6.16.3 Cloud Computing Facts

Cloud computing is software, data access, computation, and storage services provided to clients through the internet.

- The term *cloud* is a metaphor for the internet. It is based on the basic cloud drawing used to represent the telephone network. It is now used to describe the internet infrastructure in computer network diagrams.
- Typical cloud computing providers deliver common business applications that are accessed from a web service or software (like a web browser).
- The cloud connection can exist over the internet or a LAN.
- Cloud computing does not require end-user knowledge of the physical location and configuration of the system that delivers the services.

Cloud computing can be implemented in several different ways, including the following:

Type	Description
Public Cloud	A *public cloud* can be accessed by anyone. Cloud-based computing resources, such as platforms, applications, storage, or other resources, are made available to the general public by a cloud service provider. The service provider may or may not require a fee for using these resources. For example, Google provides many publicly-accessible cloud applications, such as Gmail and Google Docs.
Private Cloud	A *private cloud* provides resources to a single organization. Access is restricted to only the users within the organization. Private clouds can be hosted internally. But because of the expense and expertise required to do so, they are typically hosted externally, by a third party. An organization commonly enters into an agreement with a cloud service provider, which provides secure access to cloud-based resources. The organization's data is kept separate and secure from any other organization using the same service provider.
Community Cloud	A *community cloud* is designed to be shared by several organizations. Access is restricted to only users within the organizations who are sharing the community cloud infrastructure. Private clouds can be hosted internally or on-premise, with each organization sharing the cost of implementation and maintenance. However, because of the expense and expertise required to do so, community clouds are commonly hosted externally, by a third party.
Hybrid Cloud	A *hybrid cloud* is composed of a combination of public, private, and community cloud resources from different service providers. The goal behind a hybrid cloud is to expand the functionality of a given cloud service by integrating it with other cloud services.

The advantages of cloud computing are:

- Flexible access
- Ease of use
- Self-service resource provisioning
- API availability
- Service metering
- The ability to try software applications in some cloud computing service models

Cloud computing service models include the following:

Model	Description
Infrastructure as a Service (IaaS)	Infrastructure as a Service (IaaS) delivers infrastructure to the client, such as processing, storage, networks, and virtualized environments. The client deploys and runs software without purchasing servers, data center space, or network equipment.
Platform as a Service (PaaS)	Platform as a Service (PaaS) delivers everything a developer needs to build an application. The deployment comes without the cost and complexity of buying and managing the underlying hardware and software layers.
Software as a Service (SaaS)	Software as a Service (SaaS) delivers software applications to the client over the internet or on a local area network. SaaS comes in two implementation types: ▪ Simple multi-tenancy: each customer has its own resources, which are segregated from other customers. ▪ Fine grain multi-tenancy: data is segregated from other customers, but resources are shared.
Security as a Service (SECaaS)	Security as a service (SECaaS) providers integrate their services into a corporate infrastructure. The applications and software are specific to organizational security. SECaaS is based on the Software-as-a-Service cloud computing model, but is limited to information security-type services and does not require on-premises hardware. These security services can include authentication, anti-virus, anti-malware, spyware, intrusion detection, penetration testing, and security event management. SECaaS can sometimes be much more cost effective for an organization than having to purchase all the necessary hardware equipment and personnel to properly protect a network from viruses, malware, and instruction. However, it is still a necessity to have an on-site security professional.

Cloud service providers reduce the risk of security breaches through the following actions:

- Authenticate all users who access the service and allow users to access only the applications and data that they need. Use a Cloud Access Security Broker (CASB). A CASB is a software tool or service that sits between an organization and a cloud service provider. Its job is to make sure that all communication and access to the cloud service provider complies with the organization's security policies and procedures.
- Segregate each organization's centrally-stored data.
- Verify, test, and apply updates to the infrastructure.
- Establish a formal process for all facets of the service, from user requests to major data breaches and catastrophic events.
- Implement security monitoring for usage, unusual behavior, and other events.
- Implement encryption up to the point of use, such as the client's web browser.
- Probe for security holes with a third-party service provider.
- Comply with all regulatory measures, such as the Sarbanes-Oxley Act.

Cloud-based services can be hosted externally by third-party service providers or internally on your own virtualization infrastructure. For example, internal private clouds are commonly used to provide a Virtual Desktop Infrastructure (VDI). Using VDI, user desktops are virtualized, running on high-end hardware in the data center instead of on the end user's workstation hardware. The physical workstation is merely used to establish a remote connection to the user's virtualized desktop. This is sometimes called a *thin client* deployment because most of the computing power is provided by servers in the data center. Traditional deployments, where most of the processing load is handled by the local workstation, are called *thick client* deployments.

Using VDI provides increased flexibility, enhanced security, efficient management, and better data protection than the traditional workstation-based desktop model. Consider the following advantages:

- Workstation hardware costs are reduced. Only minimal workstation hardware is required to run a Remote Desktop (Windows) or VNC (Linux) client and connect to the private cloud.
- User data on the desktop can be protected centrally by backing up the hypervisors where the virtualized desktops are running. There is no need to separately back up physical workstations.
- If a user's physical workstation fails, no data is lost. The user can simply access their virtualized desktop from a different workstation while the failed hardware is repaired or replaced.
- If a widespread malware infection hits multiple user desktops, the affected virtual systems can be quickly re-imaged on the hypervisor. There is no need to push large images down to end users' workstations over the network.
- If a user loses a device, such as a notebook or tablet, there is much less of a chance that critical data will be compromised because no data is saved on the device.
