

## **Lecture 12**

### **Cloud infrastructures. Types of services. Administration**

# NETWORK ADMINISTRATION

## What is Cloud computing?

**Cloud computing (NIST SP-800-145):** A model for providing ubiquitous, convenient, and unrestricted network access to a shared set of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be quickly provided and released with minimal effort by the service provider. This cloud model promotes availability and consists of five main features, three service models, and four deployment models.

# NETWORK ADMINISTRATION

## Elements of cloud infrastructures

- Remote use of resources (CPU, Storage, Network, Software, Services)

- **Characteristics**

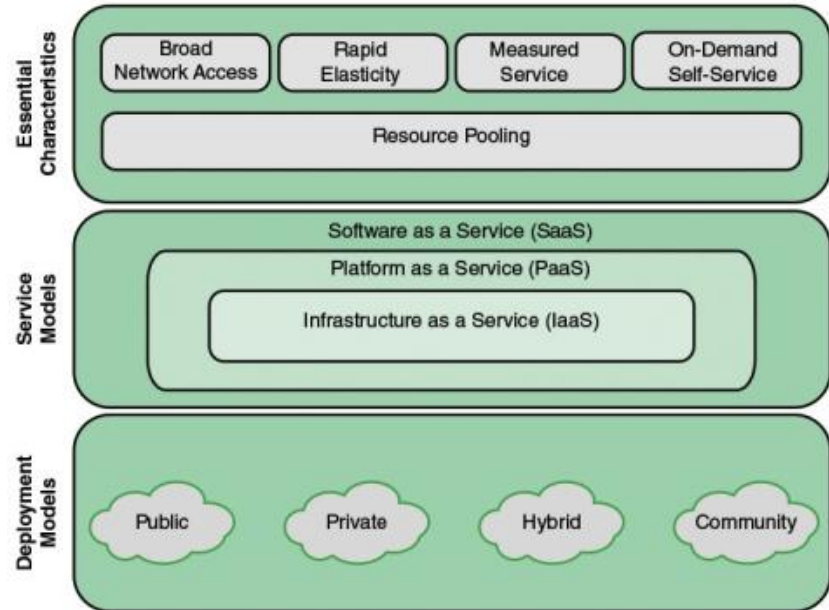
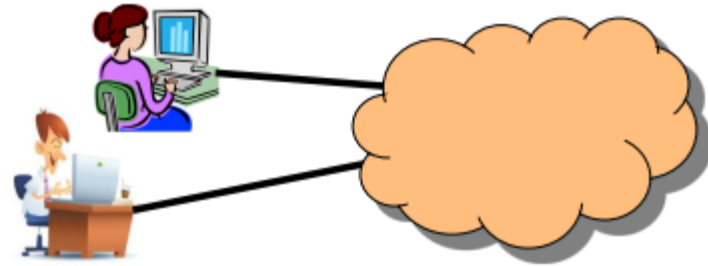
1. Sharing: pooling resources
2. Ubiquity: wide access from the network
3. Rapid deployment
4. Configurable: Measurability of services
5. Self-service on request

