# UNIT-2

# CLOUD SCENARIOS

## I) Introduction to Cloud Scenarios:

There are three different major implementations of cloud computing. The organizations are using cloud computing is quite different at a granular level, but the uses generally fall into one of these three solutions:

**i) Compute Clouds**: Compute clouds allow access to highly scalable, inexpensive, on-demand computing resources that run the code that they're given. Three examples of compute clouds are:

- Amazon's EC2
- Google App Engine
- Berkeley Open Infrastructure for Network Computing (BOINC)

Compute clouds are the most flexible in their offerings and can be used for various purposes; it simply depends on the application the user wants to access. These applications are good for any size organization, but large organizations might be at a disadvantage because these applications don't offer the standard management. Enterprises aren't shut out, however. Amazon offers enterprise-class support and there are emerging sets of cloud offerings like Terremark's Enterprise Cloud, which are meant for enterprise use.

***ii)* Cloud Storage:** One of the first cloud offerings was cloud storage and it remains a popular solution. Cloud storage is a big world. There are already in excess of 100 vendors offering cloud storage. This is an ideal solution if you want to maintain files off-site. Security and cost are the top issues in this field and vary greatly, depending on the vendor you choose. Currently, Amazon's S3 is the top level vendor.

**iii) Cloud Applications:** Cloud applications differ from compute clouds in that they utilize software applications that rely on cloud infrastructure. Cloud applications are versions of Software as a Service (SaaS) and include such things as web applications that are delivered to users via a browser or application like Microsoft Online Services. These applications offload hosting and IT management to the cloud. Cloud applications often eliminate the need to install and run the application on the customer's own computer.

Some cloud applications include

- Peer-to-peer computing (like BitTorrent and Skype)
- Web applications (like MySpace or YouTube)
- SaaS (like Google Apps)
- Software plus services (like Microsoft Online Services)

## II) Benefits of a cloud Computing:

**1) Scalability:** If you are anticipating a huge upswing in computing need, cloud computing can help you manage. Rather than having to buy, install, and configure new equipment, you can buy additional CPU cycles or storage from a third party. Since your costs are based on consumption, you wouldn't have to pay out as much as if you had to buy the equipment.

Once you have fulfilled your need for additional equipment, you just stop using the cloud provider's services, and you don't have to deal with unneeded equipment. You simply add or subtract based on your organization's need.

**2) Simplicity:** Again, not having to buy and configure new equipment allows you and your IT staff to get right to your business. The cloud solution makes it possible to get your application started immediately, and it costs a fraction of what it would cost to implement an on-site solution.

**3) Knowledgeable Vendors:** Typically, when new technology becomes popular, there are plenty of vendors who pop up to offer their version of that technology. This isn't always good, because a lot of those vendors tend to offer less than useful technology. By contrast, the first comers to the cloud computing party are actually very reputable companies.

Companies like Amazon, Google, Microsoft, IBM, and Yahoo! have been good vendors because they have offered reliable service.

**4) More Internal Resources:** By shifting your non-mission-critical data needs to a third party, your IT department is freed up to work on important, business-related tasks. You also don't have to add more manpower and training that system from having to deal with these low-level tasks. Also, since network outages are a terrible for the IT staff, this burden is offloaded onto the service provider. True, outages happen, but let Amazon worry about getting the service back online. When you're looking at service providers, make sure you find someone who offers 24-hour help and support and can respond to emergency situations.

**5) Vendor Security:** Cloud Security vendors services have more secure than traditional infrastructure. A higher cloud services provider will offer strong data center security, a world class cloud computing infrastructure, application security and validated methodology for securing and preventing the data stored within a cloud. A secure vendor must have the following capabilities:

- Network intrusion detection and prevention
- Real time Log flow analysis
- Web application Security
- Vulnerability Assessments

- Log Manager

## III) Limitations of a Cloud Computing:

**1) Your Sensitive information:** We've talked about the concern of storing sensitive information on the cloud, but it can't be simple. Once data leaves your hands and lands in the lap of a service provider, lost a layer of control.

Let's say a financial planner is using Google Spreadsheets to maintain a list of employee social security numbers. Now the financial planning company isn't the only one who should protect the data from hackers and internal data breaches. In a technical sense, it also becomes Google's problem. However, Google may release itself of responsibility in its agreement with you.

