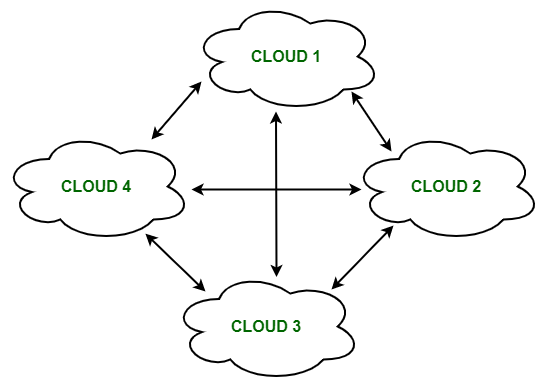
**Cloud Federation**

* Cloud federation is the practice of interconnecting service providers in cloud environments to load balance traffic and accommodate spikes in demand.
* A federated cloud (also called cloud federation) is the deployment and management of multiple external and internal cloud computing services to match business needs. A federation is the union of several smaller parts that perform a common action.



* Federated cloud is created by connecting the cloud environment of different cloud providers using a common standard.

The architecture of Federated Cloud:

**1. Cloud Exchange**

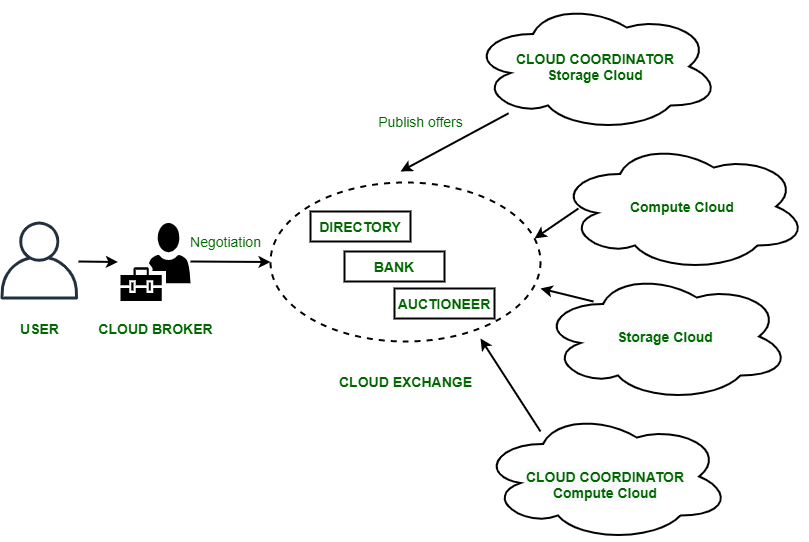
The Cloud Exchange acts as a mediator between cloud coordinator and cloud broker. The demands of the cloud broker are mapped by the cloud exchange to the available services provided by the cloud coordinator. The cloud exchange has a track record of what is the present cost, demand patterns, and available cloud providers, and this information is periodically reformed by the cloud coordinator.

**2. Cloud Coordinator**

The cloud coordinator assigns the resources of the cloud to the remote users based on the quality of service they demand and the credits they have in the cloud bank. The cloud enterprises and their membership are managed by the cloud controller.

**3. Cloud Broker**

The cloud broker interacts with the cloud coordinator, analyzes the Service-level agreement and the resources offered by several cloud providers in cloud exchange. Cloud broker finalizes the most suitable deal for their client.

* A federated cloud means constructing a seamless cloud environment that can interact with people, different devices, several application interfaces, and other entities. 
* In cloud federation, it is common to have more than one provider for processing the incoming demands. In such cases, there must be a scheme needed to distribute the incoming demands equally among the cloud service providers.
* Federated Cloud technologies:
  + **OpenNebula**
  + **Aneka coordinator**
  + **Eucalyptus**
* There are at least four basic types of federation :
  + Permissive federation
  + Verified federation.
  + Encrypted federation.
  + Trusted federation.

