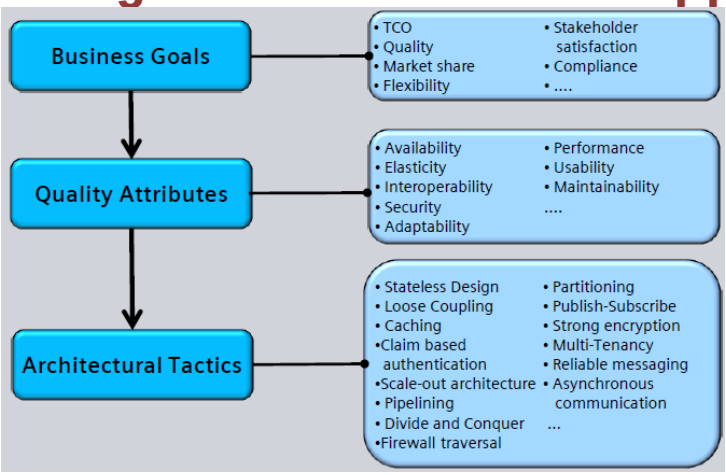
CLOUD COMPUTING

CLOUD COMPUTING ARCHITECTURE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

Context: High Level Architectural Approach



Source: http://www.sei.cmu.edu/library/assets/presentations/Cloud%20Computing%20Architecture%20-%20Gerald%20Kaefer.pdf

2

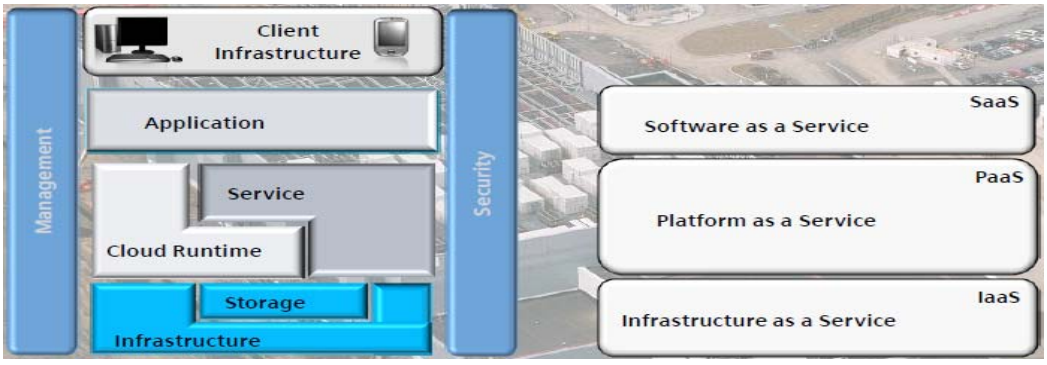
Major building blocks of Cloud Computing Architecture

- **Technical Architecture:**
  - Structuring according to XaaS stack
  - Adopting cloud computing paradigms
  - Structuring cloud services and cloud components
  - Showing relationships and external endpoints
  - Middleware and communication
  - Management and security
- **Deployment Operation Architecture:**
  - Geo-location check (Legal issues, export control)
  - Operation and Monitoring

Ref: http://www.sei.cmu.edu/library/assets/presentations/Cloud%20Computing%20Architecture%20-%20Gerald%20Kaefer.pdf

3

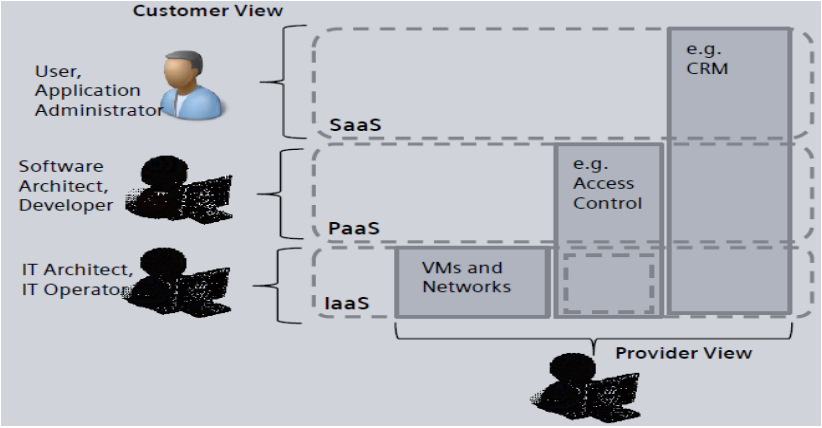
Cloud Computing Architecture - XaaS



Source: http://www.sei.cmu.edu/library/assets/presentations/Cloud%20Computing%20Architecture%20-%20Gerald%20Kaefer.pdf

4

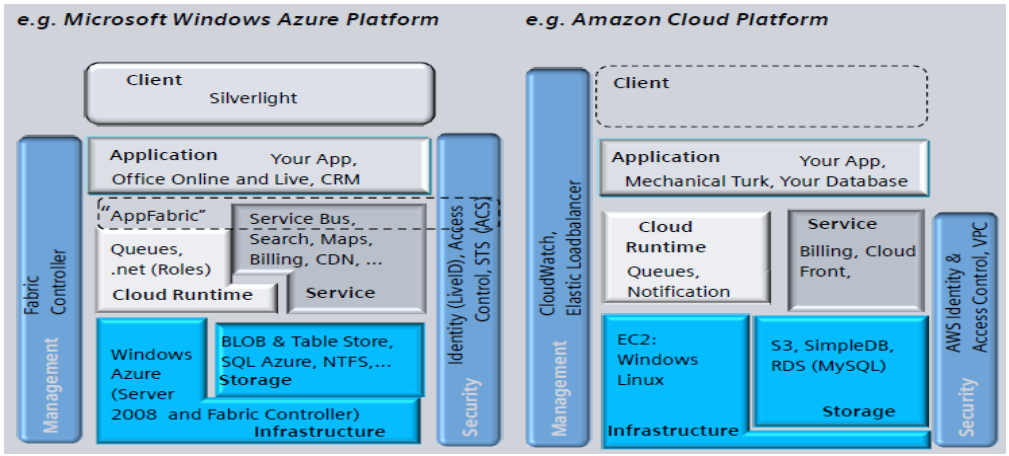
XaaS Stack views: Customer view vs Provider view



