Cloud Computing Overview & Security Issues

Author- Hitesh Malviya(Information Security analyst)

Qualifications: C!EH, EC!SA, MCITP, CCNA, MCP

Current Position: CEO at HCF Infosec Limited

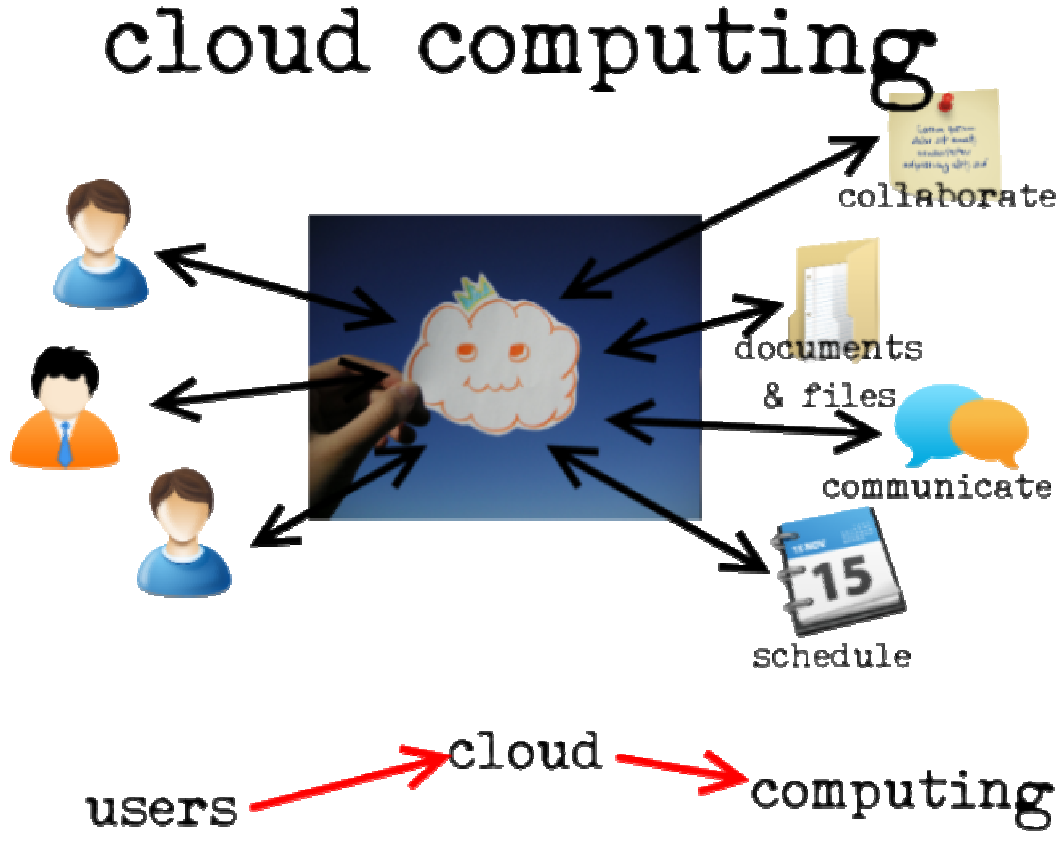
Contact: hitesh@hcf.co.in, hitesh1@hackermail.com

Website: www.hcf.co.in, www.hitesh.hcf.co.in

Overview

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. It can be used as a service rather than a product. Cloud computing is basically a remote storage of data over the internet, anyone can use stored data at any instant. Google Docs is the most familiar example of cloud computing. Google Docs is cloud computing services provided by Google where we can store our documents and can access it at any instant. Huge datacenters are used to store large amount of data.

Cloud computing providers deliver applications via the internet, which are accessed from **web** browsers and desktop and mobile apps, while the business software and data are stored on servers at a remote location.



These services are broadly divided into three categories:

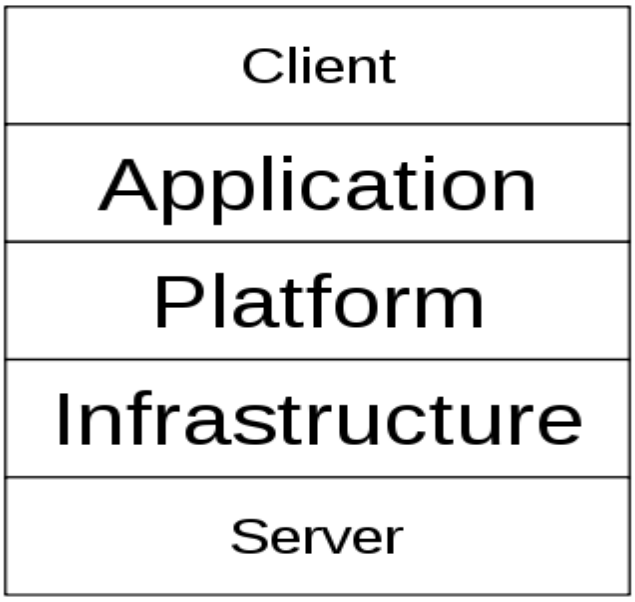
- Infrastructure-as-a-Service (IaaS)
- Platform-as-a Service(Paas)
- Software-as-a Service(Saas)

Infrastructure-as-a-Service (Iaas): Infrastructure as a Service is a provision model in which an organization outsource the equipment used to support operations, including storage, hardware, servers and networking components.