**2) Protect Your Data:** That doesn't mean you can't maintain your data on a cloud; you just need to be safe. The best way is to encrypt your data before you send it to a third party. Programs like PGP (www.pgp.com) or open-source TrueCrypt (www.truecrypt.org) can encrypt the file so that only those with a password can access it. Encrypting your data before sending it out protects it. If someone does get your data, they need the proper credentials.

**3) Developing your Applications:** Developing your own applications can certainly be a problem if you don't know how to program, or if you don't have programmers on staff. In such a case, you'll have to hire a software company (or developer).

It isn't just applications that you might need some programming sense to deploy. If you have a database on the cloud, you'll need some sort of customized interface and some knowledge of Structured Query Language (SQL) to access and manage that data. But there are benefits; this generation of web services got its start from LAMP. LAMP stands for the following popular items:

- **Linux:** An open-source operating system
- **Apache:** An open-source web server
- **MySQL:** An open-source Structured Query Language (SQL) relational database for web servers
- **Perl:** A programming language

LAMP is widely used because it is very simple. Because of its ease of use, you can get an application up and running very quickly.

**4) Integration:** There are 2 applications used in your business development team, one of the applications contains the sensitive information data and other one contains non sensitive data. So we decided not to move the sensitive data on cloud, but moved non-sensitive data on cloud. In this case, one application is installed locally and other one is cloud. It would create issues with security and speed. We might try to run high speed application on local machine and it is using the data coming from application located on cloud. The speed application will be controlled by application on the cloud.

**IV) Issues and Challenges of Cloud Computing:**

1. **Data Security concern:** Multiple serious threats like virus attack and hacking of the client's site are the biggest cloud computing data security issues. You are transferring your company's important details to a third party so it is important to ensure yourself about the manageability and security system of the cloud.

2. **Dependency on service providers:** For uninterrupted services and proper working it is necessary that you acquire a vendor services with proper infrastructural and technical expertise. An authorized vendor who can meet the security standards set by your company's internal policies and government agencies.

3. **Cost barrier:** For efficient working of cloud computing you have to bear the high charges of the bandwidth. For smaller application cost is not a big issue but for large and complex applications it is a major concern.

4. **Lack of knowledge and expertise:** Every organisation does not have sufficient knowledge about the implementation of the cloud solutions. They have not expertise staff and tools for the proper use of cloud technology. Teaching your staff about the process and tools of the cloud computing is a very big challenge in itself.

5. **Consumption basis services charges:** Cloud computing services are on-demand services so it is difficult to define specific cost for a particular quantity of services. These types of fluctuations and price differences make the implementation of cloud computing very difficult and complicated.

6. **Unauthorized service providers:** Cloud computing is a new concept for most of the business organizations. A normal businessman is not able to verify the genuineness of the service provider agency. It's very difficult for them to check the whether the vendors meet the security standards or not. It is necessary to verify that the vendor must be operating this business for a sufficient time without having any negative record in past.

7. **Recovery of lost data:** Cloud services faces issue of data loss. A proper backup policy for the recovery of data must be placed to deal with the loss. Vendors must set proper infrastructures to efficiently handle with server breakdown and outages.

8. **Data portability:** Every person wants to leverage of migrating in and out of the cloud. Ensuring data portability is very necessary. Usually, clients complain about being locked in the cloud technology from where they cannot switch without restraints.

9. **Cloud management:** Managing a cloud is not an easy task. It consist a lot of technical challenges. People think that traditional IT department will be outdated. Cloud services can easily change and update by the business users. It does not involve any direct involvement of IT department. It is a service provider's responsibility to manage the information and spread it across the organization.

10. **Real time monitoring requirements:** In some agencies, it is required to monitor their system in real time. It is compulsory term for their business that they continuously monitor and maintain their inventory system. Banks and some government agencies need to update their system in real time but cloud service providers are unable to match this requirement.

## V) Security Concerns:

Security is a two-sided coin in the world of cloud computing—there are pros and there are cons. In this section, let's examine security in the cloud and talk about what's good, and where you need to take extra care.

IDC conducted a survey of 244 IT executives about cloud services. Security led the pack of cloud concerns with 74.5 percent. In order to be successful, vendors will have to take data like this into consideration as they offer up their clouds.