Source: http://www.sei.cmu.edu/library/assets/presentations/Cloud%20Computing%20Architecture%20-%20Gerald%20Kaefer.pdf

5

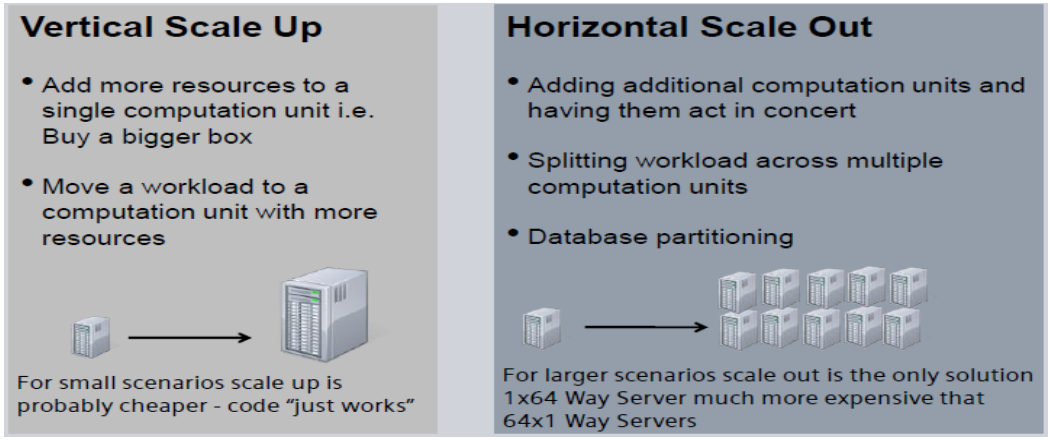
Microsoft Azure *vs* Amazon EC2



Source: http://www.sei.cmu.edu/library/assets/presentations/Cloud%20Computing%20Architecture%20-%20Gerald%20Kaefer.pdf

6

Architecture for elasticity



Source: http://www.sei.cmu.edu/library/assets/presentations/Cloud%20Computing%20Architecture%20-%20Gerald%20Kaefer.pdf

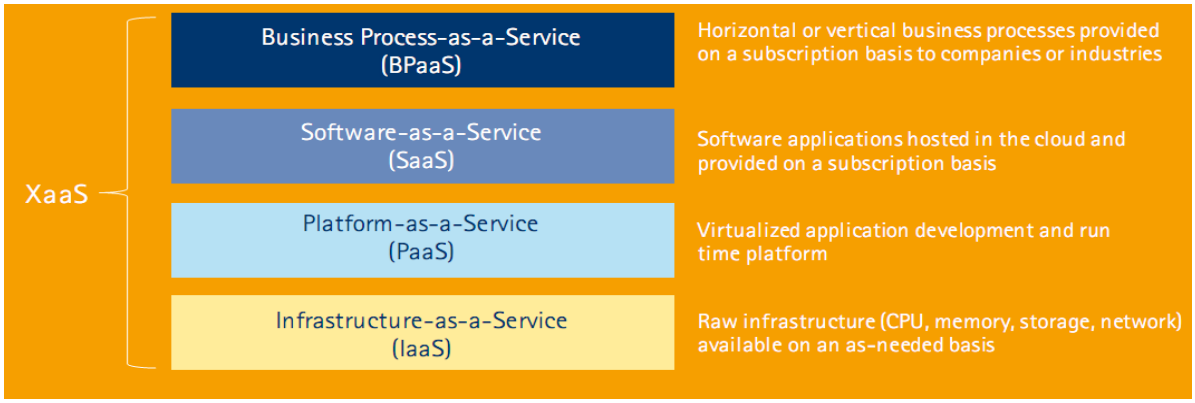
7

Service Models (XaaS)

- Combination of Service-Oriented Infrastructure (SOI) and cloud computing realizes to XaaS.
- X as a Service (XaaS) is a generalization for cloud-related services
- XaaS stands for "anything as a service" or "everything as a service"
- XaaS refers to an increasing number of services that are delivered over the Internet rather than provided locally or on-site
- XaaS is the essence of cloud computing.

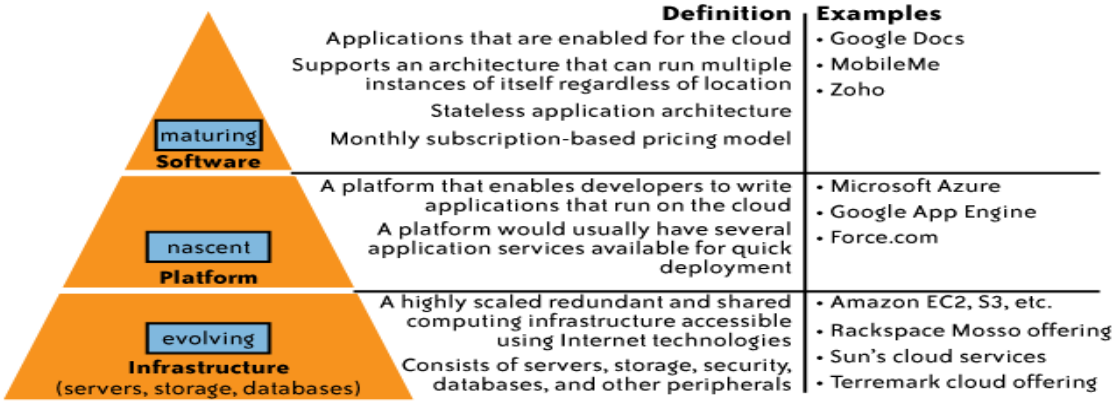
8

Service Models (XaaS)



9

Service Models (XaaS)



Source: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather and Subra Kumaraswamy

10

Service Models (XaaS)