Platform-as-a Service (Paas): Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Software-as-a Service (Saas): Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Cloud computing services use 4-layered architecture.



Client : It consists of computer hardware and software to that relies on cloud computing for application delivery.

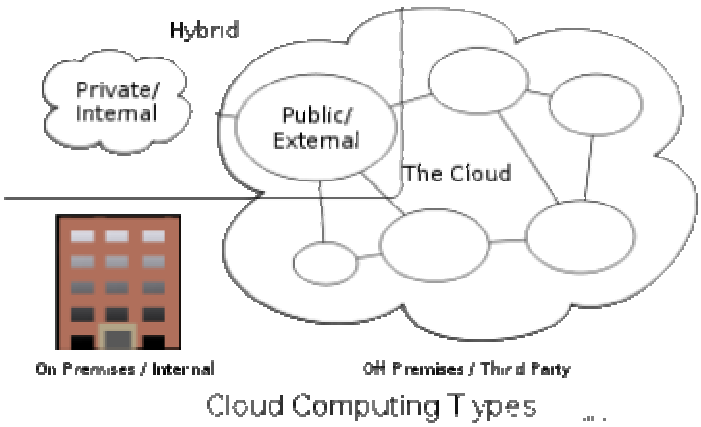
Application : Cloud application services or "Software as a Service (SaaS)" deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support

Platform : Cloud platform services, also known as platform as a service (PaaS), deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications.

Infrastructure : Cloud infrastructure services, also known as "infrastructure as a service" (IaaS), deliver computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking.

Server : The server layer consists of computer hardware and/or computer software products that are specifically designed for the delivery of cloud services, including multi-core processors, cloud-specific operating systems and combined offerings.

Deployment models



Cloud Computing Types

Public Cloud : It is based on standard cloud computing model in which service provider makes resources and general people use it over internet.

Community Cloud : It shares infrastructure between several organizations from specific community whether managed by third party or hosted internally or externally.

Hybrid Cloud : It is composition of two or more clouds(private, community or public) offering the benefits of multiple deployment models.

Private Cloud : Private cloud is infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.

Cloud Computing Providers

Gartner predicts that cloud computing will surge to 150 billion dollars by 2013. Below is a partial list of companies that provide cloud computing services:

- Google
- Amazon
- OpenID
- Microsoft
- Sun Sytems
- Intel
- IBM & many more.

Security Issues with Cloud Computing

Cloud computing is fraught with security risks. Smart customers will ask tough questions and consider getting a security assessment from a neutral third party before committing to a cloud vendor. Customers have rare information about cloud security that make them complaining about security risks.

In a customer point of view they must demand transparency, avoiding vendors that refuse to provide detailed information on security programs. Ask questions related to the qualifications of policy makers, architects, coders and operators, risk-control processes and technical mechanisms.

Here are seven of the specific security issues customers should raise with vendors before selecting a cloud vendor.

(1)Privileged user access : With cloud computing, your confidential data can be accessible to outside the enterprise . It proceeds an inherent level of risk because now **Outsiders is Insiders.**

Advice: Get much information as can about the people who manage your data

(2) Regulatory compliance : Traditional service provider is subjected to external audits and security certifications. Cloud computing doesn't provide any kind of external audit service in that case **Customers are only responsible for the security & intregity of their data**.

(3) Data Location : Customers won't know about the location of cloud where their data is hosted, they might not even know what country data will be stored in.

Advice: Ask service providers to make a commitment to store data in specific jurisdictions.

(4) Data segregation : Data in the cloud is typically in the shared enviorenment, service providers provide effective encryption but it isn't a cure at all.

Advice: The cloud provider should make a commitment to customer to provide evidence that encryption schemes were designed and tested by experienced specialists.

(5) Recovery : Customers don't know where their data is hosted, a cloud provider should tell them what will happen to their data in case of disaster.

Advice : Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

(6) Investigative support : Investigating inappropriate or illegal activity may be impossible in cloud computing. because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.

(7) Long-term viability : Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event.

Advice: Ask potential providers how you would get your data back and in what format.

Refrences:

www.google.com

www.wikipedia.com