- **Service models**

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

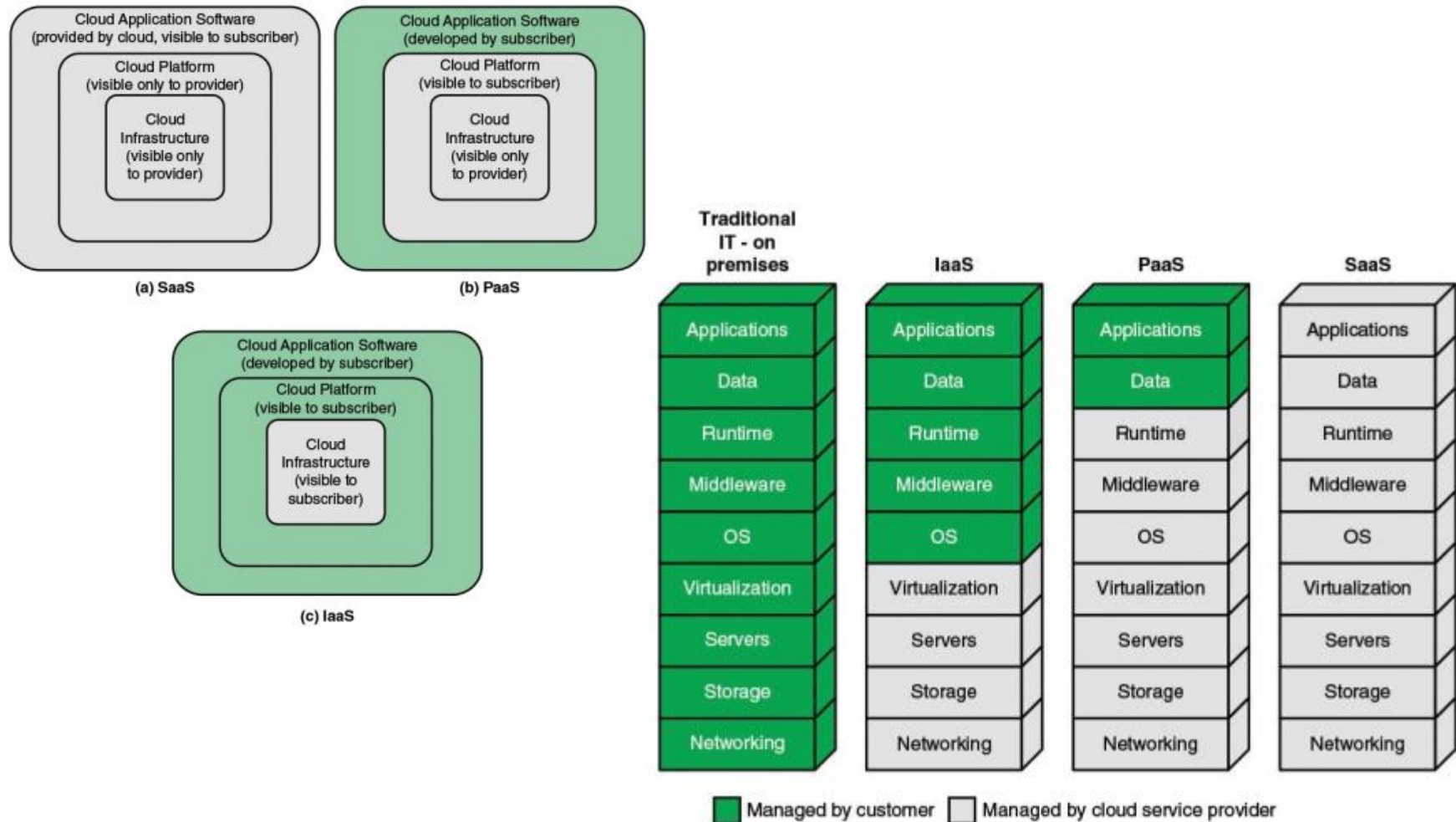
- **Deployment models**

- Public
- Private
- Hybrid
- Community



# NETWORK ADMINISTRATION

## Cloud service models



# NETWORK ADMINISTRATION

## SaaS

- **SaaS** provides customer service in the form of software, in particular application software, that runs and is available in the cloud. SaaS follows the familiar model of web services, in this case applied to cloud resources. SaaS enables the customer to use the cloud provider's applications running on his cloud infrastructure. The applications are accessible from various client devices through a simple interface such as a web browser. Instead of purchasing desktop and server licenses for the software products that the organization uses, it receives the same features when using the service. Using SaaS avoids the complexity of software installation, maintenance, upgrades, and patches. Examples of services at this level are Google Gmail, Microsoft 365, Salesforce, Citrix GoToMeeting and Cisco WebEx.

# NETWORK ADMINISTRATION

## SaaS

- **SaaS** services provide platforms for:
  - ◆ Customer charging
  - ◆ Cooperation - tools for consumer cooperation in working groups
  - ◆ Content Management - Web
  - ◆ Customer Relationship Management (CRM)
  - ◆ Document management
  - ◆ Education
  - ◆ Enterprise resource planning
  - ◆ Finance
  - ◆ Healthcare
  - ◆ Human Resources
  - ◆ Management of IT services
  - ◆ Personal productivity
  - ◆ Project management
  - ◆ Sales
  - ◆ Security
  - ◆ Social media

# NETWORK ADMINISTRATION

## PaaS

**PaaS** provides customer service in the form of a platform on which customer applications can run. PaaS allows the customer to deploy client-created or acquired applications to the cloud infrastructure. PaaS provides useful software building blocks, as well as a number of development tools, such as programming tools, runtime interfaces, and other tools that help deploy new applications. In fact, PaaS is a cloud operating system. PaaS is useful for an organization that wants to develop new or customized applications, while paying for the necessary computer resources only when needed and only as much as needed. AppEngine, Motor Yard, Heroku, Microsoft Azure, Force.com and Apache Stratos are examples of PaaS.