- **Most common examples of XaaS are**
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)

- **Other examples of XaaS include**
  - Business Process as a Service (BPaaS)
  - Storage as a service (another SaaS)
  - Security as a service (SECaaS)
  - Database as a service (DaaS)
  - Monitoring/management as a service (MaaS)
  - Communications, content and computing as a service (CaaS)
  - Identity as a service (IDaaS)
  - Backup as a service (BaaS)
  - Desktop as a service (DaaS)

11

Requirements of CSP (Cloud Service Provider)

- Increase productivity
- Increase end user satisfaction
- Increase innovation
- Increase agility

12

Service Models (XaaS)

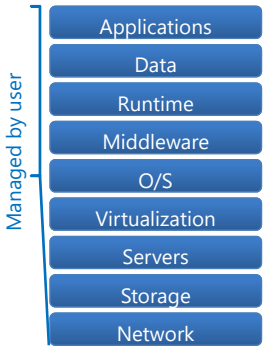
- Broad network access (cloud) + resource pooling (cloud) + business-driven infrastructure on-demand (SOI) + service-orientation (SOI) = **XaaS**
- Xaas fulfils all the 4 demands!

Source: Understanding the Cloud Computing Stack: PaaS, SaaS, IaaS © Diversity Limited, 2011

13

Classical Service Model

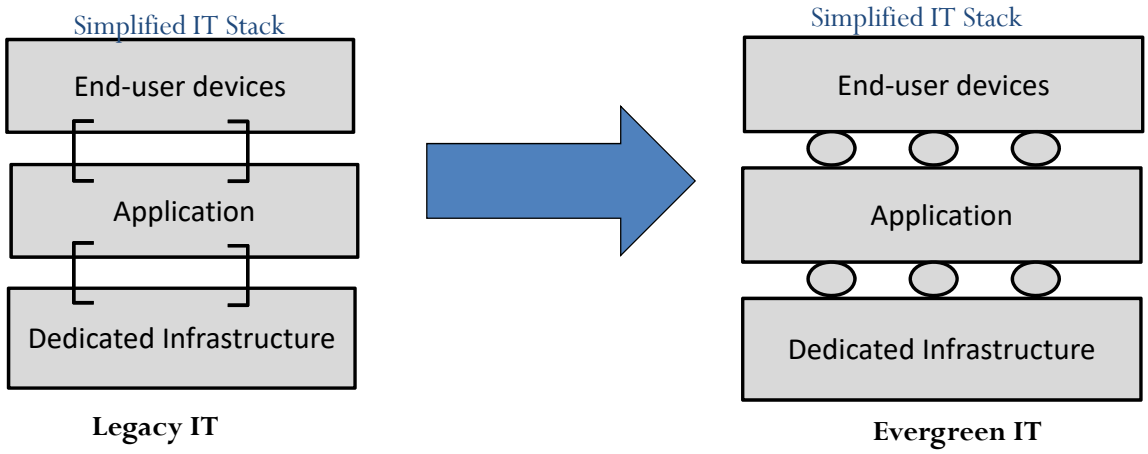
- All the Layers(H/W, Operating System, Development Tools, Applications) Managed by the Users
- Initial IT budget and resources.
- Users bears the costs of the hardware, maintenance and technology.
- Each system is designed and funded for a specific business activity: custom build-to-order
- Systems are deployed as a vertical stack of "layers" which are tightly coupled, so no single part can be easily replaced or changed
- Prevalent of manual operations for provisioning, management
- Result: Legacy IT



Source: Dragan , "XaaS as a Modern Infrastructure for eGoverement Busines Model in the Republic of Croatia"

14

Key impact of cloud computing for IT function: From Legacy IT to Evergreen IT



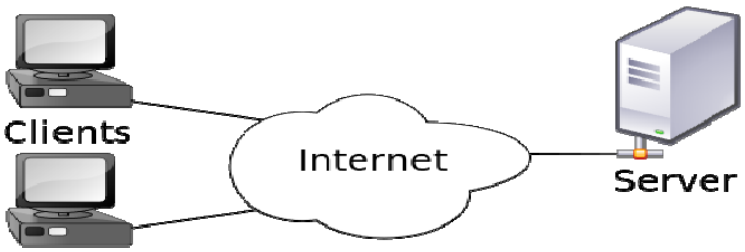
15

Classic Model vs. XaaS

		Business Model	Definition/Example
Traditional	1	Licensed Software	Traditional Software Licenses (w/ upgrade + maintenance) Examples: Oracle; SAP, Microsoft
	2	Hardware Product	Hardware Product sale (e.g. PC, Server, Router) plus maintenance / support services Examples: Cisco, Dell, HP
	3	People-based Services	Professional Services Examples: IBM Global Services, Accenture, Wipro
New/ Emerging	4	SaaS	Software functionality delivered as utility services Examples: Salesforce.com; Taleo; Workday; NetSuite
	5	IaaS	Storage-on-demand, compute capacity Examples: eVault; Amazon EC2; Dropbox
	6	PaaS	Provide entire web services dev. environment/ platform Examples: Force.com; Azure; Amazon Web Services

16

Client Server Architecture



Source: Wikipedia

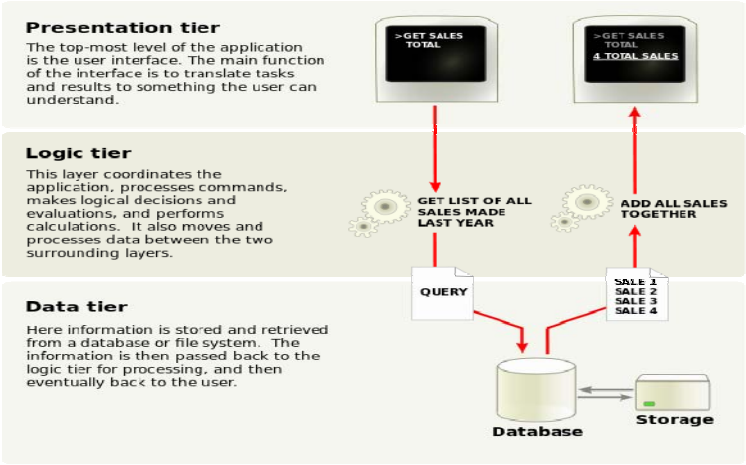
17

Client Server Architecture

- Consists of one or more load balanced servers servicing requests sent by the clients
- Clients and servers exchange message in request-response fashion
- Client is often a thin client or a machine with low computational capabilities
- Server could be a load balanced cluster or a stand alone machine.