**Privacy Concerns or with a Third party:**

Many cloud vendors implement their own proprietary standards and security technologies, and implement differing security models, which need to be evaluated on their own merits.

There are several types of security threats to which cloud computing is vulnerable.

**1. Data Breaches:** A data breach is an incident in which sensitive, protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so. A data breach may be the primary objective of a targeted attack or may simply be the result of human error, application vulnerabilities or poor security practices. A data breach may involve any kind of information that was not intended for public release including, but not limited to, personal health information, financial information, personally identifiable information (PII), trade secrets and intellectual property.

**2. Insufficient Identity, Credential and Access Management:** Data breaches and enabling of attacks can occur because of a lack of scalable identity access management systems, failure to use multifactor authentication, weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates.

Multifactor authentication systems – smartcard, OTP, and phone authentication, for example – are required for users and operators of a cloud service. This form of authentication helps address password theft, where stolen passwords enable access to resources without user consent.

**3. Insecure Interfaces and APIs:** Cloud computing providers expose a set of software user interfaces (UIs) or application programming interfaces (APIs) that customers use to manage and interact with cloud services. The security and availability of general cloud services is dependent on the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts.

**4. System Vulnerabilities:** System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a computer system for the purpose of stealing data, taking control of the system or disrupting service operations. Vulnerabilities within the components of the operating system – kernel, system libraries and application tools – put the security of all services and data at significant risk.

**5. Malicious Insiders:** "A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

**6. Data Loss:** Data stored in the cloud can be lost for reasons other than malicious attacks. An accidental deletion by the cloud service provider, or worse, a physical calamity such as a fire or earthquake, can lead to the permanent loss of customer data unless the provider or cloud consumer takes adequate measures to back up data

**7. Insufficient Due Diligence:** With **cloud computing** being a new implementation, especially to the hiring organizations, there is a knowledge gap that can prevent sufficient exercise of **due diligence** when hiring a **cloud** service provider.

**8. Abuse and Nefarious Use of Cloud Services:** Poorly secured cloud service deployments, free cloud service trials and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.

**9. Denial of Service:** Denial-of-service (DoS) attacks are attacks meant to prevent users of a service from being able to access their data or their applications. By forcing the targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker—or attackers, as is the case in distributed denial-of-service (DDoS) attacks—causes an intolerable system slowdown and leaves all legitimate service users confused and angry as to why the service is not responding.

## VI) Security Benefits:

Cloud Security includes all the useful services including anti-virus, URL filters, firewalls, sandboxes, SSL inspection in a unified platform.

### 1) Data Encryption:

Robust data encryptions within cloud-based security systems have substantially reduced the possibilities of data breaches; these solutions offer a layered approach that consists of security intelligence, key management, and secure access controls.

The multi-layered security features weed out the possibilities of a breach of data to a great extent.

### 2) Avoid DDoS Attacks:

Distributed denial of service attacks are on the rise, particularly for retail and gaming websites. In 2014, CDNetworks saw a 29 percent increase in DDoS attack frequency on client websites. If a DDoS attack is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.

CDNetworks' cloud security is a suite of services that monitor, identify and analyze DDoS attacks. A four-step process starts with identifying incoming DDoS attacks, alerting website managers of the DDoS attacks, effectively absorbing DDoS traffic and dispersing it across global PoPs (points of presence) and providing post-attack analysis.

### 3) Regulatory Compliance

Cloud computing security solutions usually provide reliable SOC1 and SOC2 certifications to the entertainment businesses. These certifications ensure periodic scrutiny of data and all types of possible faults or malfunctions. Cloud-based solutions manage the requisite infrastructure for regulatory compliance and the protection of data.

### 4) Secure Storage

Traditional storage solutions don't provide any protection against possible disasters that have the potential to erase required data from devices. Cloud storage solutions offer private, public, and hybrid solutions which the businesses may choose as per their requirements. The hybrid cloud storage systems allow the users to keep their data secure in the most effective manner.

### 5. Protection against Data Breaches:

Data breach is one of the major concerns for businesses and Internet users alike. According to a report, over 2.6 billion online records were stolen in 2016. To help you avoid data breach issues, cloud security solutions include various security protocols, and different controls. You have the freedom to choose the users who can access data outsourced to the cloud.