

Unit – 1 Introduction

Cloud Computing

The discovery of innovative technology goes back around 1960's and the evolution of cloud computing has seen multiple stages. We have come so far, and its equally important to know about how and when did cloud computing start empowering enterprises along with the entire history of cloud computing, before we dive into top trends in the future.

The term “cloud” was actually derived from telephony. Cloud computing is a technology that puts your entire computing infrastructure in both hardware and software applications online. It uses the internet, remote central servers to maintain data & applications. Gmail, Yahoo mail, Facebook, Hotmail, Orkut, etc are all the most basic and widely used examples of cloud computing. One does not need his own PC or laptop to check some stored mail/data/photos in the mailbox but any computer with an internet connection since the data is stored with the mail service provider on a remote cloud.

1.1 The evolution of cloud computing:-

In 1999, Salesforce.com started delivering of applications to users using a simple website. The applications were delivered to enterprises over the Internet, and this way the dream of computing sold as utility were true.

- In 2002, Amazon started Amazon Web Services, providing services like storage, computation and even human intelligence. However, only starting with the launch of the Elastic Compute Cloud in 2006 a truly commercial service open to everybody existed.
- In 2009, Google Apps also started to provide cloud computing enterprise applications.

1.2 Characteristics of cloud computing

Cloud Computing is getting more and more popularity day by day. The reason behind is the gradual growth of the companies which are in need of the place to store their data.

Following are the characteristics of Cloud Computing:-

Resources Pooling is an IT term used in cloud computing environments to describe a situation in which providers serve multiple clients, customers or “tenants” with provisional and scalable services. These services can be adjusted to suit each client's needs without any changes being apparent to the client or end user.

- **On-Demand Self-Service :-**

It is one of the important and valuable features of Cloud Computing as the user can continuously monitor the server uptime, capabilities, and allotted network storage.

- **Easy Maintenance :-**

The servers are easily maintained and the downtime is very low and even in some cases, there is no downtime. Cloud Computing comes up with an update every time by gradually making it better.

- **Large Network Access:-**

The user can access the data of the cloud or upload the data to the cloud from anywhere just with the help of a device and an internet connection. These capabilities are available all over the network and accessed with the help of internet.

- **Availability :-**

The capabilities of the Cloud can be modified as per the use and can be extended a lot. It analyzes the storage usage and allows the user to buy extra Cloud storage if needed for a very small amount.

- **Automatic System:-**

Cloud computing automatically analyzes the data needed and supports a metering capability at some level of services. We can monitor, control, and report the usage.

- **Security:-**

Cloud Security, is one of the best features of cloud computing. It creates a snapshot of the data stored so that the data may not get lost even if one of the servers gets damaged. The data is stored within the storage devices, which cannot be hacked and utilized by any other person. The storage service is quick and reliable.

- **Pay as you go :-**

In cloud computing, the user has to pay only for the service or the space they have utilized. There is no hidden or extra charge which is to be paid. The service is economical and most of the time some space is allotted for free.

1.3 Types of cloud and its Services

- Public cloud — data and other info delivered over the internet that can be shared with various people and organizations.
- Private cloud — data and other info that is only accessible to users within your organization.

- Hybrid cloud — a combination of the two. This environment uses public and private clouds.

1.3 AND its services

SaaS (Software as a Service):-

Otherwise known as Software as a Service, SaaS is a cloud-based method of providing software to users. This type of software is licensed on a subscription basis and hosted in the cloud. Users can log into and use a SaaS application from any compatible device over the internet. Google Drive, Dropbox, and Salesforce are all examples of SaaS.

PaaS (Platform as a Service):-

Platform as a Service, also known as PaaS, is similar to SaaS only instead of providing software, PaaS provides a platform for software creation. With PaaS, developers are provided with a framework that they can use to create and build customized applications. Examples include Windows Azure, Google App Engine, or OpenShift.

IaaS (Infrastructure as a Service) :-

Infrastructure as a Service delivers cloud computing infrastructure such as servers, networks, operating systems, and storage. Through a dashboard or an API, IaaS gives businesses complete control of the same technologies that a traditional data center provides without the need to physically maintain or manage those resources.

1.4 Application of cloud computing:-

1. Data Storage & Backup

Cloud is widely used to store and protect data.

- Store files, photos, videos online
- Automatic backup and recovery

Examples:

- Google Drive
- Dropbox

2. Web Hosting & Applications

Businesses host websites and apps on the cloud.

- Scalable hosting for websites
- Supports high traffic easily

Examples:

- Amazon Web Services
- Microsoft Azure

3. Big Data Analytics

Cloud helps process huge amounts of data quickly.

- Data analysis and visualization
- Business intelligence

Example:

- Google BigQuery

4. Artificial Intelligence & Machine Learning

Cloud platforms provide tools to build smart systems.

- Image recognition
- Chatbots
- Predictive analytics

Examples:

- Google Cloud Platform AI tools
- Microsoft Azure AI services

5. Online Gaming

Cloud supports multiplayer and streaming games.