18

Three-Tier Client-Server Architecture



Source: Wikipedia

19

Client Server model vs. Cloud model

Client server model

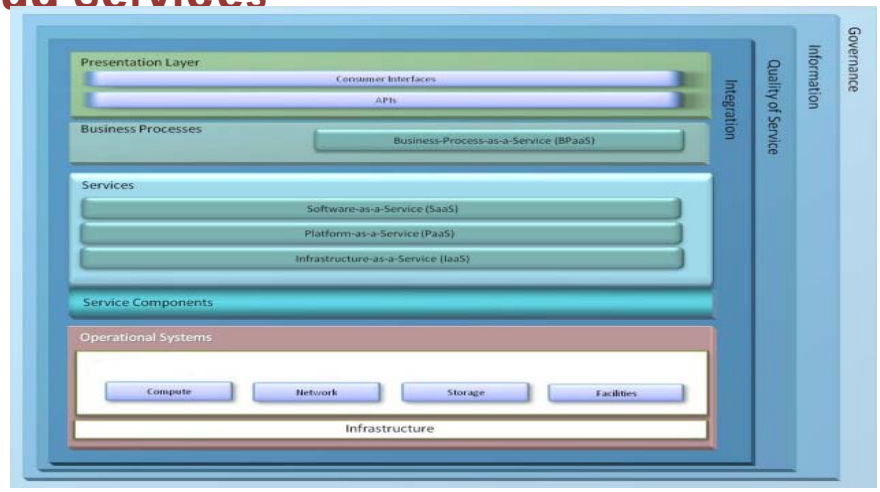
- Simple service model where server services client requests
- May/may not be load balanced
- Scalable to some extent in a cluster environment.
- No concept of virtualization

Cloud computing model

- Variety of complex service models, such as, IaaS, PaaS, SaaS can be provided
- Load balanced
- Theoretically infinitely scalable
- Virtualization is the core concept

20

Cloud Services



Source : http://www.opengroup.org/soa/source-book/socci/extend.htm#figure2

21

Cloud service models

Service Class	Main Access & Management Tool	Service content
SaaS	Web Browser	**Cloud Applications** Social networks, Office suites, CRM, Video processing
PaaS	Cloud Development Environment	**Cloud Platform** Programming languages, Frameworks, Mashups editors, Structured data
IaaS	Virtual Infrastructure Manager	**Cloud Infrastructure** Compute Servers, Data Storage, Firewall, Load Balancer

Source: http://www.cs.helsinki.fi/u/epsavola/seminaari/Cloud%20Service%20Models.pdf

22

Simplified description of cloud service models

- **SaaS** applications are designed for end users and are delivered over the web
- **PaaS** is the set of tools and services designed to make coding and deploying applications quickly and efficiently
- **IaaS** is the hardware and software that powers it all – servers, storage, network, operating systems

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

23

Transportation Analogy

- By itself, infrastructure isn't useful – it just sits there waiting for someone to make it productive in solving a particular problem. Imagine the Interstate transportation system in the U.S. Even with all these roads built, they wouldn't be useful without cars and trucks to transport people and goods. In this analogy, the *roads are the infrastructure* and the *cars and trucks are the platform* that sits on top of the infrastructure and transports the people and goods. These *goods and people* might be considered the *software and information in the technical realm*

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

24

Software as a Service

- SaaS is defined as software that is deployed over the internet. With SaaS, a provider licenses an application to customers either as a service on demand, through a subscription, in a "pay-as-you-go" model, or (increasingly) at no charge when there is opportunity to generate revenue from streams other than the user, such as from advertisement or user list sales.

Ref: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

25

SaaS characteristics

- Web access to commercial software
- Software is managed from central location
- Software is delivered in a 'one to many' model
- Users not required to handle software upgrades and patches
- Application Programming Interfaces (API) allow for integration between different pieces of software.

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

26

Applications where SaaS may be useful

- Applications where there is significant interplay between organization and outside world. e.g. email newsletter campaign software
- Applications that have need for web or mobile access. E.g. mobile sales management software
- Software that is only to be used for a short term needs.
- Software where demand spikes significantly. E.g. Tax/Billing software.
- E.g. of SaaS: Sales Force Customer Relationship Management (CRM) software

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

27

Applications where SaaS may not be the best option

- Applications where extremely fast processing of real time data is needed
- Applications where legislation or other regulation does not permit data being hosted externally
- Applications where an existing on-premise solution fulfills all of the organization's needs

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

28

Platform as a Service

- Platform as a Service (PaaS) brings the benefits that SaaS brought for applications, but over to the software development world.
- PaaS can be defined as a computing platform that allows the creation of web applications quickly and easily and without the complexity of buying and maintaining the software and infrastructure underneath it.
- PaaS is analogous to SaaS except that, rather than being software delivered over the web, it is a platform for the creation of software, delivered over the web.

