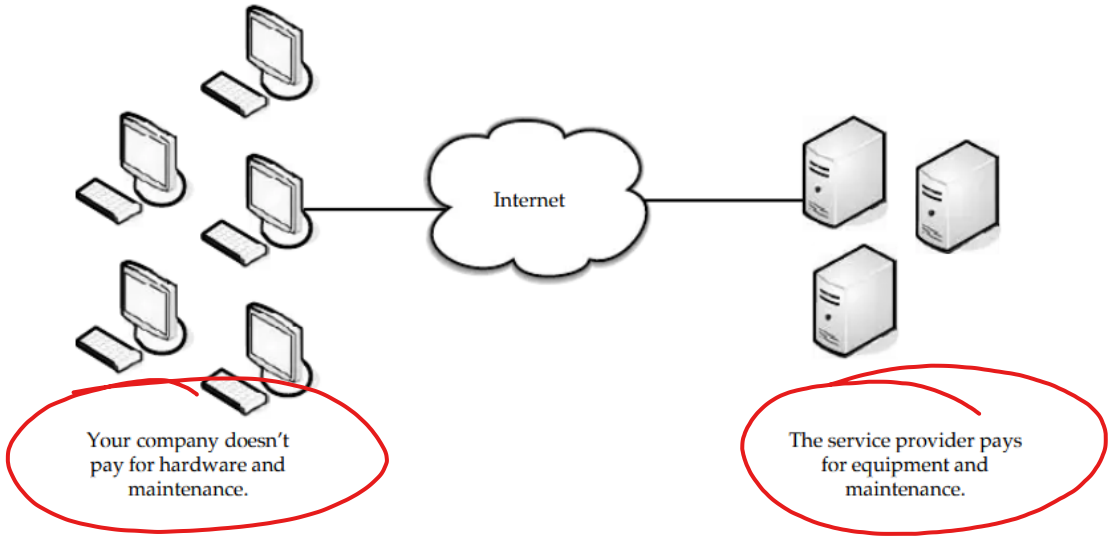
Introduction to Cloud Computing

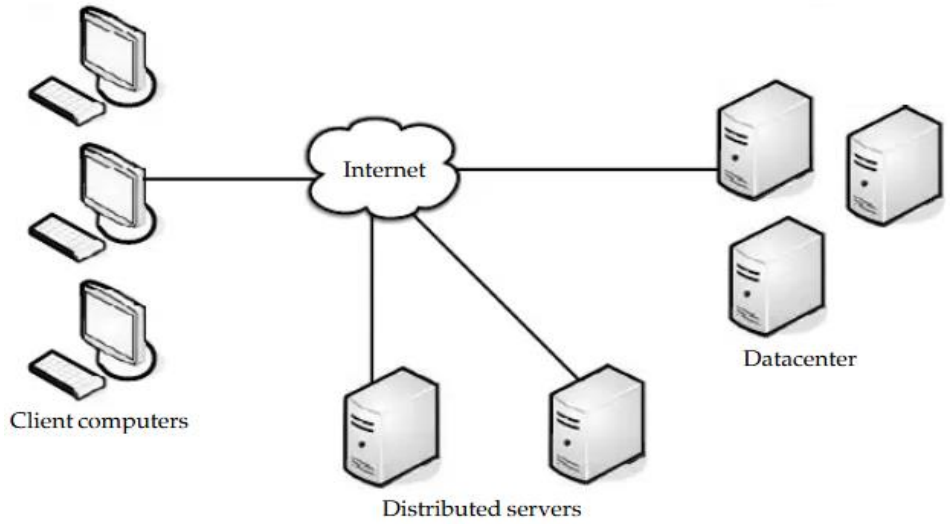
- What is cloud computing?
  - Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources like processing servers, storage, networks, applications and services
  - It promises to cut capital/operational expenditures of companies and to let them focus on strategic projects instead of keeping their datacenter running



Introduction to Cloud Computing

2

- Components of cloud computing
  - Cloud computing solution made up of several elements: clients, datacenters and distributed servers