- Real-time gaming
- No need for high-end hardware

Example:

- Xbox Cloud Gaming

1.6 Cloud Service Requirements

To effectively use cloud computing services, certain **basic requirements** must be met. These ensure smooth access, security, and performance.

1. Internet Connection

- A stable and reasonably fast internet connection is essential
- Cloud services work over the internet

Faster internet = better performance

2. Device (Client System)

- Any device like:
 - Computer
 - Smartphone
 - Tablet

Examples of access tools:

- Web browsers (Chrome, Edge)
- Apps like Google Drive or Dropbox

3. User Account

- You need an account to access cloud services

Examples:

- Google account for Google Drive
- Microsoft account for OneDrive

4. Cloud Service Provider

- A company that provides cloud infrastructure and services

Examples:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

5. Security Measures

- Strong passwords
- Encryption
- Authentication (e.g., 2-factor login)

Protects data from unauthorized access

6. Storage & Computing Resources

- Enough cloud storage space
- Processing power depending on the task

1.7 Cloud Infrastructure:-

It offers services on the host level, network level, and application level. Cloud infrastructure includes hardware and software components like servers, storage, network devices, virtualization software, and various other storage resources that are needed to support the cloud computing model.

Main Components of Cloud Infrastructure

1. Servers (Compute Power)

- Powerful computers that process data and run applications
- Hosted in large data centers

Example providers:

- Amazon Web Services
- Google Cloud Platform

2. Storage Systems

- Used to store data (files, databases, backups)
- Can scale up or down easily

Examples:

- Amazon S3
- Google Cloud Storage

3. Networking

- Connects servers, storage, and users
- Includes internet, routers, switches

✓ Ensures fast and secure data transfer

4. Virtualization

- Technology that creates virtual machines (VMs)

- Allows multiple systems to run on one physical server
- ✓ Improves efficiency and resource use

5. Management Software

- Tools to monitor and control cloud resources
- Handles automation, scaling, and security

1.8 Cloud Adoption

Cloud adoption is the process of **moving data, applications, and services from traditional (on-premise) systems to cloud environments.**

Types of Cloud Adoption

1. Full Cloud Adoption

- All systems are moved to the cloud
- No local servers

2. Partial (Hybrid) Adoption

- Some services stay on-premise, others move to cloud
- Very common approach

3. Multi-Cloud Adoption

- Using services from multiple providers
- Example: AWS + Azure together

Challenges in Cloud Adoption

- Data security concerns
- Migration complexity
- Cost management
- Need for skilled professionals
- Compliance and regulations

Why organizations Adopt Cloud

Companies choose cloud services from providers like Amazon Web Services, Microsoft Azure, and Google Cloud Platform for several reasons:

- **Cost savings** – no need to buy expensive hardware

- **Scalability** – easily increase or decrease resources
- **Remote access** – access systems from anywhere
- **High performance** – faster and more reliable systems
- **Better security options**

Unit – 2 Cloud reference and deployment models

2.1 Platform as a Service (PaaS):-

Platform as a Service, also known as PaaS, is similar to SaaS only instead of providing software, PaaS provides a platform for software creation. With PaaS, developers are provided with a framework that they can use to create and build customized applications. Examples include Windows Azure, Google App Engine, or OpenShift.

2.2 Software as a Service (SaaS):-

Otherwise known as Software as a Service, SaaS is a cloud-based method of providing software to users. This type of software is licensed on a subscription basis and hosted in the cloud. Users can log into and use a SaaS application from any compatible device over the internet. Google Drive, Dropbox, and Salesforce are all examples of SaaS.

2.3 Infrastructure as a Service (IaaS) :-

Infrastructure as a Service delivers cloud computing infrastructure such as servers, networks, operating systems, and storage. Through a dashboard or an API, IaaS gives businesses complete control of the same technologies that a traditional data center provides without the need to physically maintain or manage those resources.