Ref http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

29

Characteristics of PaaS

- Services to develop, test, deploy, host and maintain applications in the same integrated development environment.
- Web based user interface creation tools help to create, modify, test and deploy different UI scenarios.
- Multi-tenant architecture where multiple concurrent users utilize the same development application.
- Built in scalability of deployed software including load balancing and failover.
- Integration with web services and databases via common standards.
- Support for development team collaboration – some PaaS solutions include project planning and communication tools.
- Tools to handle billing and subscription management

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

30

Scenarios where PaaS is useful

- PaaS is especially useful in any situation where multiple developers will be working on a development project or where other external parties need to interact with the development process
- PaaS is useful where developers wish to automate testing and deployment services.
- Popularity of agile software development, a group of software development methodologies based on iterative and incremental development, will also increase the uptake of PaaS as it eases the difficulties around rapid development and iteration of software.
- PaaS Examples: Microsoft Azure, Google App Engine

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

31

Scenarios where PaaS is not ideal

- Where the application needs to be highly portable in terms of where it is hosted.
- Where proprietary languages or approaches would impact on the development process
- Where a proprietary language would hinder later moves to another provider – concerns are raised about vendor lock in
- Where application performance requires customization of the underlying hardware and software

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

32

Infrastructure as a Service

- Infrastructure as a Service (IaaS) is a way of delivering Cloud Computing infrastructure – servers, storage, network and operating systems – as an on-demand service.
- Rather than purchasing servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand.

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

33

Characteristics of IaaS

- Resources are distributed as a service
- Allows for dynamic scaling
- Has a variable cost, utility pricing model
- Generally includes multiple users on a single piece of hardware

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

34

Scenarios where IaaS makes sense

- Where demand is very volatile – any time there are significant spikes and troughs in terms of demand on the infrastructure
- For new organizations without the capital to invest in hardware
- Where the organization is growing rapidly and scaling hardware would be problematic
- Where there is pressure on the organization to limit capital expenditure and to move to operating expenditure
- For specific line of business, trial or temporary infrastructural needs

Ref: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

35

Scenarios where IaaS may not be the best option

- Where regulatory compliance makes the offshoring or outsourcing of data storage and processing difficult
- Where the highest levels of performance are required, and on-premise or dedicated hosted infrastructure has the capacity to meet the organization's needs

Source: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

36

SaaS providers

Provider	Software	Pricing model
Salesforce.com	CRM	Pay per use
Google Gmail	Email	Free
Process Maker Live	Business process management	Pay per use
XDrive	Storage	Subscription
SmugMug	Data sharing	Subscription
OpSource	Billing	Subscription
Appian Anywhere	Business process management	Pay per use
Box.net	Storage	Pay per use
MuxCLoud	Data processing	Pay per use

Source: http://www.cs.helsinki.fi/u/epsavola/seminaari/Cloud%20Service%20Models.pdf

37

Feature comparison of PaaS providers

Provider	Target to Use	Programming language, Frameworks	Programming Models	Persistence options
Aneka	.NET enterprise applications, Web applications	.NET	Threads, Task, MapReduce	Flat files, RDBMS
AppEngine	Web applications	Python, Java	Request-based Web programming	BigTable
Force.com	Enterprise applications	Apex	Workflow, Request-based Web programming, Excel-like formula language	Own object database
Azure	Enterprise applications, Web applications	.NET	Unrestricted	Table/BLOB/queue storage, SQL Services
Heroku	Web applications	Ruby on Rails	Request-based Web programing	PostgreSQL, Amazon RDS
Amazon Elastic MapReduce	Data processing	Hive and Pirg, Cascading, Java, Ruby, Perl, Python, PHP, C++	MapReduce	Amazon S3

Source: http://www.cs.helsinki.fi/u/epsavola/seminaari/Cloud%20Service%20Models.pdf

38

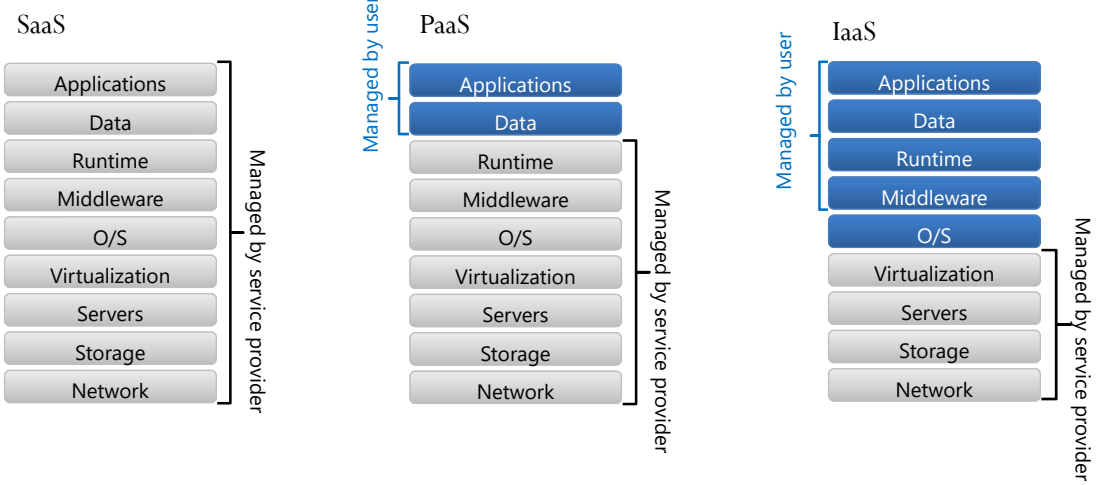
Feature comparison of IaaS providers

Provider	Geographic distribution of data centers	User interfaces and APIs	Hardware capacity	Guest operating systems	Smallest billing unit
Amazon E2C	US Europe	CLI, WS, Portal	CPU: 1_20 EC2 compute units Memory: 1.7-15 GB Storage: 160-1690 GB, 1 GB – 1 TB (per ESB units)	Linux Windows	Hour
Flexiscale	UK	Web console	CPU: 1-4 Memory: 0.5-16 GB Storage: 20-270 GB	Linux, Windows	Hour
GoGrid		REST, Java, PHP, Python, Ruby	CPU: 1-6 Memory: 0.5-8 GB Storage: 30-480 GB	Linux, Windows	Hour
Joyent	US		CPU: 1/16-8 Memory: 0.25-32.5 GB Storage: 5-100GB	OpenSolaris	Month
RackSpace	US	Portal, REST, Python, PHP, Java, .NET	CPU: Quad-core Memory: 0.25-16 GB Storage: 10-620 GB	Linux	Hour

Source: http://www.cs.helsinki.fi/u/epsavola/seminaari/Cloud%20Service%20Models.pdf

39

XaaS



40

Role of Networking in Cloud Computing

- In cloud computing, network resources can be provisioned dynamically.
- Some of the networking concepts that form the core of cloud computing are Virtual Local Area Networks, Virtual Private Networks and the different protocol layers.
- Examples of tools that help in setting up different network topologies and facilitate various network configurations are OpenSSH, OpenVPN etc.