  - Each element has a purpose and plays a specific role in delivering a functional cloud-based application

Components of Cloud Computing

- Clients
  - Clients are devices that end-users interact with to manage their information on the cloud (typically served by cloud)
  - Mobile clients: Include smartphones and PDAs
  - Thin clients: Clients are computers that do not have internal hard drives (rather let the server do all the work) but then display the information
  - Thick clients: Include regular computers (that may use a web browser like Firefox to connect to the cloud)

Components of Cloud Computing

- Datacenter
  - Datacenter is a collection of servers where the subscribed application is housed (may be accessed via Internet)
  - A growing trend in the IT world is **virtualizing** servers
  - One can have multiple **virtual** servers running on one physical server
  - Software is installed allowing multiple instances of virtual servers to be used

Components of Cloud Computing

- Distributed servers
  - Distributed servers are installed in geographically disparate locations
  - To cloud subscriber, these servers act as if they are right next to each other
  - Distributed environment gives service provider more flexibility and security
  - For instance, Amazon has their cloud solution in servers spread across globe
  - Avoiding single point of failure, achieving scalability

Deployment Models of Cloud

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

Public Cloud

- Cloud infrastructure is provisioned for open use by general public
- May be owned, managed, and operated by a business, academic, or government organization, or some combination of them
- Exists on the premises of the cloud provider
- Examples
  - Google App Engine
  - Microsoft Windows Azure
  - IBM Smart Cloud
  - Amazon EC2

Public Cloud

- Provider's computing and storage resources are potentially large
- Communication links can be assumed to be implemented over the public Internet
- Cloud serves a diverse pool of clients (and possibly attackers)

Public Cloud

- Workload locations hidden from clients
  - In the public scenario, a provider may migrate a subscriber's workload, whether processing or data, at any time
  - Workload can be transferred to datacenters where cost is low
  - Workloads in a public cloud may be relocated anywhere at any time unless the provider has offered (optional) location restriction policies

- Risks from multi-tenancy
  - A single machine may be shared by the workloads of any combination of subscribers (a subscriber's workload may be co-resident with the workloads of competitors or adversaries)
  - Introduces both reliability and security risk

Public Cloud

- Network dependency
  - Subscribers connect to providers via the public Internet
  - Connection depends on Internet's Infrastructure like
    - Domain Name System (DNS) servers
    - Router infrastructure
    - Inter-router links
- Limited visibility and control over data (security and privacy concerns)
  - Details of provider system operation are usually considered proprietary information and are not shared with subscribers
  - In many cases, the software employed by a provider is usually proprietary and not available for examination by subscribers
  - A subscriber cannot verify that data has been completely deleted from a provider's systems

Public Cloud

- Elasticity: Illusion of unlimited resource availability
  - Public clouds are generally “unrestricted” in their location or size
  - Public clouds potentially have high degree of flexibility in the movement of subscriber workloads to correspond with available resources
- Low up-front costs to migrate into the cloud
- Restrictive default service-level agreements (SLAs)
  - Default SLAs of public clouds specify limited promises that providers make to their subscribers

Private Cloud

- Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., units/users)
- May be owned, managed, and operated by the organization, a third party, or some combination of them
- May be on- or off-premises
- Examples
  - Eucalyptus
  - Ubuntu Enterprise Cloud (UEC)
  - Amazon VPC (Virtual Private Cloud)
  - VMware Cloud Infrastructure Suite
  - Microsoft ECI datacenter

Private Cloud

- Private cloud may exist off premises and can be managed by a third party

- On-site Private Cloud
  - Applies to private clouds implemented at a customer's premises

- Outsourced Private Cloud
  - Applies to private clouds where the server side is outsourced to a hosting company

14

On-site Private Cloud

- The security perimeter extends around both the subscriber's on-site resources and the private cloud's resources

- Security perimeter does not guarantee control over the private cloud's resources but subscriber can exercise control over the resources