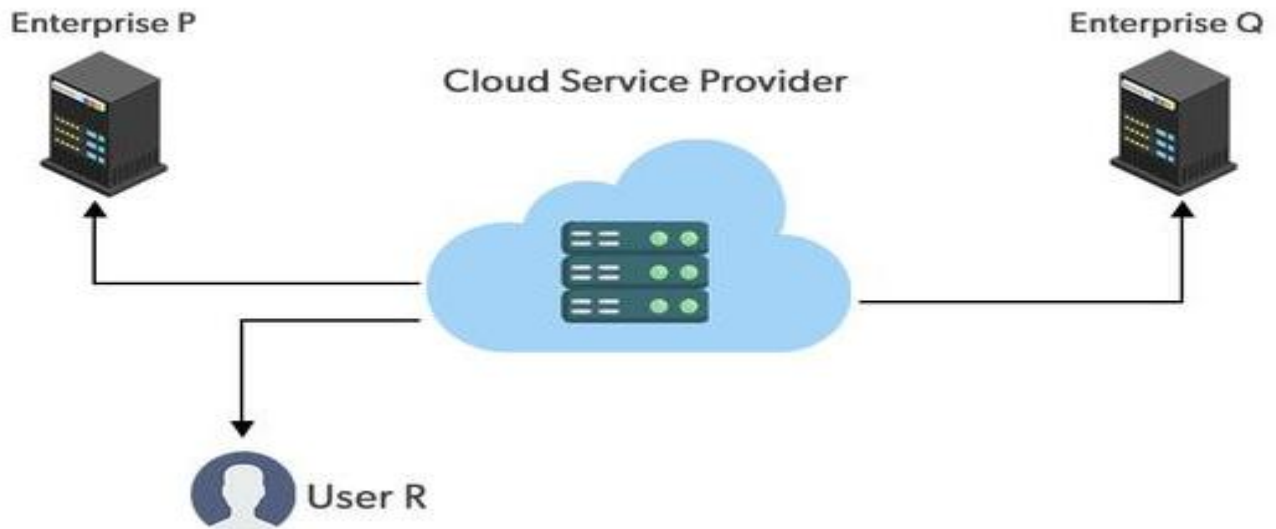
2.4 Public clouds

Public cloud — data and other info delivered over the internet that can be shared with various people and organizations. **public cloud** is a type of cloud computing where **services (like storage, servers, and applications) are provided over the internet by third-party companies** and shared among multiple users.

Examples of Public Cloud Providers

- Amazon Web Services

- Microsoft Azure
- Google Cloud Platform



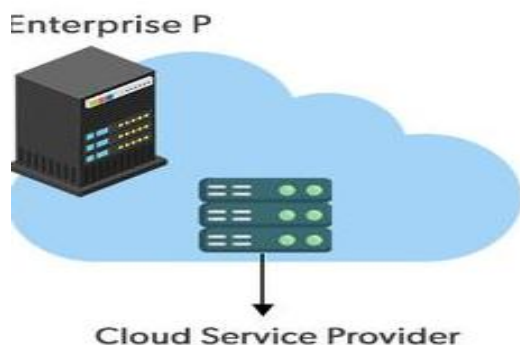
How It Works

- Data and applications are stored in remote data centers
- Users access them via the internet
- Resources are shared among many customers (multi-tenant system)

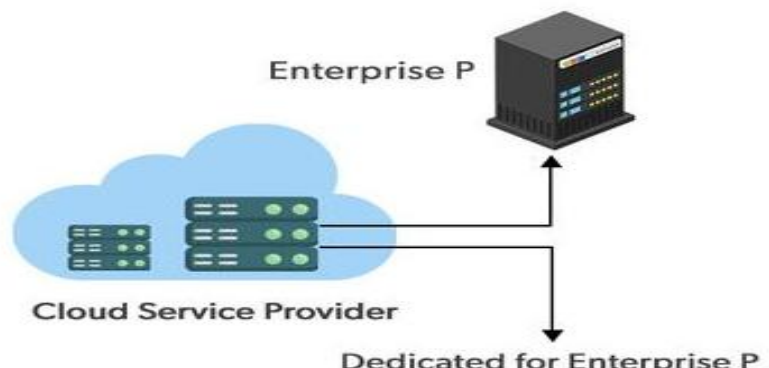
2.5 Private cloud:-

Private cloud — data and other info that is only accessible to users within your organizations. A **private cloud** is a cloud computing environment that is **used by only one organization**. It is not shared with the public, making it more **secure and controlled**.

On premise Private cloud



Externally hosted Private cloud



How It Is Managed

A private cloud can be:

- Hosted **inside the organization** (on-premise), or
- Managed by a third-party provider like Microsoft Azure or Amazon Web Services but dedicated only to one client