Source: http://www.slideshare.net/alexamies/networking-concepts-and-tools-for-the-cloud

41

Networking in different Cloud Models

OSI Layer	Example Protocols	IaaS	PaaS	SaaS
7 Application	HTTP, FTP, NFS, SMTP, SSH	Consumer	Consumer	Provider
6 Presentation	SSL, TLS	Consumer	Provider	Provider
5 Session	TCP	Consumer	Provider	Provider
4 Transport	TCP	Consumer	Provider	Provider
3 Network	IP, IPSec	Consumer	Provider	Provider
2 Data Link	Ethernet, Fibre channel	Provider	Provider	Provider
1 Physical	Copper, optic fibre	Provider	Provider	Provider

Source: http://www.slideshare.net/alexamies/networking-concepts-and-tools-for-the-cloud

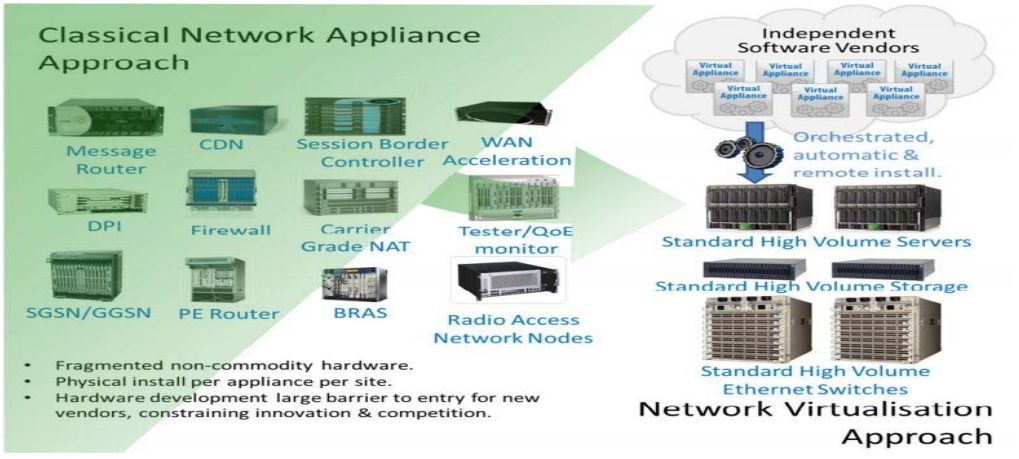
42

Network Function Virtualization

- Network Functions Virtualization aims to transform the way that network operators architect networks by evolving standard IT virtualization technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises.
- It involves the implementation of network functions in software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in, various locations in the network as required, without the need for installation of new equipment.

Ref: https://portal.etsi.org/nfv/nfv_white_paper.pdf

Network Function Virtualization



Source: https://portal.etsi.org/nfv/nfv_white_paper.pdf

Deployment Models

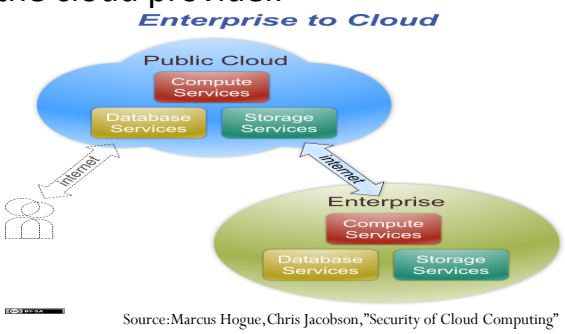
- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

45

Public Cloud

- The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

- Examples of Public Cloud:
- Google App Engine
- Microsoft Windows Azure
- IBM Smart Cloud
- Amazon EC2

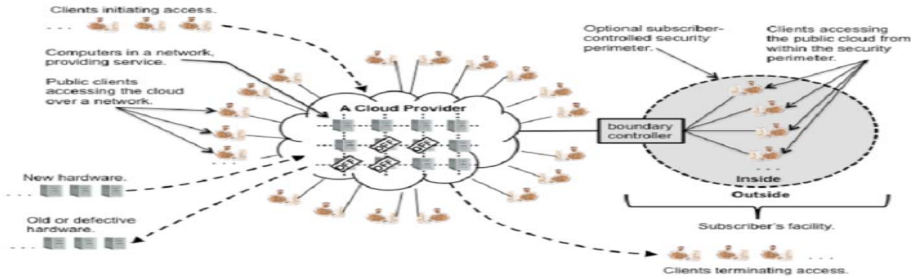


Source:Marcus Hogue,Chris Jacobson,"Security of Cloud Computing"

46

Public Cloud

- In Public setting, the provider's computing and storage resources are potentially large; the communication links can be assumed to be implemented over the public Internet; and the cloud serves a diverse pool of clients (and possibly attackers).



Source: LeeBadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsis and Recommendations "

47

Public Cloud

- **Workload locations are hidden from clients (public):**
  - In the public scenario, a provider may migrate a subscriber's workload, whether processing or data, at any time.
  - Workload can be transferred to data centres 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 (public):**
  - 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

48

Public Cloud

- Organizations considering the use of an on-site private cloud should consider:
  - **Network dependency (public):**
    - 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

49

Public Cloud

- **Limited visibility and control over data regarding security (public):**
  - The details of provider system operation are usually considered proprietary information and are not divulged to 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.
- **Elasticity: illusion of unlimited resource availability (public):**
  - 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.

