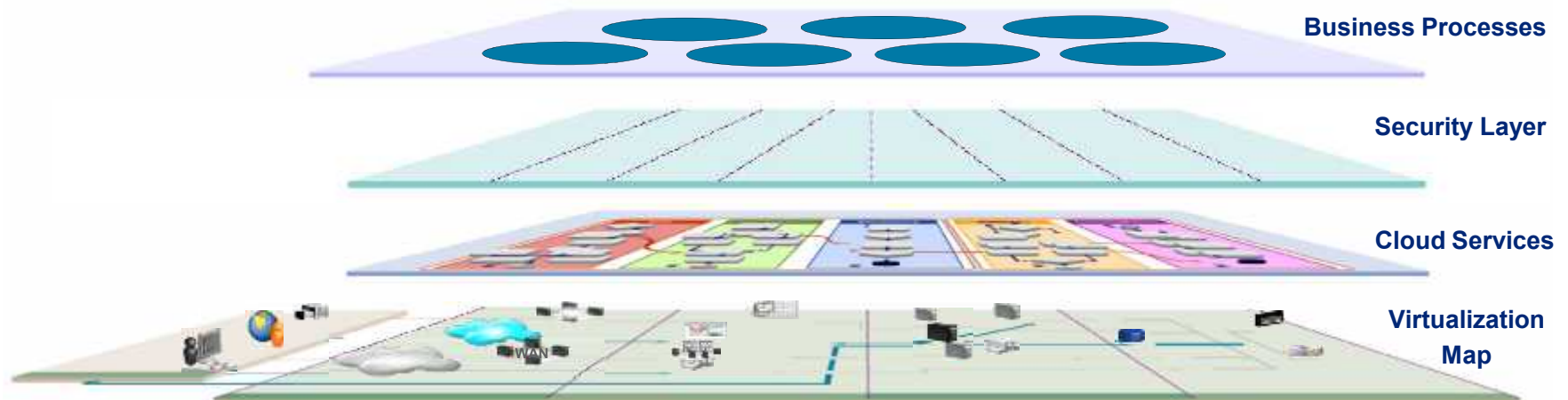
1. Private cloud
2. Community cloud
3. Public cloud
4. Hybrid cloud



Source: <http://csrc.nist.gov/groups/SNS/cloud-computing/>

What is Virtualization and Cloud Computing?

- **Virtualization** is the replacement of a physical system with a virtual version of the operating system, storage device, application, network resource, security appliances, etc
- **Cloud computing** is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources
- **Virtualization** enables cloud computing, but cloud computing does not require virtualization