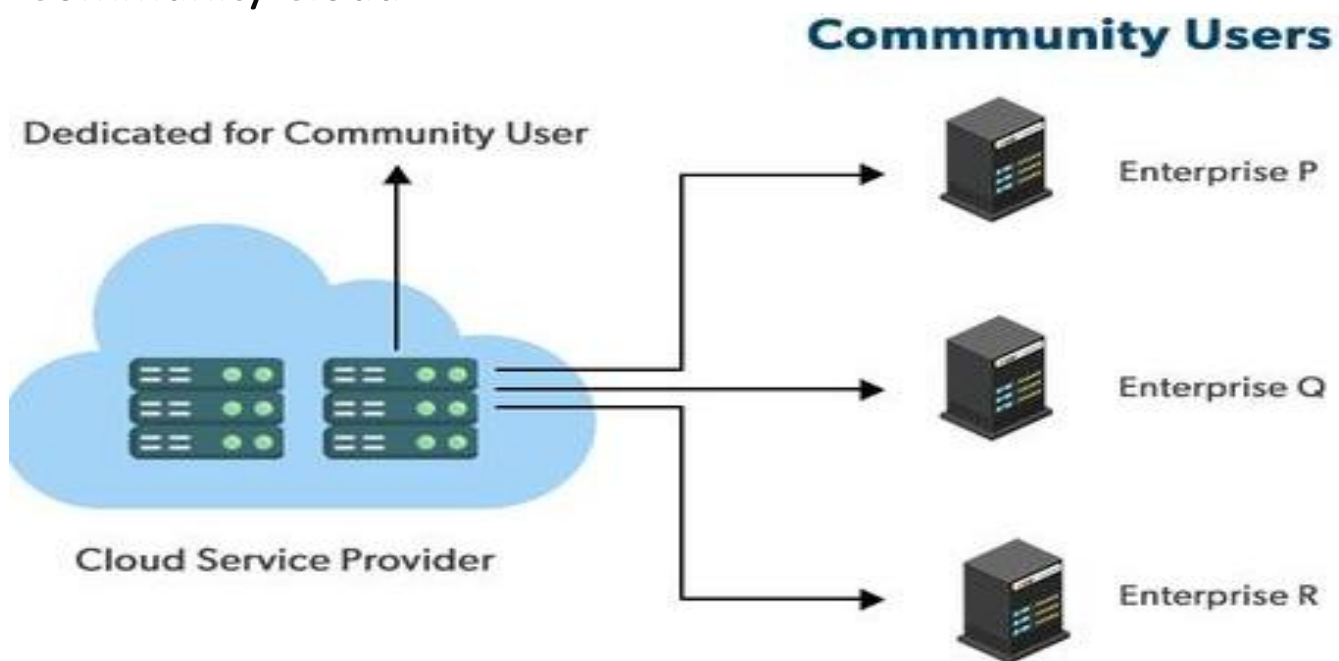
Features

- **High security** – not shared with others
- **Dedicated resources** – only one organization uses it
- **Full control** – customize as needed
- **Better compliance** – suitable for sensitive data

Advantages

- Strong data privacy and security
- Greater control over infrastructure
- Customizable environment
- Ideal for sensitive industries (banking, healthcare, government)

2.6 Community Cloud



A **community cloud** is a type of cloud computing where the **infrastructure is shared by several organizations that have similar needs**, such as security, policies, or industry requirements.

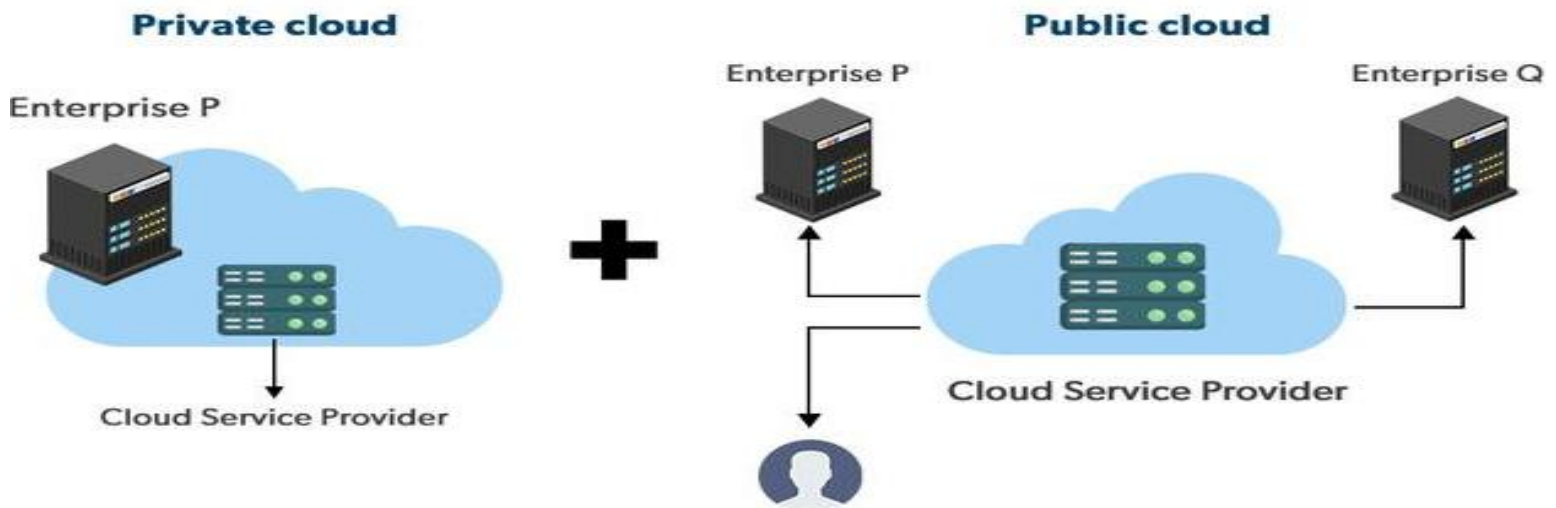
Features

- **Shared among similar organizations**
- **Better security than public cloud**
- **Designed for specific compliance needs**
- **Cost shared among users**

Advantages

- More secure than public cloud
- Cost is lower than private cloud (shared expenses)
- Customized for specific industry needs
- Supports collaboration between organizations

2.7 Hybrid Cloud:-



1. Definition: Hybrid cloud combines private cloud and public cloud for flexible use.
2. Allows data sharing between on-premises and cloud.
3. Provides scalability with public cloud resources.
4. Maintains security with private cloud control.
5. Cost-effective by balancing workloads.
6. Supports disaster recovery and backup.
7. Enables smooth migration of applications.
8. Useful for businesses needing both control and flexibility.