# NETWORK ADMINISTRATION

## PaaS

➤ Examples of **PaaS** services :

- ◆ **Big data as a service** - cloud-based services for analyzing large or complex data sets that require high scalability.
- ◆ **Business intelligence** – Platforms for creating business intelligence applications such as dashboards, reporting systems and large data analysis.
- ◆ **Databases**- These services offer scalable database systems ranging from relational database solutions to mass-scalable non-SQL data.
- ◆ **Development and testing** - These platforms are only for developing and testing application developments that expand and contract as needed..

# NETWORK ADMINISTRATION

## PaaS

➤ Examples of **PaaS** services :

- ◆ **General purpose** - Platforms suitable for developing general purpose applications. These services provide a database, web application execution environment, and typically support web integration services.
- ◆ **Integration** - Application integration services ranging from cloud-to-cloud integration to custom application integration.

# NETWORK ADMINISTRATION

## IaaS

With **IaaS**, the client has access to the resources of the main cloud infrastructure. IaaS provides virtual machines and other abstract hardware and operating systems. IaaS offers the client processing, storage, networking, and other fundamental computing resources so that the client can deploy and manage any software that can include operating systems and applications. IaaS allows customers to combine basic computer services, such as storage systems, to build highly customizable computer systems. Typically, customers are able to provide this infrastructure on their own, using a web-based graphical user interface that serves as a console to manage IT operations for the general environment. API access to the infrastructure can also be offered as an option. Examples of IaaS are Amazon Elastic Compute Cloud (Amazon EC2), Microsoft Windows Azure, Google Compute Engine (GCE) and Rackspace.

# NETWORK ADMINISTRATION

## IaaS

➤ Examples of **IaaS** services :

- ◆ **Backup and recovery** - Platforms providing services for backing up and restoring file systems and storing raw data on servers and desktop systems.
- ◆ **Cloud broker** – Tools that manage services on more than one cloud infrastructure platform. Some tools support private-public cloud configurations.
- ◆ **Content delivery networks** - CDNs store content and files in order to improve the performance and cost of providing content for web-based systems.

# NETWORK ADMINISTRATION

## IaaS

### ➤ Examples of **IaaS** services

- ◆ **Service management** - Services that manage cloud infrastructure platforms. These tools often provide features that cloud providers do not provide or specialize in managing certain application technologies..
- ◆ **Storage** - Provides massively scalable storage capacity that can be used for applications, archiving, backup, file storage, etc..

# NETWORK ADMINISTRATION

## Other cloud services:

- ◆ **Communications as a Service (CaaS)** – Integration of *real-time interaction and collaboration services* to optimize business processes. This service provides a single interface and consistent user operation on different devices. Examples of services include video teleconferencing, web conferencing, instant messaging, and VoIP
- ◆ **Compute as a Service (CompaaS)** - *Providing and using processing resources* required for software implementation and execution. CompaaS can be considered a simplified IaaS, with a focus on providing computing capacity.
- ◆ **Data Storage as a Service (DSaaS)** - *Providing and using a system for data storage and data related capabilities*. DSaaS describes a storage model in which the customer rents storage space from a third-party vendor.

# NETWORK ADMINISTRATION

## Other cloud services:

The data is transferred from the customer to the service provider via the Internet, and the customer then accesses the stored data using the software provided by the service provider. The software is used to perform common storage tasks, such as data archiving and data transfer..

- ◆ **Network as a Service (NaaS)** – service providing transport connectivity and opportunities related to it. NaaS involves optimizing resource allocation by looking at network and computing resources as a whole. NaaS can include a flexible and extended virtual private network (VPN), on-demand bandwidth, custom routing, multicast protocols, firewall, intrusion detection and prevention, WAN, content monitoring and filtering, and antivirus.