50

Public Cloud

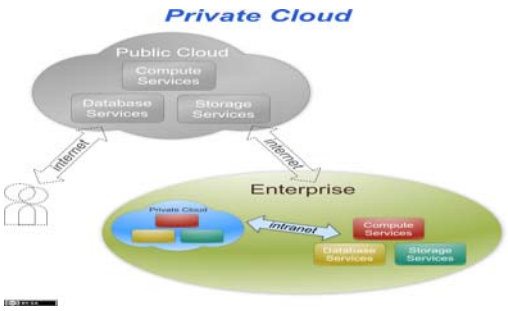
- **Low up-front costs to migrate into the cloud (public)**
- **Restrictive default service level agreements (public):**
  - The default service level agreements of public clouds specify limited promises that providers make to subscribers

51

Private Cloud

- The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

- Examples of Private Cloud:
  - Eucalyptus
  - Ubuntu Enterprise Cloud - UEC
  - Amazon VPC (Virtual Private Cloud)
  - VMware Cloud Infrastructure Suite
  - Microsoft ECI data center.



52

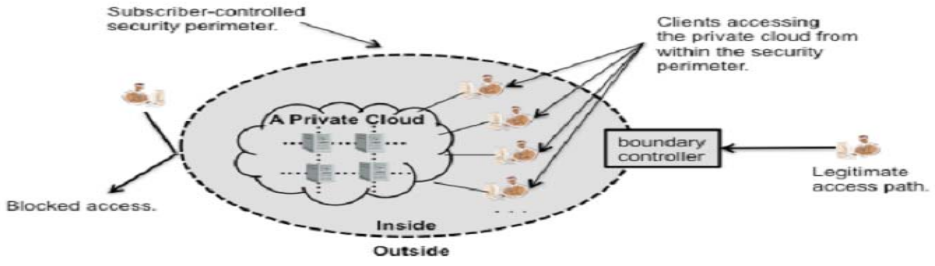
Private Cloud

- Contrary to popular belief, private cloud may exist off premises and can be managed by a third party. Thus, two private cloud scenarios exist, as follows:
- 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.

53

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 guarantees control over the private cloud's resources but subscriber can exercise control over the resources.



Source: LeeBadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsis and Recommendations "

54

On-site Private Cloud

- Organizations considering the use of an on-site private cloud should consider:
  - **Network dependency (on-site-private):**
  - **Subscribers still need IT skills (on-site-private):**
    - 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 (on-site-private):**
    - 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, however, 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

55

On-site Private Cloud

- **Risks from multi-tenancy (on-site-private):**
  - 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 or the policies could compromise the security of a subscriber organization by exposing client workloads to one another
- **Data import/export, and performance limitations (on-site-private):**
  - On-demand bulk data import/export is limited by the on-site private cloud's network capacity, and real-time or critical processing may be problematic because of networking limitations.

56

On-site Private Cloud

- **Potentially strong security from external threats (on-site-private):**
  - 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 (on-site-private):**
  - An on-site private cloud requires that cloud management software be installed on computer systems within a subscriber organization. If the cloud is intended to support process-intensive 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.

57

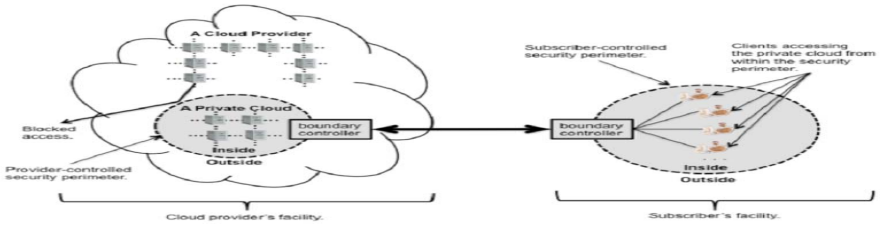
On-site Private Cloud

- **Limited resources (on-site-private):**
  - 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.

58

Outsourced Private Cloud

- Outsourced private cloud has two security perimeters, one implemented by a cloud subscriber (on the right) and one implemented by a provider.
- Two security perimeters are joined by a protected communications link.
- The 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.



59

Outsourced Private Cloud

- Organizations considering the use of an outsourced private cloud should consider:
  - **Network Dependency (outsourced-private):**
    - 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 (outsourced-private):**
  - **Risks from multi-tenancy (outsourced-private):**
    - The implications are the same as those for an on-site private cloud.

60

Outsourced Private Cloud

- **Data import/export, and performance limitations (outsourced-private):**
  - 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, however, 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 (outsourced-private):**
  - As with the on-site private cloud scenario, a variety of techniques exist to harden a security perimeter. The main difference with the outsourced private cloud is that the techniques need to be applied both to a subscriber's perimeter and provider's perimeter, and that the communications link needs to be protected.

61

Outsourced Private Cloud

- **Modest-to-significant up-front costs to migrate into the cloud (outsourced-private):**
  - In the outsourced private cloud scenario, the 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

62

Outsourced Private Cloud

- **Extensive resources available (outsourced-private):**
  - In the case of the outsourced private cloud, a subscriber can rent resources in any quantity offered by the provider. Provisioning and operating computing equipment at scale is a core competency of providers.

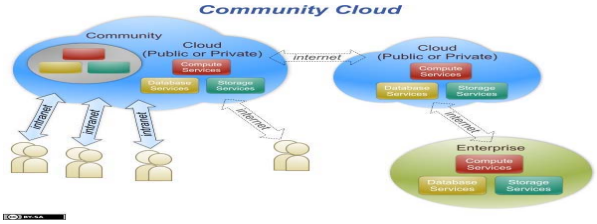
63

Community Cloud

- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community,

  a third party, or some combination of them, and it may exist on or off premises.

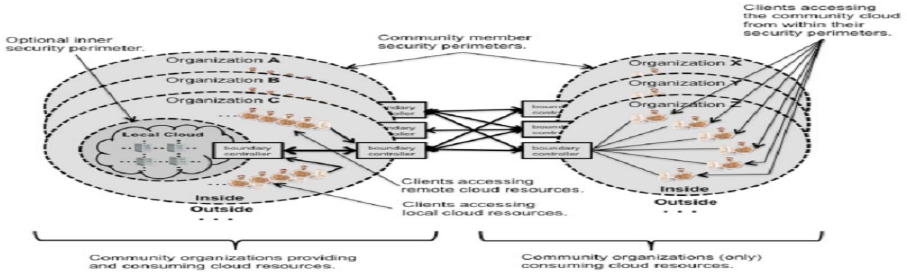
- Examples of Community Cloud:
  - Google Apps for Government
  - Microsoft Government Community Cloud



64

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



Source: LeeBadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsis and Recommendations "

65

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
  - Ex. :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 (RBAC), attribute-based access control can be used to express sharing policies.