Unit - 3 Cloud Virtualization technology

3.1 Overview Of Virtualization Techniques:-

Virtualization is a process that allows a computer to share its hardware resources with multiple digitally separated environments. Each virtualized environment runs within its allocated resources, such as memory, processing power, and storage. With virtualization, organizations can switch between different operating systems on the same server without rebooting.

By using virtualization, we can interact with any hardware resource with greater flexibility. Physical servers consume electricity, take up storage space, and need maintenance.

3.2 Types of Virtualizations:-

Let's understand Guest OS and Host OS first. A guest operating system is the operating system installed on either a virtual machine (VM) or partitioned disk. It is usually different from the host operating system (OS). Simply put, a host OS runs on hardware while a guest OS runs on a VM.

3.2.1 Full virtualization:-

Full virtualization refers to the ability to run a program, most likely an operating system, directly on top of a virtual machine and without any modification, as though it were run on the raw hardware. Full virtualization is a type of virtualization in which the guest operating system is unaware that it is running in a virtualized environment. It uses a hypervisor to create and run multiple virtual machines (VMs) on a single physical server, with each VM having its own complete set of virtual hardware, including CPU, memory, storage, and network interfaces.

3.2.2 Para Virtualization:-

Paravirtualization is a virtualization technique in which the guest operating system is aware that it is running in a virtualized environment and requires modification to work efficiently. In paravirtualization, the guest OS interacts with the hypervisor to optimize performance and resource utilization, resulting in improved efficiency compared to full virtualization.

3.3 Virtualization Benefits:-

When virtualization is used correctly, it provides a firm foundation for all cloud computing efforts. Your storage devices, network resources, operating systems, hardware platforms and other key computing features remain secure, and you can comfortably scale any cloud infrastructure as necessary.

The **benefits** of virtualization in cloud computing include the following items:

1. Hassle-Free Data Transfers:-

Another benefit of virtualization in cloud computing is expedited data transfer. You can easily transfer data from physical storage to a virtual server, and vice versa. Virtualization in cloud computing can also handle long-distance data transfers.

2. Smoother IT Operations:-

Virtual networks help IT professionals improve efficiency in the workplace. These networks are easy to operate and faster to process, eliminating downtime and helping you save progress in real time Resource.

3. Efficient Resource Use :-

Virtualization improves hardware resources used in your data center. For example, instead of running one server on one computer system, you can create a virtual server pool on the same computer system by using and returning servers to the pool as required.

4. Protection from Failure and Disaster:-

Virtualization in cloud computing can prevent your IT system from failing. Even if one part of your system crashes, it doesn't mean the entire system will.

5. Cost-Effectiveness:-

Virtualization is a great way to cut expenses. If you store data on virtual servers or clouds, you won't have to buy physical hardware or systems.

3.4 Server Virtualization:-

Server virtualization is a process that partitions a physical server into multiple virtual servers. It is an efficient and cost-effective way to use server resources and deploy IT services in an organization. Without server virtualization, physical servers use only a small amount of their processing capacities, which leave devices idle.

3.5 Hypervisor Management Software:-

A hypervisor management software is a software that you can use to run multiple virtual machines on a single physical machine. Every virtual machine has its own operating system and applications. The hypervisor allocates the underlying physical computing resources such as CPU and memory to individual virtual machines as required. Thus, it supports the optimal use of physical IT infrastructure.

3.6 VMware Features And Infrastructure:-

3.6.1 Virtual Box :-

virtual box is a free and open-source virtualization software developed by Oracle. It allows users to create and run virtual machines on their host operating system. It enables users to install and run multiple operating systems on a single physical machine. It supports a wide range of guest operating systems, including Windows, Linux, macOS, and others. It provides features like snapshotting

(saving the state of a VM at a particular point in time), shared folders between the host and guest systems, and the ability to configure virtual hardware settings. . A virtual machine and VirtualBox are related but have key differences. A virtual machine (VM) is an emulation of a computer system that runs within a physical computer. It allows you to run multiple operating systems on a single machine.

3.6.2 Thin Client:-

A thin client is a virtual desktop computing model that runs services and software from a centralized server. Most people are familiar with desktop computers with software installed on a local drive that interacts with local hardware, all controlled by an operating system. With a thin client, only a monitor, network card, mouse, and keyboard are available to the end user, and other hardware and services run on the network. The primary advantages to thin client would be in an environment like a medium to large company, where the end user's systems are being used more as a terminal than as a full-on computer and each end user, or at least large groups of end users, will have the same needs and use the same software.

Unit – 4 Cloud Security

4.1 Introduction to Security

Since, cloud computing is the delivery of different services through the Internet. Therefore, it is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security.

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion.

The reality is that cloud is no more or less secure than on-premises security. So, security refers to the cybersecurity policies, best practices, controls, and technologies used to secure applications, data, and infrastructure in cloud environments. In particular, cloud security works to provide storage and network protection against

internal and external threats, access management, data governance and compliance, and disaster recovery.