# NETWORK ADMINISTRATION

## Other cloud services:

According to the recommendation of ITU Y.3500 (Cloud computing – review and dictionary)

| Cloud service categories    | Cloud capabilities types |          |             |
|-----------------------------|--------------------------|----------|-------------|
|                             | Infrastructure           | Platform | Application |
| Compute as a Service        | X                        |          |             |
| Communications as a Service |                          | X        | X           |
| Data Storage as a Service   | X                        | X        | X           |
| Infrastructure as a Service | X                        |          |             |
| Network as a Service        | X                        | X        | X           |
| Platform as a Service       |                          | X        |             |
| Software as a Service       |                          |          | X           |

# NETWORK ADMINISTRATION

## Other cloud services:

The ITU Y.3500 recommendation also defines :

- ◆ **Database as a Service** - on-demand database where the installation and maintenance of databases is performed by the cloud service provider.
- ◆ **Desktop as a Service** - ability to build, configure, manage, store, perform and remotely assign functions to the user's desktop.
- ◆ **E-mail as a Service** - email that includes related support services, such as storing, receiving, sending, archiving, and retrieving emails.

# NETWORK ADMINISTRATION

## **Other cloud services:**

The ITU Y.3500 recommendation also defines :

- ◆ **Identity as a Service** - Identity and access management (IAM), which can be extended and centralized in existing operating environments. This includes the provisioning, management of directories and the operation of the SSO.

# NETWORK ADMINISTRATION

## Other cloud services:

- ◆ **Management as a Service** - application management, asset and change management, capacity management, problem management (service desk), project portfolio management, service catalog, and service level management.
- ◆ **Security as a Service** - the integration of a set of security services with the existing operating environment by the cloud service provider. This may include authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management.
- ◆ **XaaS**
  - **Anything as a Service** – any service other than the three traditional services
  - **Everything as a Service ???**
  - **X as a Service**

# NETWORK ADMINISTRATION

## Other cloud services:

The ITU Y.3500 recommendation also defines :

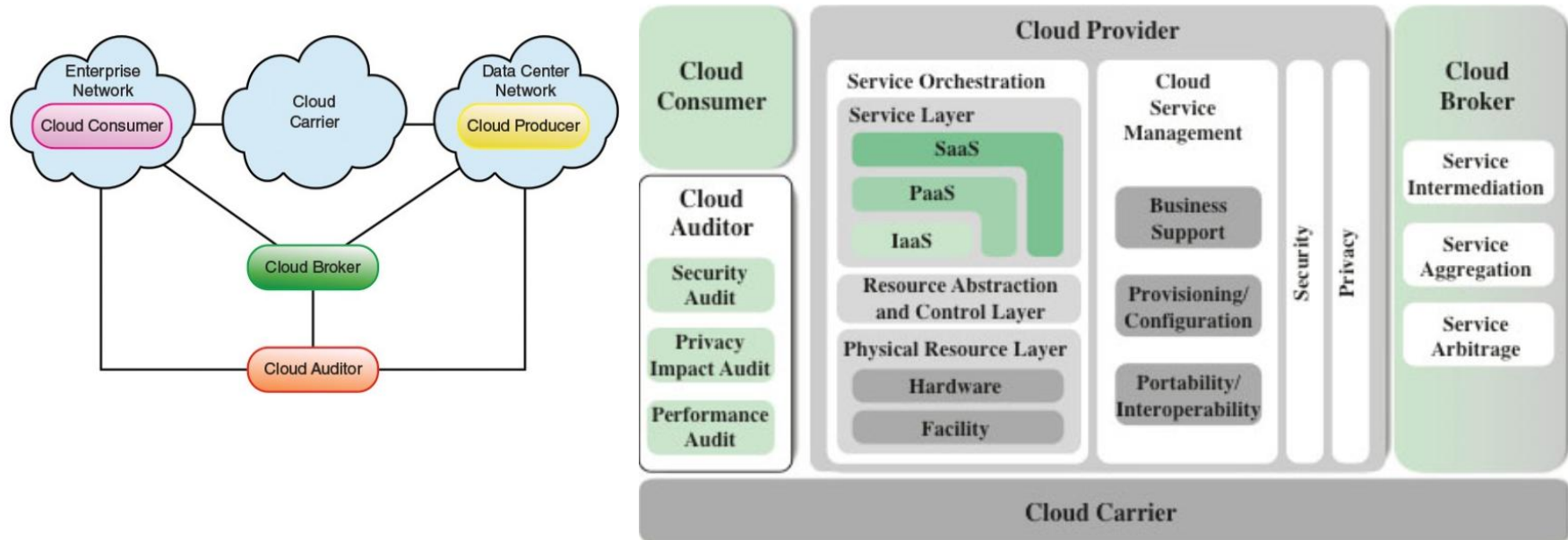
- ◆ **Database as a Service**
- ◆ **Desktop as a Service**
- ◆ **E-mail as a Service**
- ◆ **Identity as a Service**
- ◆ **Management as a Service**
- ◆ **Security as a Service**
- ◆ **XaaS**
  - **Anything as a Service** - any service other than the three traditional services
  - **Everything as a Service ???**
  - **X as a Service**