On-site Private Cloud

- Network dependency

- Subscribers still need IT skills
  - Subscriber organizations will need the traditional IT skills required to manage user devices that access the private cloud, and will require cloud IT skills as well

- Workload locations are hidden from clients
  - To manage a cloud's hardware resources, a private cloud must be able to migrate workloads between machines without inconveniencing clients
  - With an on-site private cloud, a subscriber organization chooses the physical infrastructure, but individual clients still may not know where their workloads physically exist within the subscriber organization's infrastructure

16

On-site Private Cloud

- Risks from multi-tenancy
  - Workloads of different clients may reside concurrently on the same systems and local networks, separated only by access policies implemented by a cloud provider's software
  - A flaw in the software/policies can compromise the security of a subscriber organization by exposing client workloads to one another
- Data import/export and performance limitations
  - On-demand bulk data import/export is limited by the on-site private cloud's network capacity, and real-time/critical processing may be problematic because of networking limitations

On-site Private Cloud

- Potentially strong security from external threats
  - In an on-site private cloud, a subscriber has the option of implementing an appropriately strong security perimeter to protect private cloud resources against external threats to the same level of security as can be achieved for non-cloud resources
- Significant-to-high up-front costs to migrate into the cloud
  - An on-site private cloud requires cloud-management software be installed on computer systems within a subscriber organization
  - If the cloud is intended to support process- or data-intensive workloads, the software will need to be installed on numerous commodity systems or on a more limited number of high-performance systems
  - Installing cloud software and managing the installations will incur significant up-front costs, even if the cloud software itself is free, and even if much of the hardware already exists within a subscriber organization

On-site Private Cloud

- Limited resources: An on-site private cloud, at any specific time, has a fixed computing and storage capacity that has been sized to correspond to anticipated workloads and cost restrictions

19

Outsourced Private Cloud

- Outsourced private cloud has two security perimeters, one implemented by a cloud subscriber and one implemented by a provider

- Two security perimeters are joined by a protected communication link

- Security of data and processing conducted in the outsourced private cloud depends on the strength and availability of both security perimeters and of the protected communication link

Outsourced Private Cloud

- Network dependency
  - In the outsourced private scenario, subscribers may have an option to provision unique protected and reliable communication links with the provider
- Workload locations are hidden from clients
- Risks from multi-tenancy
  - The implications are same as those for an on-site private cloud

Outsourced Private Cloud

- Data import/export and performance limitations
  - On-demand bulk data import/export is limited by the network capacity between a provider and subscriber, and real-time or critical processing may be problematic because of networking limitations
  - In the outsourced private cloud scenario, these limits may be adjusted, although not eliminated, by provisioning high-performance and/or high-reliability networking between the provider and subscriber
- Potentially strong security from external threats
  - As with the on-site private cloud scenario, a variety of techniques exist to harden a security perimeter
  - The main difference is that the techniques need to be applied both to a subscriber's perimeter and provider's perimeter, and that the communication link needs to be protected

Outsourced Private Cloud

- Modest-to-significant up-front costs to migrate into the cloud
  - Resources are provisioned by the provider
  - Main start-up costs for the subscriber relate to:
    - Negotiating the terms of the service level agreement (SLA)
    - Possibly upgrading the subscriber's network to connect to the outsourced private cloud
    - Switching from traditional applications to cloud-hosted applications
    - Porting existing non-cloud operations to the cloud
    - Training
- Extensive resources available
  - A subscriber can rent resources in any quantity offered by the provider
  - Provisioning and operating computing-equipment at a huge scale is a core competency of providers

Community Cloud

- Cloud infrastructure provisioned for exclusive use by a specific community of consumers
- These consumers belong to organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations)
- Cloud may be owned, managed, and operated by one or more of the organizations in community, or a third party, or some combination of them
- May be on- or off-premises
- Examples
  - Google Apps for Government
  - Microsoft Government Community Cloud

On-site Community Cloud

- Community cloud is made up of a set of participant organizations
- Each participant organization may provide cloud services, consume cloud services, or both
- At least one organization must provide cloud services
- Each organization implements a security perimeter

