9.5.2 Cloud Computing Facts

Cloud computing is a combination of software, data access, computation, and storage services provided to clients through the internet. The term *cloud* is a metaphor for the internet 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). A cloud connection can exist over the internet or a LAN. Cloud computing does not require end-user knowledge of the physical location or configuration of the system that delivers the services.

The advantages of cloud computing are:

- Flexibility of access
- Ease of use
- Self-service provisioning of resources
- API availability
- Metering of services
- The ability to test software applications (in some cloud computing service models)

Cloud Types

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, and storage 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 granted only to 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 granted to only the users within the organizations who share the community cloud infrastructure. Community clouds can be hosted internally, with each organization sharing the cost of implementation and maintenance. 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 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.

Cloud Services

Cloud computing service models include the following:

Model	Description
Infrastructure as a Service (IaaS)	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)	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)	SaaS delivers software applications to the client either over the internet or on a local area network. SaaS can be: ▪ A simple multi-tenancy implementation in which customers have their own resources that are segregated from other customers. ▪ A fine grain multi-tenancy implementation in which resources are shared, but data is segregated from other customers.

Cloud Service Benefits

Cloud computing service providers reduce the risk of security breaches in multiple ways. They:

- Authenticate all users who access the service and only allow users to access the

applications and data that they need.
- 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 of things like usage and unusual behavior.
- 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, like the Sarbanes-Oxley Act.