# NETWORK ADMINISTRATION

## Roles

The following roles can be defined:

- ◆ **Cloud Consumer**
- ◆ **Cloud Service Provider**
- ◆ **Cloud Service Partner:** Cloud Broker & Cloud Auditor
- ◆ **Cloud Carrier: (ISP)**



# NETWORK ADMINISTRATION

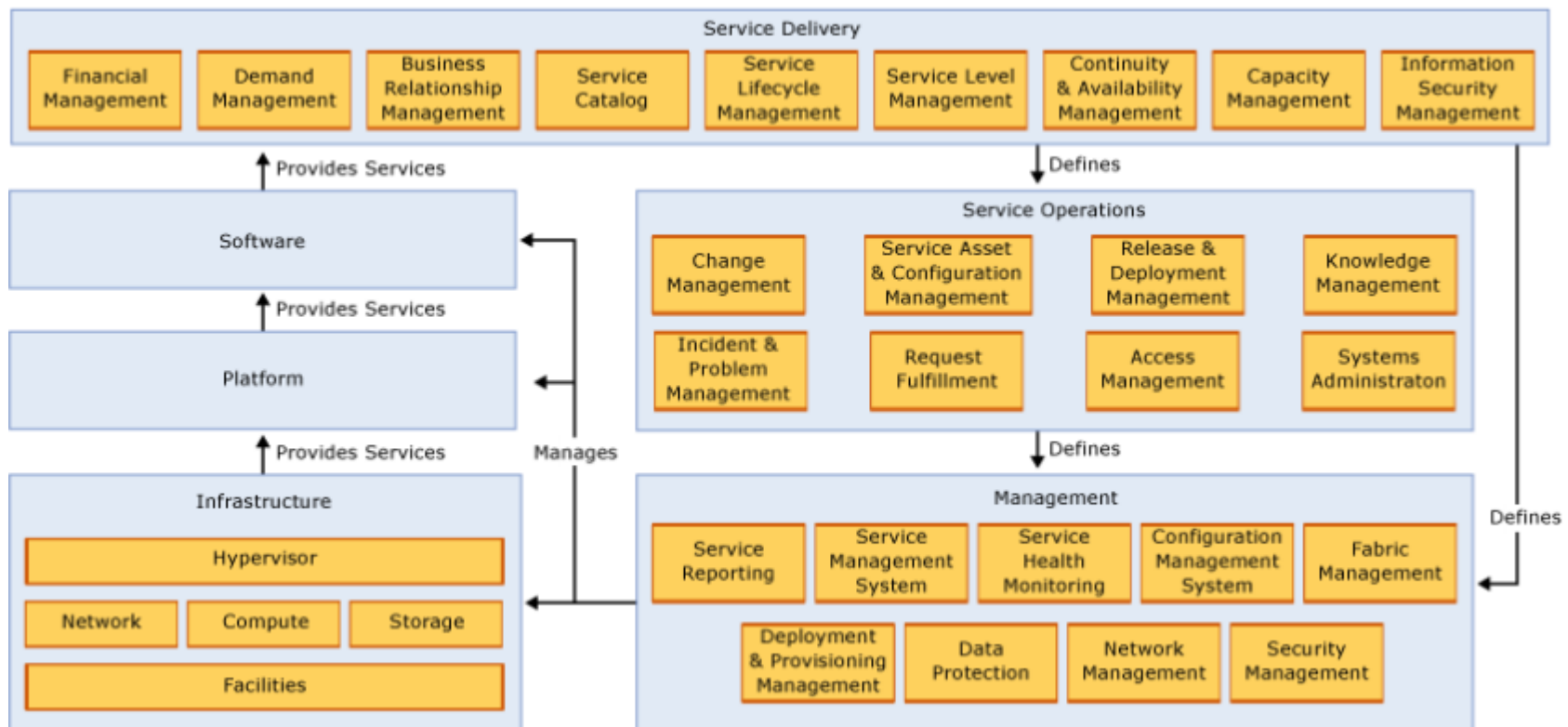
## Deployment models

- ◆ **Public Cloud** – A deployment model where *cloud services are potentially available to each customer of such a service and its resources are controlled by the cloud service provider*. A public cloud can be owned, managed, and used by a business, academic, or government organization, or a combination thereof. The service is provided at the premises of the service provider. The actual availability for specific customers of the service is subject to a specific SLA.;
- ◆ **Private Cloud** - A cloud deployment model *where cloud services are used exclusively by one client and resources are controlled by that client*. Private cloud can be owned, managed and used by the organization itself or by a third party and can exist on the client's premises or outside them (colocation). The customer of the service may allow access to other parties in his favor;

# NETWORK ADMINISTRATION

## Deployment models

The private cloud reference model—IaaS view



Assoc. Prof. Rosen Radkov PhD

# NETWORK ADMINISTRATION

## Deployment models

- ◆ **Community Cloud** – A model in which services are maintained and shared by a specific group of cloud service customers who have shared requirements and relationships with each other and where resources are controlled by at least one member of that group. Community cloud may be owned, managed and used by one or more of the organizations in the community, by a third party or by some combination thereof and may exist on or off the premises of the owner;
- ◆ **Hybrid Cloud** - A model using at least two different implementation models. The included installations remain unique, but are united by appropriate technology that allows interoperability, data portability and application portability. A hybrid cloud may be owned, managed and used by the organization itself or by a third party and may exist indoors or outdoors.

# NETWORK ADMINISTRATION

## Comparison of implementation models

|                    | Private            | Community   | Public            | Hybrid         |
|--------------------|--------------------|-------------|-------------------|----------------|
| <b>Scalability</b> | Limited            | Limited     | Very high         | Very high      |