On-site Community Cloud

- The participant organizations are connected via links between the boundary controllers that allow access through their security perimeters

- Access policy of a community cloud may be complex
  - If there are *N* community members, a decision must be made, either implicitly or explicitly, on how to share a member's local cloud resources with each of the other members

  - Policy specification techniques like role-based access control, attribute-based access control can be used to express sharing policies

On-site Community Cloud

- Network dependency
  - Subscribers in an on-site community cloud need to either provision controlled inter-site communication links or use a secure channel over a less controlled communications media (such as the public Internet)
  - Reliability and security of the community cloud depends mainly on the reliability and security of the communication links
- Subscribers still need IT skills
  - Organizations in the community, which provide cloud resources, require IT skills similar to those required for the on-site private cloud scenario except that the overall cloud configuration may be more complex and hence require a higher skill level
  - Identity- and access-control configurations among participant organizations may be complex

On-site Community Cloud

- Workload locations are hidden from clients
  - Participant organizations providing cloud services to the community cloud may wish to employ an outsourced private cloud as a part of its implementation strategy

- Data import/export and performance limitations
  - The communication links between various participant organizations in a community cloud can be provisioned to various levels of performance, security and reliability, based on the needs of the participant organizations

  - The network-based limitations are similar to those of the outsourced-private cloud scenario

On-site Community Cloud

- Highly variable up-front costs to migrate into the cloud
  - The up-front costs of an on-site community cloud for a participant organization depend greatly on whether the organization plans to consume cloud services only or also to provide cloud services
  - For a participant organization, that intends to provide cloud services within the community cloud, the costs appear to be similar to those for the on-site private cloud scenario (i.e., significant-to-high)

Outsourced Community Cloud

- Network dependency
  - Similar to that of the outsourced private cloud
  - The primary difference is that multiple protected communications links are likely from the community members to the provider's facility
- Workload locations are hidden from clients
  - Same as outsourced private cloud
- Risks from multi-tenancy
  - Same as on-site community cloud

Outsourced Community Cloud

- Data import/export and performance limitations
  - Same as outsourced private cloud
- Potentially strong security from external threats
  - Same as on-site community cloud
- Modest-to-significant up-front costs to migrate into the cloud
  - Same as outsourced private cloud
- Extensive resources available
  - Same as outsourced private cloud

Hybrid Cloud

- The cloud infrastructure is a composition of two or more distinct cloud infrastructures (i.e., private, community and/or public) which remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability

- Examples
  - Windows Azure
  - VMware vCloud

Hybrid Cloud

- A hybrid cloud is composed of two or more private, community and/or public clouds
- Significant variations in performance, reliability and security depending upon the type of clouds chosen to build hybrid cloud
- A hybrid cloud can be extremely complex – may change over time with constituent clouds joining and leaving

Cloud-service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Cloud-service Models

- Software as a Service (SaaS)
  - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure
  - The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface
  - The consumer 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 user-specific application configuration settings
  - Example: Google Spread Sheet

Cloud-service Models

- Platform as a Service (PaaS)
  - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider
  - The consumer 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 configuration settings for the application-hosting environment
  - Example: Google App Engine

Cloud-service Models

- Infrastructure as a Service (IaaS)
  - The capability provided to provision processing, storage, networks and other fundamental computing resources
  - Consumer can deploy and run arbitrary software
  - Example: Amazon Web Services

Benefits of Cloud Computing

- Scalability
  - If you, as a subscriber, are anticipating a huge upswing in computing need (or even if you are surprised by a sudden demand), cloud computing can help you manage
  - Rather than having to buy, install, and configure new equipment, you can buy additional CPU cycles or storage from a third party
  - Since your costs are based on consumption, you likely wouldn't have to pay out as much as if you had to buy the equipment
  - Once you have fulfilled your need for additional equipment, you just stop using the cloud provider's services, and you don't have to deal with unneeded equipment
  - You simply add or subtract based on your organization's need

