* **Write note on a charteristics and challenges of cloud computing? (6 Marks)**

**Ans :**

* **Essential characteristics of Cloud Computing**

1. **On demand self services :** computer services such as email, applications, network or server service can be provided without requiring human interaction with each service provider. Cloud service providers providing on demand self services include Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com. New York Times and NASDAQ are examples of companies using AWS (NIST).
2. **Broad network access** : Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs.
3. **Resource pooling** : The provider’s computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The resources include among others storage, processing,memory, network bandwidth, virtual machines and email services. The pooling together of the resource builds economies of scale (Gartner)
4. **Rapid elasticity :** Cloud services can be rapidly and elastically pro

versioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

The “**flexibility and elasticity**” allows these systems to scale up and down at will

* + utilising the resources of all kinds
    - CPU, storage, server capacity, load balancing, and databases

1. **Multi Tenacity** : It refers to the need for policy –driven **e**nforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Consumers might utilize a public cloud provider’s service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure
   * Cloud are transparent to users and applications, they can be built in multiple ways
   * branded products, proprietary open source, hardware or software, or just off-the-shelf PCs.
2. **Measured service :** Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilised service. Cloud computing services use a metering capability which enables to control and optimise resource use. This implies that just like air time,electricity or municipality water IT services are charged per usage metrics – **pay for play**. The more you utilise the higher the bill. Just as utility companies sell power to subscribers, and telephone companies sell voice and data services, IT services such as network security management, data center hosting or even departmental billing can now be easily delivered as a contractual service

* The “**pay as much as used and needed**” type of utility computing and the “**always on!, anywhere and any place**” type of network-based computing.

1. **Service-Level Agreements (SLAs**) : Organizations should understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers. Organization should also understand customer responsibilities, and those of the service provider, before using a cloud service.
2. **Geographically Distributed Data centers**

* **Essential Challenges of Cloud Computing**
* Most security problems stem from:
  + Loss of control
  + Lack of trust (mechanisms)
  + Multi-tenancy
* These problems exist mainly in 3rd party management models
  + Self-managed clouds still have security issues, but not related to above

1. **Consumer’s loss of control**
   * Data, applications, resources are located with provider
   * User identity management is handled by the cloud
   * User access control rules, security policies and enforcement are managed by the cloud provider
   * Consumer relies on provider to ensure
     + Data security and privacy
     + Resource availability
     + Monitoring and repairing of services/resources
2. **Lack of Trust in the Cloud**
   * A brief deviation from the talk
     + Trusting a third party requires taking risks
     + Defining trust and risk : Opposite sides of the same coin (J. Camp)
   * People only trust when it pays (Economist’s view)
   * Need for trust arises only in risky situations
3. **Multi-tenancy Issues in the Cloud**
   * Conflict between tenants’ opposing goals
     + Tenants share a pool of resources and have opposing goals
   * How does multi-tenancy deal with conflict of interest?
     + Can tenants get along together and ‘play nicely’ ?
     + If they can’t, can we isolate them?
   * How to provide separation between tenants?
4. **Security Issues in the Cloud**
   * In theory, minimizing any of the issues would help:
   * Loss of Control
     + Take back control
       - Data and apps may still need to be on the cloud
       - But can they be managed in some way by the consumer?
   * Lack of trust
     + Increase trust (mechanisms)
       - Technology
       - Policy, regulation
       - Contracts (incentives): topic of a future talk
   * Multi-tenancy
     + Private cloud :Takes away the reasons to use a cloud in the first place
     + VPC: its still not a separate system
     + Strong separation
5. **Minimize Lack of Trust: Policy Language**
   * + Consumers have specific security needs but don’t have a say-so in how they are handled
     + What the heck is the provider doing for me?
     + Currently consumers cannot dictate their requirements to the provider (SLAs are one-sided)
   * Standard language to convey one’s policies and expectations
     + Agreed upon and upheld by both parties
     + Standard language for representing SLAs
     + Can be used in a intra-cloud environment to realize overarching security posture
   * Create policy language with the following characteristics:
     + Machine-understandable (or at least processable),
     + Easy to combine/merge and compare
     + Examples of policy statements are, “requires isolation between VMs”, “requires geographical isolation between VMs”, “requires physical separation between other communities/tenants that are in the same industry,” etc.
     + Need a validation tool to check that the policy created in the standard language correctly reflects the policy creator’s intentions (i.e. that the policy language is semantically equivalent to the user’s intentions).
6. **Minimize Lack of Trust: Certification**
   * Certification
     + Some form of reputable, independent, comparable assessment and description of security features and assurance
     + Sarbanes-Oxley, DIACAP, DISTCAP, etc (are they sufficient for a cloud environment?)
   * Risk assessment
     + Performed by certified third parties
     + Provides consumers with additional assurance
7. **Minimize Loss of Control in the Cloud**

* Monitoring
* Utilizing different clouds
* Access control management