CS19741-Cloud Computing
Assignment - 4

1.Federated Cloud Computing:

Federated cloud computing is a model where multiple independent cloud providers collaborate to offer unified services. It allows for seamless interaction across different cloud environments (public, private, or hybrid), enabling organizations to harness resources from several cloud platforms while maintaining data security, compliance, and performance efficiency. The idea is to treat multiple cloud providers as part of a larger, interconnected cloud infrastructure..

Core Components of Federated Cloud Computing:

Interoperability:
The key to federated cloud computing is the ability of different cloud systems to work together. This involves standardizing protocols, APIs, and services so that workloads can move between clouds without compatibility issues. For example, a federated cloud may integrate services from AWS, Google Cloud, and Azure, allowing applications to leverage the strengths of each provider.

Federation Management:
This refers to the governance, control, and coordination mechanisms that manage the interactions between federated clouds. It ensures smooth collaboration, resource distribution, and compliance with policies across different cloud environments. Federation management helps balance loads, control resource allocation, and optimize usage across multiple clouds.

Service Orchestration:
This component allows users to orchestrate resources and services across federated clouds. Service orchestration ensures that the right cloud provider is used based on performance, cost, or location requirements. It also automates the movement of workloads between clouds, ensuring optimal performance and minimal disruption.

Data Governance and Sovereignty:
In a federated cloud model, organizations can control where their data resides based on legal and regulatory requirements. For instance, sensitive data may need to remain within a certain geographic boundary to comply with local regulations like GDPR. Federated cloud systems ensure that data is processed and stored according to these regulations.

Benefits of Federated Cloud Computing:

Enhanced Flexibility:
By combining multiple cloud providers, organizations can choose the best tools and services from each. This flexibility allows businesses to pick and choose cloud services tailored to specific workloads.

Improved Resilience:
Federated clouds reduce the risk of downtime because services and data can be spread across different providers. In case one provider experiences an outage, the workload can continue running on another provider's infrastructure.

Scalability on Demand:
Federated clouds enable scalable resource allocation, drawing from multiple cloud providers as needed. This eliminates bottlenecks and ensures that resources are available when demands spike.

Cost Optimization:
Organizations can use a combination of clouds to optimize costs, choosing cheaper storage solutions or performance-enhanced computing services depending on their workload needs. Federated cloud computing allows for cost balancing across providers.

Challenges in Federated Cloud Computing:

Complex Infrastructure Management:
Managing multiple cloud environments can become complex, especially when it comes to configuring security, monitoring performance, and managing service-level agreements (SLAs). Robust management platforms are necessary to keep track of operations across clouds.

Security and Compliance:
Ensuring consistent security policies across multiple cloud providers is a challenge. Each cloud provider has its own security protocols, so managing identities, access control, and encryption uniformly across the federation requires strong security practices and tools.

Performance and Latency:
Federating clouds involves transferring data between different providers, which can introduce latency issues. Additionally, moving large datasets between clouds might increase costs due to bandwidth charges and processing time.

Data Privacy Concerns:
With multiple cloud providers involved, keeping track of data privacy and ensuring compliance with varying data protection laws across different jurisdictions can be complex.

2.**Service level agreements in Cloud computing:**

A **Service Level Agreement (SLA)** is the bond for performance negotiated between the cloud services provider and the client. 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. Service level agreements are also defined at **different levels** which are mentioned below:

- Customer-based SLA
- Service-based SLA
- Multilevel SLA

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:

Availability of the Service (uptime)

Latency or the response time

Service components reliability

Each party accountability

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:

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.
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.