**Permissive federation**

* Permissive federation occurs when a server accepts a connection from a peer network server without verifying its identity using DNS lookups or certificate checking.
* The lack of verification or authentication may lead to domain spoofing

**Verified federation**

* This type of federation occurs when a server accepts a connection from a peer after the identity of the peer has been verified.
* It uses information obtained via DNS and by means of domain-specific keys exchanged beforehand. The connection is not encrypted, and the use of identity verification effectively prevents domain spoofing.
* there are chances of DNS attack.

**Encrypted federation**

* In Encrypted federation mode, a server accepts a connection from a peer if and only if the peer supports Transport Layer Security (TLS)
* The peer must present a digital certificate. The certificate may be self-signed, but this prevents using mutual authentication. The certificate may be self signed (prevents mutual authentication).
* The peer cloud interested in the federation must provide the digital certificate which still provides mutual authentication. Thus, encrypted federation results in weak identity verification.

**Trusted federation**

* Here, a server accepts a connection from a peer only under the stipulation that the peer supports TLS and the peer can present a digital certificate issued by a root certification authority (CA) that is trusted by the authenticating server.
* The list of trusted root CAs may be determined by one or more factors, such as the operating system, XMPP server software, or local service policy.
* In trusted federation, the use of digital certificates results not only in a channel encryption but also in strong authentication.

**Cloud Security Challenges**

1. In the cloud, you lose control over assets in some respects, so your security model must be reassessed.

2. With the cloud model, you lose control over physical security.

3. Exposing your data in an environment shared with other companies could give the government “reasonable cause” to seize your assets because another company has violated the law.

4. Storage services provided by one cloud vendor may be incompatible with another vendor’s services – Difficult to move from one to the other.

5. If information is encrypted while passing through the cloud, who controls the encryption/decryption keys?

6. Does data encrypted while it is at rest in the cloud vendor’s storage pool.

7. Common standard to ensure data integrity does not yet exist. Ensuring the integrity of the data really means that it changes only in response to authorized transactions.

8. Cloud applications undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected. The speed at which applications will change in the cloud will affect both the SDLC and security. This means that users must constantly upgrade, because an older version may not function, or protect the data.

9. Core business practices provide competitive differentiation. Security needs to move to the data level, so that enterprises can be sure their data is protected wherever it goes. Sensitive data is the domain of the enterprise, not the cloud computing provider. One of the key challenges in cloud computing is data-level security.

10. Outsourcing means losing significant control over data

11. Cloud-based services will result in many mobile IT users accessing business data and services without traversing the corporate network. So, attackers no longer have to come onto the premises to steal data, and they can find it all in the one “virtual” location.

12. The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the auditability of records.

13. Proving the security state of a system and identifying the location of an insecure virtual machine will be challenging.

14. The co-location of multiple virtual machines increases the attack surface and risk of virtual machine-to-virtual machine compromise.

15. Virtual machine are vulnerable as they move between the private cloud and the public cloud.

16. Enterprises are often required to prove that their security compliance is in accord with regulations, standards, and auditing practices, regardless of the location of the systems at which the data resides.

17. To establish zones of trust in the cloud, the virtual machines must be self-defending, effectively moving the perimeter to the virtual machine itself.

18. Enterprise perimeter security (i.e., firewalls, network segmentation, intrusion detection and prevention systems, monitoring tools, and the associated security policies) only controls the data that resides and transits behind the perimeter.

# **Service level agreements in Cloud computing**

* When cloud server user wants to communicate with cloud service provider it can be achieved by SLA.
* A Service Level Agreement (SLA) is the bond for performance negotiated between the cloud services provider and the client (service user).
* Earlier, in cloud computing all Service Level Agreements were negotiated between a client and the service consumer.
* Nowadays, with the initiation of large utility-like cloud computing providers, most Service Level Agreements are standardized until a client becomes a large consumer of cloud services.
* Customer-based SLA
* Service-based SLA
* Multilevel SLA

Customer-based SLA:

-> Used for individual customers.

-> Consists of all kinds of services that customer needs.