4.2 Cloud Security Challenges And Risks

As cloud computing evolves, security threats keep changing, too. With cloud service providers constantly updating the threat landscape, security threats evolve, and new threats emerge daily. Additionally, as cloud service providers become more and more reliant on their cloud infrastructure to run their business processes and applications, security threats have the potential to impact their business.

- **Data Breaches**

A data breach is any security incident in which unauthorized parties gain access to sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) or corporate data (customer data records, intellectual property, financial information).

- **Attack Surface**

The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment.

- **Data Loss**

Data loss is an incident where data is destroyed, deleted, corrupted, or made unreadable by users and software applications.

- **Shadow IT**

Shadow IT is the use of information technology systems, devices, software, applications, and services without explicit IT department approval.

- **Hijacking**

In cybersecurity, hijacking refers to the unauthorized takeover of a computing system or network by an attacker. Here are a few common **types of hijacking attacks**:

1. **Session Hijacking:**

Also known as session fixation, this type of attack occurs when an attacker takes control of a user's session on a website or application.

2. **DNS Hijacking:**

In a DNS hijacking attack, the attacker intercepts or redirects Domain Name System (DNS) queries to malicious servers.

3. **Clickjacking:**

Clickjacking involves tricking a user into clicking on a hidden element on a web page by overlaying it with a transparent or opaque layer.

4. **Man-in-the-Middle (MitM) Attack:**

In a man-in-the-middle attack, the attacker intercepts communication between two parties without their knowledge.

5. Browser Hijacking:

Browser hijacking involves modifying a user's browser settings without their consent.

6. ARP Spoofing:

ARP spoofing is a type of attack where the attacker sends falsified Address Resolution Protocol (ARP) messages over a local area network.

4.3 Software-As-A-Service Security

SaaS (Software as a Service) security refers to the measures and processes implemented to protect the data and applications hosted by a SaaS provider. This includes security measures such as encryption, authentication, access controls, network security, and data backup and recovery.

SaaS security focuses on protecting data, applications, and user identities in the cloud. It deals with challenges in cloud-based software to keep information safe and available. SaaS security aims to reduce risks like unauthorized access and data exposure while enhancing the security of SaaS applications. It does not not only shield data and apps but also manages user identities effectively. It verifies and manages user access to cloud based resources.

4.4 Security Monitoring

Cloud security monitoring is the technic of continuously supervising both virtual and physical servers to analyze data for threats and vulnerabilities. Cloud security monitoring solutions often rely on automation to measure and assess behaviors related to data, applications and infrastructure.

When customer data is stored in the cloud, cloud monitoring can prevent loss of business and frustrations for customers by ensuring that their personal data is safe. The use of web services can increase security risks, yet cloud computing offers many benefits for businesses, from accessibility to a better customer experience.

4.5 Security Architecture Design

Cloud security architecture describes all the hardware and technologies designed to protect data, workloads, and systems within cloud platforms. It provides the written and visual model to define how to configure and secure activities and operations within the cloud, including such things as identity and access management; methods and controls to protect applications and data.

4.6 Data Security

Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers

everything—hardware, software, storage devices, and user devices; access and administrative controls; and organizations’ policies and procedures.

The process also helps organizations streamline their auditing procedures and comply with increasingly stringent data protection regulations. A robust data security management and strategy process enables an organization to protect its information against cyberattacks. It also helps them minimize the risk of human error and insider threats, which continue to be the cause of many data breaches.

4.7 Application Security

Cloud application security is the process of securing cloud-based software applications throughout the development lifecycle. It includes application level policies, tools, technologies and rules to maintain visibility into all cloud-based assets, protect cloud-based applications from cyberattacks and limit access only to authorized users.

Cloud application security is crucially important for organizations that are operating in a multi-cloud environment hosted by a third-party cloud provider such as Amazon, Microsoft or Google, as well as those that use collaborative web applications such as Slack, Microsoft Teams or Box.

4.8 Virtual Machine Security

Virtualization security has become a very important part of our lives. From cloud computing to virtual desktops, virtualization has changed how we live and work. It allows us to run multiple operating systems simultaneously without having to install them on each computer.

Simply, virtual security refers to protecting data centers from malicious attacks. It is a type software which refers to the implementation of security measures and policies within a virtual environment or infrastructure, such as virtual machines, servers, and networks. This approach allows for more flexible and scalable security management in cloud and virtualized data centers.

4.9 Identity Management and Access Control

Identity and access management (IAM) is the cybersecurity discipline that deals with how users access digital resources and what they can do with those resources. It is a way to tell who a user is and what they are allowed to do. IAM systems keep hackers out while ensuring that each individual user has the exact permissions, they need to do their jobs and not more than that.

5.1 Web Services

Before knowing Web Services, Let's talk about the internet. The Internet is a global medium for providing connectivity between devices. But it is just allowing these devices to connect to each other. It does not connect application or program so that we can communicate. For the communication between server and client we use a certain medium that is protocol (a web service application) which connect applications or programs. Web services provide the protocols for communicating and exchanging data between different web applications irrespective of underlying platform or language.