| <b>Security</b>    | Most secure option | Very secure | Moderately secure | Very secure    |
| <b>Performance</b> | Very good          | Very good   | Low to medium     | Good           |
| <b>Reliability</b> | Very high          | Very high   | Medium            | Medium to high |
| <b>Cost</b>        | High               | Medium      | Low               | Medium         |

# NETWORK ADMINISTRATION

## Cloud security

- **What will we do if we do not have access to the Internet?**
- **What will happen if our customers don't have access to the cloud to place orders?**
- ◆ Before relocating critical infrastructure to the cloud, companies must assess and address *security threats both outside and inside the cloud*. Many of the problems associated with protecting clouds from external threats are similar to those traditionally faced by data centers.
- ◆ In the cloud, however, the *responsibility* to provide adequate protection is often *shared* between users, vendors, and all third parties that users rely on to maintain software, hardware, or security..

# NETWORK ADMINISTRATION

## Cloud security

- ◆ Cloud users are responsible for the security of the application. Cloud providers are responsible for the physical security and security of the software, such as the application of external firewall rules. The security of the intermediate layers of the software is shared between users and providers.
- ◆ A security risk that can be ignored by companies, that are considering moving to the cloud, is that which arises from sharing vendor resources with other cloud users. Cloud providers must guard against theft or DoS attacks from their users and ensure that users are protected from each other.

# NETWORK ADMINISTRATION

## Cloud security

- ◆ Virtualization can be a powerful mechanism for dealing with these potential risks, as it protects against most user attempts to attack each other or attack the provider's infrastructure. However, not all resources are virtualized, and not all virtualization environments are error-free. Improper virtualization can allow user code to access sensitive parts of a provider's infrastructure or other users' resources.
- ◆ Another security concern that businesses need to consider is the extent to which subscribers are protected by the provider, especially in the context of unintentional data loss. For example, in the case of improving the provider's infrastructure, what happens to hardware that is unusable or replaced?