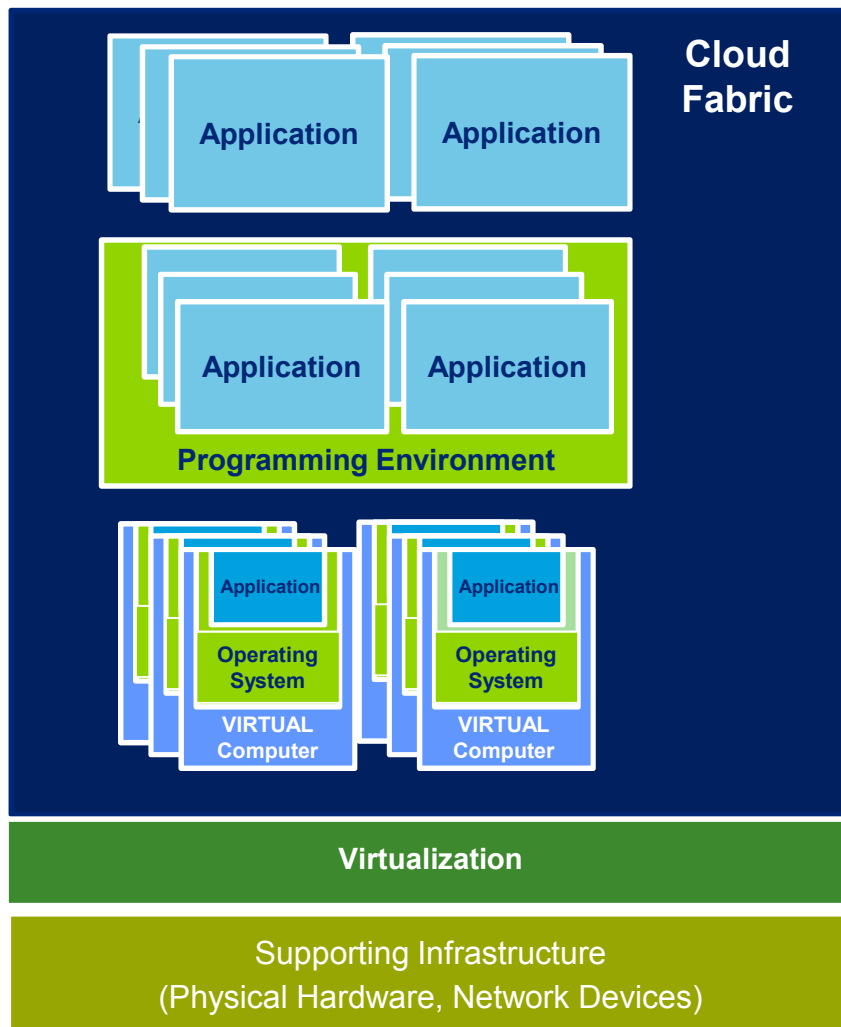


Cloud computing delivery models, based on their characteristics and purpose

Cloud computing technology is deployed in different ways, with varying internal or external ownership and technical architectures

| | |
|-------------------------------------|--|
| Vendor cloud (External) | Cloud computing services from vendors that can be accessed across the Internet or a private network, using one or more data centers, shared among multiple customers, with varying degrees of data privacy control. Sometimes called “public” cloud computing. |
| Private cloud (Internal) | Computing architectures modeled after vendor clouds, yet built, managed, and used internally by an enterprise; uses a shared services model with variable usage of a common pool of virtualized computing resources. Data is controlled within the enterprise. |
| Hybrid cloud | A mix of vendor cloud services, internal cloud computing architectures, and classic IT infrastructure, forming a hybrid model that uses the best-of-breed technologies to meet specific needs. |
| Community cloud | Community clouds are used across organizations that have similar objectives and concerns, allowing for shared infrastructure and services. Community clouds can be deployed using any of the three methods outlined above, simplifying cross-functional IT governance. |

Visualizing the differences



Software as a service (SaaS)

SaaS covers the range of application that are licensed for use as services provided to customers on demand typically across the Web.

Platform as a service (PaaS)

The PaaS model makes all of the facilities required to support the complete life cycle of building and delivering Web applications and services entirely available from the Internet.

Infrastructure as a service (IaaS)

IaaS is the delivery of computer infrastructure as a service. Rather than purchasing servers, software, data center space, or network equipment, clients instead buy those resources as a fully outsourced service.

Virtual layer

Common IT Infrastructure

Risks in the Cloud



Operations management

Risks created if IT operations management processes are not enhanced

| | |
|-------------------------|--|
| Deployment Rules | <ul style="list-style-type: none">• Mix of High, Medium and Low Risk applications• Segregation of Duties – who can manage VM, apps, physical & virtual network interfaces• Application lifetime – how long from time virtualized application is started up until it is ended• VM & application movement – vMotion |
| IT Operations | <ul style="list-style-type: none">• Architecture Standards/Hardening Guidelines• Configuration Management• Patch Management• Capacity Planning• Incident Response• Logging and Monitoring• Disaster Recovery |

New attack modes/surfaces

Cloud Computing and Virtualization can increase and introduce new challenges in the attack surface...

| | |
|---------------------|---|
| Attack Types | <ul style="list-style-type: none">• Hyperjacking — Bluepill/Subvirt• Guest Hopping• Migration — potential Man in Middle type attacks• Compromise of VM templates• Exploiting weaknesses in software on the Hypervisor |
| Management | <ul style="list-style-type: none">• Protecting Virtual Center or equivalent• Ensuring appropriate privileged user access controls• Starting, moving or changing VMs outside procedural controls |
| Network | <ul style="list-style-type: none">• Virtual network layer• Trust Zone Architecture• Physical or virtual (VLAN segmentation)• Use of API like VMSafe/tools like Trend Micro, Reflex, Altor, etc. |