5.2 App Engine

App Engine is a fully managed, serverless platform for developing and hosting web applications at scale. It provides several popular languages, libraries, and frameworks to develop your apps, and then let App Engine take care of provisioning servers and scaling your app instances based on demand.

Google App Engine is a Platform as a Service (PaaS) offering from Google Cloud Platform that allows developers to build and host web applications on Google's infrastructure. With Google App Engine, developers can focus on writing code for their applications without having to worry about managing the underlying infrastructure, such as servers, storage, and networking. These applications are required to be written in one of a few supported languages, namely: Java, Python, PHP and Go.

5.3 Azures Platform

Azures is Microsoft's public cloud computing platform that provides a wide variety of services including compute, analytics, storage and networking. Users can pick and choose from these services to develop and scale new applications or run existing applications in the public cloud. It provides the following services.

- Compute services
- Data services
- Application services
- Network services

Services model of Azure:

- It was launched on February 1, 2010, significantly later than its main competitor, AWS.
- It's free to start and follows a pay-per-use model, which means you pay only for the services you opt for.

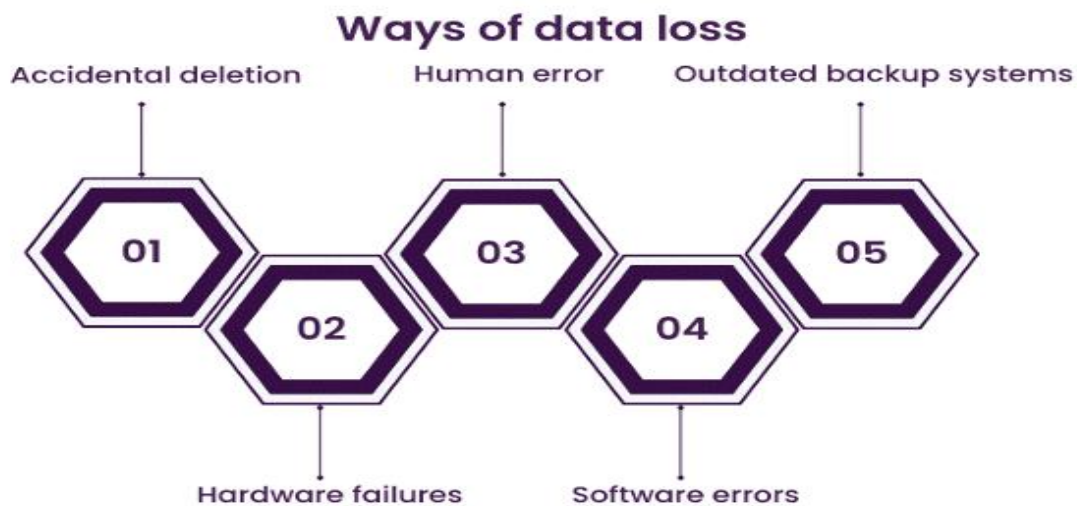
- Interestingly, 80 percent of the Fortune 500 companies use Azure services for their cloud computing needs.
- Azure supports multiple programming including Java, Node Js, and C#. languages,
- Another benefit of Azure is the number of data centers it has around the world. There are 42 Azure data centers spread around the globe, which is the highest number of data centers for any cloud platform. Also, Azure is planning to get 12 more data centers, which will increase the number of data centers to 54, shortly.

5.4 Aneka

Aneka is a cloud application development platform that allows building applications that can run on private, public, and hybrid clouds. It provides a scalable middleware (a web server is middleware that connects websites to the backend database. When you submit a form on a website, your computer sends the request in XML to the web server). that can deploy applications across heterogeneous computing resources. Aneka uses a service-oriented architecture and includes services for elasticity, runtime management, resource management, application management, and more. It supports programming models like MapReduce and can integrate with existing cloud technologies.

5.5 Open Challenges

Today, cloud computing has become an integral part of how businesses and individuals store, process, and access data and applications. However, there is quite a lot of ambiguity surrounding the cloud, and it has its own drawbacks when it comes to privacy concerns and data management. The list below discusses some of the key challenges in the adoption of cloud computing. Some of cloud computing challenges are:



5.6 Scientific Applications

Cloud services can be leveraged at a personal level as well as at an organizational level. At the personal level (also known as the lower level), the cloud can be used to store personal data. So instead of saving all our data on local memory e.g., computer hard disk and then worrying about the capacity of the disk, we can store our data on a cloud. Now we do not have to worry about the capacity of our local memory. We also do not have to worry about our data and its accessibility.

Cloud services offer some amount of capacity free of cost but in the future, if the size of our data increases, we can just extend the storage capacity by paying some amount of money. Another significant advantage of storing our data on the cloud is if someday our local memory (hard disk) got corrupted or crashes our data won't get affected because it is stored on the cloud.

5.7 Business and Consumer applications

Cloud Computing has indeed changed the way how business operates. There is plenty of business applications that a cloud computing system can support. Here are few ways of cloud computing business applications that may be useful for you.

- **Document Storage**

Cloud based document storage services lets you to store and access word files, pdfs, spreadsheets and many other data through your internet connection.

- **Website hosting**

Many users prefer cloud hosting rather than purchasing physical server to host your website.

- **Work Management**

Tracking and allocating of work is much easier with the help of cloud computing. If you have a team who are sitting at office or who are working on field or remotely then work management solution hosted on cloud is very much useful.

- **CRM (Customer Relationship Management)**

Customer Relationship Management Software solution is one of the widely used method to manage and improve customer relationships.

- **Sales & Marketing Management**

With the sales & marketing management system, you will always have an easy reach to the latest data. Track all the converted, potential customers or even enquiries.

UNIT-6 Cloud Application

6.1 Migration :-

To the Cloud migration is the process of moving applications, data, infrastructure, security, and other objects to a cloud computing environment. Typically, companies are moving data, applications, and IT workloads from on-premises servers to the public cloud, but cloud migration also includes moving data and applications from one cloud provider to another. The highly scalable, pay-as-you-go nature of the public cloud provides businesses with the flexibility to use only the resources needed, for only as long as needed, and pay only for those resources that are actually consumed. It's an attractive paradigm shift that entices businesses of all sizes and verticals.

6.2 Software Licenses:-

Every business uses software to manage various parts of the company. In most cases, the business agrees to certain terms or conditions to use that software. A software license is a contract between the owner of a software and the user, stating guidelines for the use of the software. This type of software license agreement grants the user access to software functions, though some have restrictions in place for how they can be used. The user can use the software without violating copyright. Various types of software license models are outlined in this blog. A software license is a document that provides legally binding guidelines for the use and distribution of software. Software licenses typically provide end .

6.3 Cloud Cost Model:-

Cloud cost models, describe the various methods that cloud providers may use to charge for their services. There are three major types of pricing providers tend to use – pay-as-you-go, reserved instances, and spot instances. The term “cloud costs models” is often used interchangeably with the term “cloud pricing models.”

6.4 Cloud Applications For Service Level:-

Such an agreement is called an SLA. SLA stands for Service Level Agreement. SLAs are not only used in cloud computing - they can be in place where any external service is being provided. However, they are commonly used for SaaS, IaaS, or PaaS products. As such, the definition of what a service level agreement is shifts. It all depends on what service is being provided.

6.5 Web Application Design:-

Web application design is an important stage when building a web application. It focuses on the look and feel of the web application in the wider context of software development. The web app design process encompasses several different aspects, including user interface design (UI), usability (UX), content production, and graphic design. Within this post, we focused mainly on UI and UX design.

6.6 Privacy design:-

Privacy by design (often called “privacy design”) is an approach in technology and systems development where **privacy is built into a product from the very beginning**, rather than added later as a fix.

Key principles of privacy by design

The concept was popularized by Ann Cavoukian, and it's based on 7 widely accepted principles:

1. Proactive, not reactive

Anticipate privacy risks before they happen, instead of responding after a breach.

2. Privacy as the default

Users shouldn't have to change settings to be protected—privacy is automatic.

3. Privacy embedded into design

Privacy is part of the system architecture, not an add-on feature.

4. Full functionality (not a trade-off)

You don't sacrifice usability or features for privacy—both should coexist.

5. End-to-end security

Protect data throughout its lifecycle (collection → storage → deletion).

6.7 Cloud for IoT:-

Let's understand IoT first, The term IoT, or Internet of Things, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves. Thanks to the advent of inexpensive computer chips and high bandwidth telecommunication, we now have billions of devices connected to the internet. This means everyday devices like toothbrushes, vacuums, cars, and machines can use sensors to collect data and respond intelligently to users. The Internet of Things (IoT) refers to a network of physical objects that are connected to the Internet so that they can exchange data and information in order to improve productivity, efficiency, services, and more.

6.8 Amazon Web Services for IoT:-

Amazon Web Services internet of things or AWS IoT is a platform that connects billions of IoT devices with AWS cloud services and other IoT devices. Think of it as a middle layer between IoT devices and various AWS services, providing bi-directional and secure communication between them, over the internet.

#	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)
1	Provides virtualized computing resources over the internet.	Provides a platform for software creation and deployment.
2	You have control over the Operating System (OS) and Runtime.	You only control the Application and its Data.
3	You manage patches, updates, and middleware.	The provider manages the OS, middleware, and runtime.
4	System Administrators and Network Architects.	Software Developers and Data Scientists.
5	Maximum flexibility to customize the entire stack.	Limited to the languages and tools supported by the platform.
6	Slower, as you must configure the environment first.	Faster, as you can start coding and deploying immediately.
7	You must manually scale or set up complex auto-scaling rules.	Typically offers "push-button" or automatic scaling.
8	Usually pay-as-you-go based on hardware allocation.	Usually based on platform usage or application resources.
9	High; requires deep knowledge of networking and OS.	Low to Moderate; abstracts away the technical "under-the-hood" work.
10	Harder to move (often tied to specific VM configurations).	Highly portable for code, but may have "provider lock-in" for tools.