Benefits of Cloud Computing

- Simplicity
  - Not having to buy and configure new equipment allows you and your IT staff to get right to your business
  - The cloud solution makes it possible to get your application started immediately, and it costs a fraction of what it would cost to implement an on-site solution

Benefits of Cloud Computing

- Knowledgeable vendors
  - Typically, when new technology becomes popular, there are plenty of vendors who pop up to offer their version of that technology
  - This isn't always good, because a lot of those vendors tend to offer less than useful technology
  - By contrast, the first comers to the cloud computing party are actually very reputable companies
  - Companies like Amazon, Google, Microsoft, IBM, and Yahoo! have been good vendors because they have offered reliable service, plenty of capacity, and you get some brand familiarity with these well-known names

Benefits of Cloud Computing

- More internal resources
  - By shifting your non-mission-critical data needs to a third party, your IT department is freed up to work on important, business-related tasks
  - You also don’t have to add more manpower and training that stem from having to deal with these low-level tasks
  - Also, since network outages are a nightmare for the IT staff, this burden is offloaded onto the service provider
  - Outages may still happen, but let Amazon worry about getting the service back online

41

Benefits of Cloud Computing

- Security
  - There are plenty of security risks when using a cloud vendor, but reputable companies strive to keep you safe and secure
  - Vendors have strict privacy policies and employ stringent security measures, like proven cryptographic methods to authenticate users
  - Further, you can always encrypt your data before storing it on a provider's cloud
  - In some cases, between your encryption and the vendor's security measures, your data may be more secure than if it were stored in-house

Limitations of Cloud Computing

- Leakage of sensitive/confidential information/data

Limitations of Cloud Computing

- Classification of data
  - Public data
    - Information that is similar to unclassified information
    - All of a company's information that does not fit into any of the next categories can be considered public
    - While its unauthorized disclosure may be against policy, it is not expected to impact seriously or adversely the organization, its employees, and/or its customers

Limitations of Cloud Computing

- Classification of data
  - Private data
    - This classification applies to personal information that is intended for use within the organization
    - Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees
    - For example, salary levels and medical information are considered private

Limitations of Cloud Computing

- Classification of data
  - Sensitive data
    - Information that requires a higher level of classification than normal data
    - This information is protected from a loss of confidentiality as well as from a loss of integrity due to an unauthorized alteration
    - This classification applies to information that requires special precautions to ensure its integrity by protecting it from unauthorized modification or deletion
    - It is information that requires a higher-than-normal assurance of accuracy and completeness

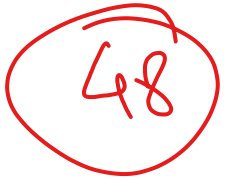
Limitations of Cloud Computing

- Classification of data
  - Confidential data
    - This classification applies to the most sensitive business information that is intended strictly for use within the organization
    - Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners, and/or its customers
    - This information is exempt from disclosure under the provisions of applicable federal laws or regulations
    - For example, information about new product development, trade secrets, and merger negotiations is considered confidential

47

Limitations of Cloud Computing

- Leakage of sensitive/confidential information/data
  - It's much complicated a task to sort out how sensitive/confidential information stored on a cloud is genuinely secured
  - Also, the door is wide open for government investigators to subpoena that information
  - It has become much easier for the government to get information from third parties than from a privately owned server
  - Google's policy states that the company will share data with the government if it has a "good faith belief" that access is necessary to fulfill lawful requests
  - Less scrupulous service providers might share that data with a marketing firm



Limitations of Cloud Computing

- Applications not ready
  - An application might require a lot of bandwidth to communicate with users – it might turn out to be *less* expensive in the *long run* to simply house the application locally
  - The application might also take a lot of effort to integrate with your other applications
  - If the application has to talk with an on-site database, it may be better to also have the application hosted locally until you move the entire infrastructure to the cloud
  - It may be the case that you need a very specific application and you'll have to commission its development yourself