# NETWORK ADMINISTRATION

## Cloud security risks and possible countermeasures

1. **Abuse and malicious use of cloud computing:** With many Cloud providers it is relatively easy to register and start using cloud services, some even offer free limited trial periods. This allows attackers to enter the cloud to carry out various attacks, such as spam, malicious attacks and denial of service (most in PaaS).

**Countermeasures** include (1) stricter initial registration and validation procedures, (2) enhanced monitoring and coordination of credit card fraud, (3) comprehensive inspection of customer network traffic, and (4) monitoring of public blacklists for own IP network blocks.

# NETWORK ADMINISTRATION

## Cloud security risks and possible countermeasures

2. **Unprotected interfaces and application programming interfaces (APIs):** CPs offer a set of software interfaces or application programming interfaces (APIs) that customers use to manage and interact with cloud services. The security and availability of shared cloud services depends on the security of these core APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against accidental and malicious attempts to circumvent the rules.

**Countermeasures** include (1) analyzing the security model of CP interfaces, (2) ensuring that rigorous authentication and access controls are performed in accordance with the encrypted transmission, and (3) understanding the API-related dependency chain.

# NETWORK ADMINISTRATION

## Cloud security risks and possible countermeasures

3. **Malice from within:** Within the cloud computing paradigm, the organization discontinues direct control over many aspects of security and thus provides an unprecedented level of trust to the CP. One of the serious concerns is the risk of malicious internal activity. Cloud architectures require certain roles that are extremely risky, such as system administrators and managed security service providers.

**Countermeasures** include (1) implementing strict supply chain management and conducting a comprehensive assessment of suppliers, (2) human resource requirements to be part of the legal contract, (3) a requirement for transparency in overall information security and management practices. ; and (4) defining security breach notification processes.

# NETWORK ADMINISTRATION

## Cloud security risks and possible countermeasures

4. **Technology sharing issues** : IaaS providers provide their services in a scalable way by sharing the infrastructure. Often the main components that make up this infrastructure (CPU caches, GPUs, etc.) are not designed to offer strong insulation properties for an architecture used by many customers. CPs usually treat this risk by using isolated VMs for individual clients. This approach is still vulnerable to attacks by both insiders and outsiders, and can therefore only be part of an overall security strategy.

**Countermeasures** include (1) implementing best security practices for installation/configuration, (2) monitoring the environment for unauthorized changes/activities, (3) using strict authentication and access control for administration, (4) implementing of the SLA for protection against vulnerabilities and (5) performing audits to scan and configure vulnerabilities.

# NETWORK ADMINISTRATION

## Cloud security risks and possible countermeasures

5. **Data loss or leakage:** For many customers, the most devastating impact of a security breach is the loss or leakage of data.

**Countermeasures** include (1) the introduction of strict control of API access, (2) encryption and protection of data integrity during transit and at rest, (3) analysis of data protection both during design and during execution; management and destruction.

# NETWORK ADMINISTRATION

## Cloud security risks and possible countermeasures

6. **Abduction of accounts or services:** The theft of accounts and services, usually with stolen credentials, remains the biggest threat. With stolen credentials, attackers can often access critical areas of embedded cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services.

**Countermeasures** include (1) prohibiting the sharing of rights between users and services, (2) using rigorous two-factor authentication methods where possible, (3) using proactive monitoring to detect unauthorized activity, and (4) understanding of the security policy of the CP and SLA.

# NETWORK ADMINISTRATION

## Cloud security risks and possible countermeasures

7. **Unknown risk profile:** When using cloud infrastructures, the customer must transfer the management of a number of security issues to the cloud service provider. In this way, the client must pay attention and clearly define the roles and responsibilities associated with risk management. For example, employees may deploy data applications and resources to the CP without following the usual privacy, security, and oversight rules and procedures.

**Countermeasures** include (1) detecting applicable logs and data, (2) partially/fully disclosing infrastructure details (eg patch levels and firewalls), and (3) monitoring and signaling the necessary information. Similar lists have been developed by the European Network and Information Security Agency and NIST.

# NETWORK ADMINISTRATION

## **Cloud data protection**

- Multi-instance model – provides a separate instance of the database to each client
- Multi-tenant model – one database is shared between all customers

# NETWORK ADMINISTRATION

**THANK YOU FOR THE ATTENTION!**

Assoc. Prof. Rosen Radkov PhD