-> Type & QOS

-> Ex : telecommunication

Service-based SLA

-> Includes one identical type of service for all of its customers

-> more convinient for vendors(service providers)

-> Ex : Gmail

Multilevel SLA

-> This is customized according to the needs of end-user company

-> It also allows users to integrate several conditions into the same system

-> It's combination of both 1 & 2

-> It has 3 levels : Corporate level, Customer level, Service level

Few Service Level Agreements are enforceable as contracts, but mostly are agreements or contracts which are more along the lines of an Operating Level Agreement (OLA) and may not have the restriction of law. It is fine to have an attorney review the documents before making a major agreement to the cloud service provider. Service Level Agreements usually specify **some parameters** which are mentioned below:

1. Availability of the Service (uptime)
2. Latency or the response time
3. Service components reliability
4. Each party accountability
5. Warranties

In any case, if a cloud service provider fails to meet the stated targets of minimums then the provider has to pay the penalty to the cloud service consumer as per the agreement. So, Service Level Agreements are like insurance policies in which the corporation has to pay as per the agreements if any casualty occurs. Microsoft publishes the Service Level Agreements linked with the Windows Azure Platform components, which is demonstrative of industry practice for cloud service vendors. Each individual component has its own Service Level Agreements. Below are two **major Service Level Agreements (SLA)**described:

1. **Windows Azure SLA –**  
   Window Azure has different SLA’s for compute and storage. For compute, there is a guarantee that when a client deploys two or more role instances in separate fault and upgrade domains, client’s internet facing roles will have external connectivity minimum 99.95% of the time. Moreover, all of the role instances of the client are monitored and there is guarantee of detection 99.9% of the time when a role instance’s process is not runs and initiates properly.
2. **SQL Azure SLA –**  
   SQL Azure clients will have connectivity between the database and internet gateway of SQL Azure. SQL Azure will handle a “Monthly Availability” of 99.9% within a month. Monthly Availability Proportion for a particular tenant database is the ratio of the time the database was available to customers to the total time in a month. Time is measured in some intervals of minutes in a 30-day monthly cycle. Availability is always remunerated for a complete month. A portion of time is marked as unavailable if the customer’s attempts to connect to a database are denied by the SQL Azure gateway.

Service Level Agreements are based on the usage model. Frequently, cloud providers charge their pay-as-per-use resources at a premium and deploy standards Service Level Agreements only for that purpose. Clients can also subscribe at different levels that guarantees access to a particular amount of purchased resources. The Service Level Agreements (SLAs) attached to a subscription many times offer various terms and conditions. If client requires access to a particular level of resources, then the client need to subscribe to a service. A usage model may not deliver that level of access under peak load condition.

Security issues :

Privileged user access

Data location

Data segregation – encryption

Recovery

Long-term viability

**The 14 NCSC cloud security principles**

**1.Data in transit protection**

User data which is transitioning between networks should be protected against any interference.

**2.Asset protection and resilience**

User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

**3.Separation between users**

If a user of a service is compromised by malicious software, this should not affect the service or data of another user.

**4.Governance framework**

A Security Governance Framework should be followed by the service provider, in order to internally coordinate its management of the service.

**5.Operational security**

In order to prevent and detect attacks, the service must be operated securely. Adequate security shouldn’t require complex or expensive processes.

**6.Personnel security**

Service provider personnel should be thoroughly screened, followed by in-depth training to reduce the likelihood of accidental or malicious compromise.

**7.Secure development**

Services should be designed with security in mind. Done By following a Secure by Design approach.

**8.Supply chain security**

The service provider should ensure that their supply chain adheres to all of the same security principles.

**9.Secure user management**

Your service provider should ensure that you have the relevant tools to securely manage the use of their services. Management interfaces prevent unauthorised access to your data, making them a vital part of the security barrier.

**10.Identity and authentication**

Access to the service interfaces should only be granted to specific individuals and should all be guarded by adequate authentication measures – two party authentication if possible.

**11.External interface protection**

Any external or less trustworthy service interfaces must be identified and defended appropriately.

**12.Secure service administration**

If a cloud service is compromised through its administration system, important company data could be stolen or manipulated. It is vital that these services are secure.

**13.Audit information for users**

A service provider should supply their customers with the audit recorded needed to monitor the service and who is able to access your data. This is vital as it gives you a means to identify inappropriate or malicious activity.

**14.Secure use of service**

You have a responsibility to ensure the service is used properly, to ensure your data is kept safe and protected.