66

On-site Community Cloud

- Organizations considering the use of an on-site community cloud should consider:
  - **Network Dependency (on-site community):**
    - The subscribers in an on-site community cloud need to either provision controlled inter-site communication links or use cryptography over a less controlled communications media (such as the public Internet).
    - The reliability and security of the community cloud depends on the reliability and security of the communication links.

67

On-site Community Cloud

- **Subscribers still need IT skills (on-site-community).**
  - Organizations in the community that provides cloud resources, requires 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 the participant organizations may be complex
- **Workload locations are hidden from clients (on-site-community):**
  - Participant Organizations providing cloud services to the community cloud may wish to employ an outsourced private cloud as a part of its implementation strategy.

68

On-site Community Cloud

- **Data import/export, and performance limitations (on-site-community):**
  - The communication links between the 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 thus similar to those of the outsourced-private cloud scenario.
- **Potentially strong security from external threats (on-site-community):**
  - The security of a community cloud from external threats depends on the security of all the security perimeters of the participant organizations and the strength of the communications links. These dependencies are essentially similar to those of the outsourced private cloud scenario, but with possibly more links and security perimeters.

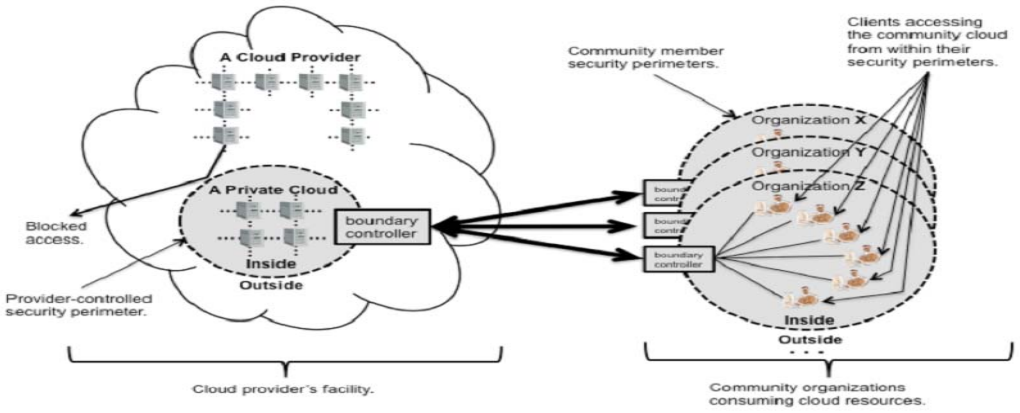
69

On-site Community Cloud

- **Highly variable up-front costs to migrate into the cloud (on-site-community):**
  - 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).

70

Outsourced Community Cloud



Source: LeeBadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsis and Recommendations "

Outsourced Community Cloud

- Organizations considering the use of an on-site community cloud should consider:
- **Network dependency (outsourced-community):**
  - The network dependency of the outsourced community cloud is 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 (outsourced-community).**
  - Same as the outsourced private cloud

Outsourced Community Cloud

- **Risks from multi-tenancy (outsourced-community):**
  - Same as the on-site community cloud
- **Data import/export, and performance limitations (outsourced-community):**
  - Same as outsourced private cloud
- **Potentially strong security from external threats (outsourced-community):**
  - Same as the on-site community cloud
- **Modest-to-significant up-front costs to migrate into the cloud (outsourced-community):**
  - Same as outsourced private cloud

73

Outsourced Community Cloud

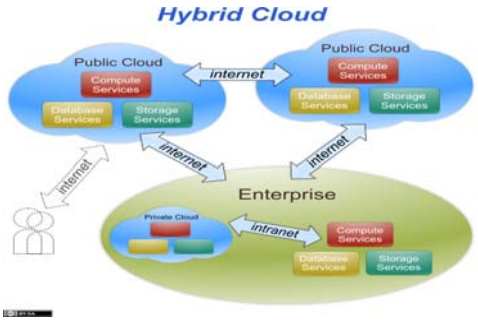
- **Extensive resources available (outsourced-community).**
  - Same as outsourced private cloud

74

Hybrid Cloud

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

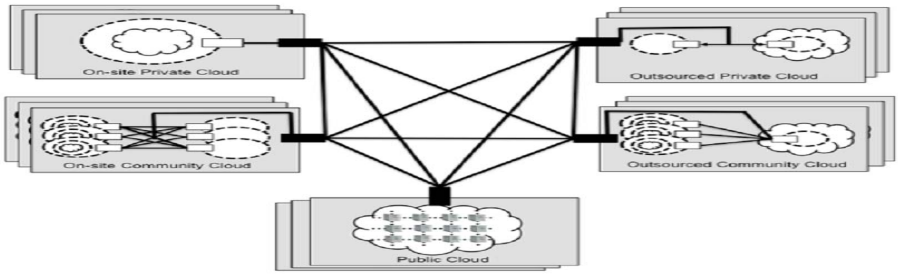
- Examples of Hybrid Cloud:
  - Windows Azure (capable of Hybrid Cloud)
  - VMware vCloud (Hybrid Cloud Services)



75

Hybrid Cloud

- A hybrid cloud is composed of two or more private, community, or public clouds.
- They have significant variations in performance, reliability, and security properties depending upon the type of cloud chosen to build hybrid cloud.



Source: LeeBadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsis and Recommendations "

76

Hybrid Cloud

- A hybrid cloud can be extremely complex
- A hybrid cloud may change over time with constituent clouds joining and leaving.

77

Thank You!

78