Threats - Confidentiality

| Threat | Description |
|--------------|--|
| Insider | <ul style="list-style-type: none">• Malicious cloud provider user• Malicious cloud customer user• Malicious third party user |
| External | <ul style="list-style-type: none">• Remote software attack of cloud infrastructure• Remote software attack of cloud applications• Remote hardware attack against the cloud• Remote software and hardware attack against cloud user organizations' endpoint software and hardware• Social engineering of cloud provider users, and cloud customer users |
| Data Leakage | <ul style="list-style-type: none">• Failure of security access rights across multiple domains• Failure of electronic and physical transport systems for cloud data and backups |

Threats - Integrity

| Threat | Description |
|--------------------------|--|
| Data Segregation | <ul style="list-style-type: none">• Incorrectly defined security perimeters• Incorrect configuration of virtual machines and hypervisors |
| User Access | <ul style="list-style-type: none">• Poor identity and access management procedures• Implemented an inadequate Identity & Access Management (IAM) system• User provisioning and de-provisioning policies and procedures do not address virtualized/cloud specific requirements• User rights not adequately segregated or defined |
| Data Quality | <ul style="list-style-type: none">• Introduction of faulty application or infrastructure components• Data input inadequately validated |
| Configuration Management | <ul style="list-style-type: none">• Baseline VM templates are not kept up to date with patches, anti-malware signatures, system configuration changes |

Threats - Availability

| Threat | Description |
|-------------------------------------|--|
| Change Management | <ul style="list-style-type: none">• Customer penetration testing impacting other cloud customers• Infrastructure changes upon cloud provider, customer and third party systems impacting cloud customers |
| DoS Threats | <ul style="list-style-type: none">• Network bandwidth distributed denial of service• Network DNS denial of service• Application and data denial of service |
| Physical Disruption | <ul style="list-style-type: none">• Disruption of cloud provider IT services through physical access• Disruption of cloud customer IT services through physical access• Disruption to third party WAN providers services |
| Exploiting Weak Recovery Procedures | <ul style="list-style-type: none">• Invocation of inadequate disaster recovery or business continuity processes• Data and VM backups protected at a lower level than running systems |

IT Operations

Change Management

Updates to system and application configuration

- Who is responsible for what updates and within what time frame?
- Testing and validating configurations in constantly changing environments
- Ensuring only authorized people make approved changes to software and configurations
- Patching running systems and system templates

Pre and Post Deployment testing

- What environment to conduct testing in?
- Testing for correct functioning in constantly changing environment



Vendor Management

Vendor Selection

Cloud computing can push responsibility for software ownership and licensing issues to other organizations – but it can also disrupt your ability to operate.

Software developed in house by your cloud provider can run into patent or copyright problems, also putting you at risk.

Some questions to ask:

- Who is responsible for software licensing and ownership?
- What options are available if there is an issue with software we own or license?
- What can we do if parties we depend on have issues with the software they own, develop or license?
- How can we manage software costs in an elastic environment?



Infrastructure Security

Inability to independently test application security

Working with the Cloud provider

- Restrictions on continuous assessment and periodic security testing
- Coordinating software and configuration changes that may impact your systems

What is the security of the Cloud providers software

- What is the security posture of the software the Cloud provider is running?
- Does the cloud vendor securely configure their systems?
- What evidence of their security posture can they provide?

How will other Cloud users impact you

- Are other Cloud clients fully patched and up to date?
- What other software is running on systems?



Questions?



Contact information

For additional information, please contact:

Amry Junaideen

Principal

Deloitte & Touche LLP

ajunaideen@deloitte.com

+1 202 220 2664

Irfan Saif

Principal

Deloitte & Touche LLP

isaif@deloitte.com

+1 408 704 4109

Raymond Soriano

Director

Deloitte & Touche LLP

rsoriano@deloitte.com

+1 561 962 7735

Andrew Murren

Manager

Deloitte & Touche LLP

amurren@deloitte.com

+1 202 220 2121



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2011 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited