Assignment - 2

Course: MIS 6363.005

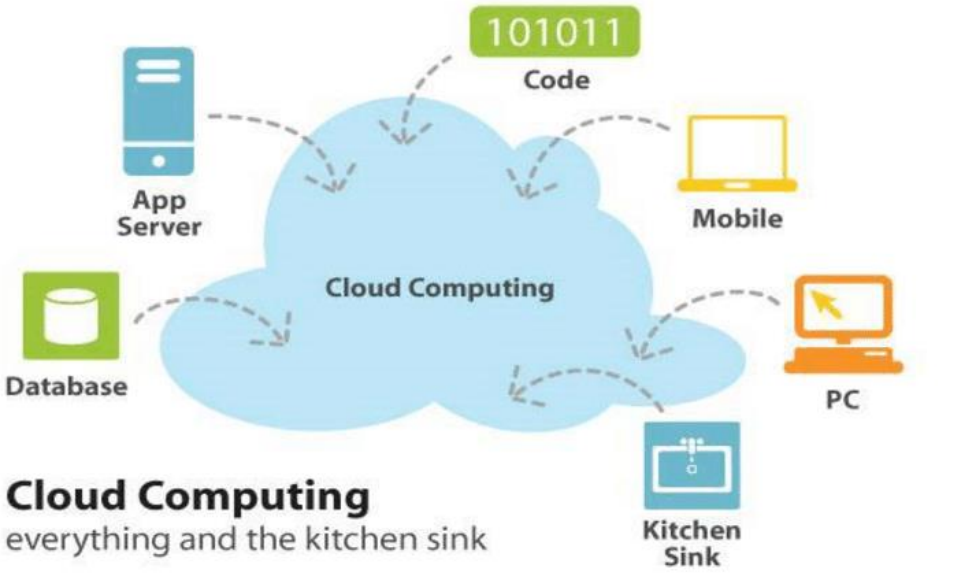
Name: **Anamika Das**

NetId: **axd240045**

1. What is Cloud Computing? Describe it in your own words

Cloud computing is fundamentally about providing computing services such as storage, servers, databases, and software **over the internet**, commonly known as "the cloud." Rather than purchasing, owning, and maintaining physical data centers or servers. It enables individuals and businesses to access their files, applications, and other computing resources on-demand from anywhere with an internet connection.

Cloud computing is built on a network of servers hosted in vast data centers worldwide, allowing cloud providers to deliver powerful, flexible, and highly available resources to users. It is an extensive **network of remote servers** around the world.



In my view, Cloud computing is like **renting** computing power and storage space over the internet. Instead of buying your own computers and servers, you can access these resources from a cloud provider, similar to renting **movies** or **music**. This allows you to scale your computing needs up or down as needed without the upfront costs or maintenance headaches.

2. Discuss the advantages and disadvantages of cloud computing.

Advantages of Cloud Computing

1. **Cost Savings**: Cloud computing eliminates the need for large upfront investments in physical infrastructure. Instead, users pay only for what they use, reducing both capital and operational expenses.
2. **Scalability and Flexibility**: Cloud services can be scaled up or down rapidly to meet changing needs, allowing businesses to adjust resources without investing in additional hardware or expansions.
3. **Availability and Mobility**: Cloud-based resources are accessible from anywhere with an internet connection, enabling employees to work remotely, collaborate, and access data from various devices worldwide.
4. **Business Continuity and Disaster Recovery**: Many cloud providers offer automated data backups, disaster recovery, and failover options, ensuring that organizations can recover data and resume operations even during disruptions.
5. **Automatic Software Updates**: Cloud providers handle routine software and security updates, ensuring users can always access the latest features and protections without requiring manual updates.
6. **Enhanced Collaboration**: Cloud computing allows teams to work together seamlessly on shared projects and documents in real-time, improving collaboration and productivity.

Disadvantages of Cloud Computing

1. **Downtime and Reliability Issues**: Cloud services depend on internet connectivity, making them susceptible to outages and slowdowns, which can disrupt business operations if the service provider experiences issues.
2. **Security and Privacy Risks**: Storing sensitive data on third-party servers can introduce security and privacy risks. Users or Organizations must ensure that cloud providers meet compliance requirements and have robust security protocols.
3. **Limited Control and Flexibility**: With public cloud services, users have limited control over the underlying infrastructure, as configurations, hardware, and updates are managed by the provider.
4. **Data Transfer Costs**: Moving large amounts of data to and from the cloud can incur significant transfer costs, which may affect businesses with high data transfer needs.

5. **Vendor Lock-In**: Migrating from one cloud provider to another can be challenging due to compatibility issues and data migration complexities, leading to potential dependency on a single provider.

3. Explain cloud deployment models and compare them.

Cloud Deployment Models

Cloud deployment models determine how cloud services are hosted, accessed, and managed. The primary cloud deployment models are **Public, Private, Hybrid**, and **Multi-Cloud**. Each model offers distinct benefits and limitations, making them suitable for different use cases and organizational needs.

1. Public Cloud

In a public cloud, services are provided by third-party vendors and delivered over the Internet **to multiple customers**. Examples include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

- **Advantages**:
    - **Cost-Effective**: Shared infrastructure reduces costs, as users pay only for resources they consume.
    - **Scalability**: Public clouds offer vast resources that can be scaled quickly in response to demand.
    - **Reduced Maintenance**: The cloud provider handles infrastructure maintenance, security, and updates.
- **Disadvantages**:
    - **Security and Privacy**: Sensitive data is stored on shared infrastructure, which may raise security and compliance concerns for regulated industries.
    - **Limited Customization**: Users have less control over the underlying infrastructure, as configurations are managed by the provider.

Best Suited For: Organizations with standard computing needs that prioritize cost savings and scalability, such as startups, smaller businesses, and companies with high variability in workloads.

2. Private Cloud

A private cloud is dedicated **to a single organization**, hosted either on-site or in a third-party data center. This model offers exclusive access to computing resources and greater control over the environment.

- **Advantages**:
    - **Enhanced Security**: Dedicated infrastructure allows for stricter access controls and custom security protocols, which is ideal for sensitive data.
    - **Customizable Environment**: Organizations have complete control over configurations, enabling tailored setups and compliance with specific industry standards.
- **Disadvantages**:
    - **Higher Cost**: Private clouds require more investment in infrastructure, maintenance, and management, making them more expensive.
    - **Limited Scalability**: Scaling a private cloud can be slower and may involve significant upfront costs for additional hardware.

Best Suited For: Organizations with stringent security and compliance requirements, such as financial institutions, government agencies, and healthcare providers.

3. Hybrid Cloud

A hybrid cloud combines elements of **both public and private clouds**, allowing data and applications to be shared between them. This model provides flexibility by using a private cloud for sensitive workloads and a public cloud for less-critical processes.

- **Advantages**:
    - **Flexibility**: Organizations can allocate resources according to workload sensitivity and compliance needs, optimizing costs and security.
    - **Scalability**: Non-sensitive operations can leverage the public cloud's scalability, while sensitive workloads remain in the private cloud.

    - **Enhanced Resilience**: Hybrid clouds offer backup options across different environments, enhancing business continuity.

- **Disadvantages**:
    - **Complexity**: Managing and integrating private and public environments requires specialized knowledge and can add complexity.
    - **Security Risks**: Data transfers between private and public clouds must be secure to prevent breaches, requiring careful management.

Best Suited For: Organizations needing both high security and flexibility, such as businesses with fluctuating or varied workloads.

4. Multi-Cloud

A multi-cloud approach involves **using multiple cloud services** from different providers simultaneously. Unlike hybrid cloud, multi-cloud environments don't necessarily combine private and public clouds; instead, they often leverage various public cloud providers.

- **Advantages**:
    - **Vendor Independence**: Multi-cloud reduces dependency on a single provider, allowing organizations to choose the best services from each provider and negotiate better terms.
    - **Improved Resilience**: Relying on multiple providers minimizes the impact of any single provider's downtime or outage.
    - **Performance Optimization**: Organizations can allocate specific workloads to the most appropriate provider based on performance or cost benefits.
- **Disadvantages**:
    - **Management Complexity**: Coordinating services and tools across different cloud providers can be challenging and requires strong cloud management skills.
    - **Increased Costs**: Using multiple providers may introduce additional costs for data transfer, integration, and management tools.

Best Suited For: Large enterprises with diverse, high-demand workloads that need flexibility and high resilience.

5. Community cloud

A community cloud is a collaborative cloud computing environment shared by a specific group of **organizations with common interests**. This shared infrastructure allows these organizations to pool resources, reduce costs, and enhance security and compliance.

It mainly shares resources **only between organizations**, such as with government institutions.

Comparison Summary

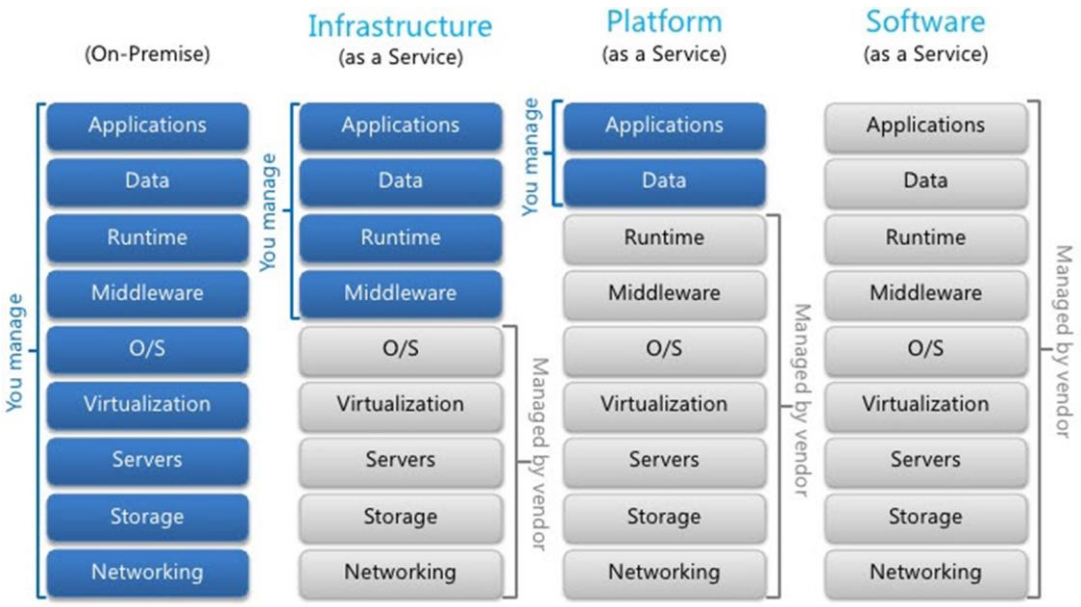
Deployment Model	Key Features	Benefits	Drawbacks	Best Fit
Public Cloud	Shared infrastructure, third-party managed	Cost-effective, scalable, low maintenance	Security concerns, limited control	Startups, SMEs, high-variability workloads
Private Cloud	Dedicated infrastructure for one organization	Enhanced security, customization	Higher cost, limited scalability	Regulated industries (finance, healthcare)
Hybrid Cloud	Mix of public and private cloud environments	Flexible, scalable, resilient	Complex management, data transfer security	Organizations with diverse security needs
Multi-Cloud	Uses multiple cloud providers	Vendor independence, resilience, optimized performance	Complex to manage, potential extra costs	Large enterprises needing flexibility and resilience

4. Discuss the shared responsibility model and comparison.

Shared Responsibility Model

The Shared Responsibility Model is a fundamental principle in cloud computing that delineates the responsibilities between a **cloud service provider** (CSP) and its **users**, especially for securing data and infrastructure. In this model, the CSP and the customer share the security responsibilities, with the exact roles depending on the type of cloud service - Infrastructure as a Service (**IaaS**), Platform as a Service (**PaaS**), or Software as a Service (**SaaS**).

As the below diagram shows, the balance of **responsibility shifts** as workloads move to the cloud:



Shared Responsibilities by Service Model

Infrastructure as a Service (IaaS):

- **Provider's Tasks**: Cloud Service Providers (like AWS, Azure, Google Cloud) responsible for the physical data centers, network firewalls, and hypervisors. They handle tasks like ensuring physical access controls and maintaining the virtual machines' isolation, protecting against threats that affect the hardware layer.
- **Customer's Tasks**: Customers handle most of the workload, including operating systems, patch management, data encryption, network security configurations (virtual

firewalls), and Identity and Access Management (IAM). Since IaaS offers the most control to customers, it also places a higher security burden on them.

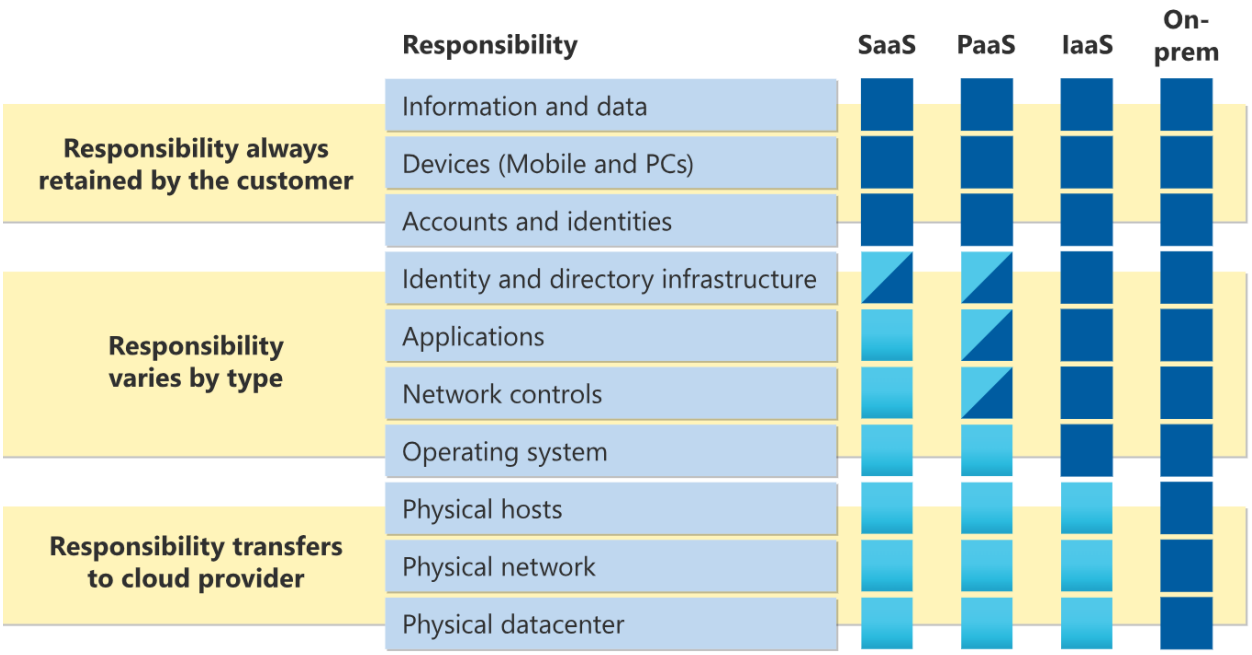
Platform as a Service (PaaS):

- **Provider's Tasks**: In PaaS, the CSP takes over the responsibility for the OS, runtime environment, and middleware, ensuring security updates and patches are applied. For example, in Microsoft Azure or AWS Elastic, the CSP manages everything up to the runtime.
- **Customer's Tasks**: Customers are still responsible for the applications they develop and the data they store. This includes implementing secure coding practices, managing user roles, and ensuring that data is encrypted as it moves to and from the platform.

Software as a Service (SaaS):

- **Provider's Tasks**: SaaS providers (like Salesforce, Microsoft 365, Google Workspace) manage the entire application, including maintenance, security patches, and infrastructure. They handle everything from data centers to the software used by end-users.
- **Customer's Tasks**: The customer's role mainly manages end-user permissions and data. They must also train users in safe practices, as human error is a common vulnerability in SaaS settings.

The below diagram shows how **responsibilities are distributed**:



Backup-as-a-Service (BaaS)

BaaS is a cloud-based service where a **provider takes on the responsibility** of backing up an organization's data. This typically involves storing copies of files, databases, and other digital assets in a secure, off-site cloud environment. BaaS automates and centralizes data backup, making it easier to manage than traditional on-premises backup solutions.

BaaS providers offer frequent, scheduled backups, reducing the risk of data loss.

Disaster-Recovery-as-a-Service (DRaaS)

DRaaS is a more comprehensive cloud-based solution aimed at **enabling full recovery** of applications, systems, and data **in the event of a disaster** (hardware failure, cyberattacks, or natural disasters). DRaaS not only stores data but also provides the infrastructure and tools needed to bring applications and systems back online quickly.

Provides near-instant access to a replicated environment, reducing Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

. Comparison of BaaS and DRaaS

Feature	Backup-as-a-Service (BaaS)	Disaster-Recovery-as-a-Service (DRaaS)
Primary Purpose	Data protection and retrieval	Full system and application recovery
Scope of Coverage	Files, databases, and specific data	Entire IT infrastructure, applications, and data
Recovery Capability	Limited to data recovery	Supports full failover for business continuity
RTO and RPO	Longer RTO/RPO, mainly for data access	Lower RTO/RPO for minimal downtime
Cost Structure	Lower cost, mainly storage-focused	Higher cost due to replication and failover needs
Management Complexity	Lower, often managed through a simple interface	Higher, involves planning and ongoing testing

5. How does Cloud Computing work?

Cloud computing works **by delivering computing resources**, such as servers, storage, databases, networking, software, analytics, and intelligence, over the internet, allowing users to access and use these resources remotely. Instead of relying on local servers or personal computers, cloud computing provides resources hosted by third-party data centers, which are accessible on demand.

Data Centers:

- Cloud providers operate massive data centers filled with servers.
- These servers store and process data.

Virtualization:

- Virtualization technology allows multiple virtual machines (VMs) to run on a single physical server.
- This enables efficient resource utilization and scalability.

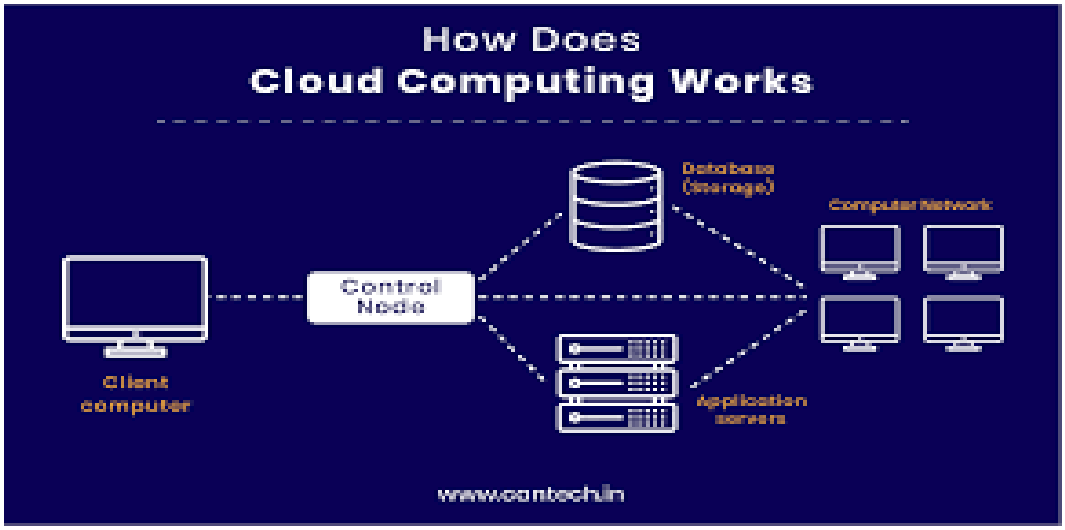
Network Connectivity:

- High-speed networks connect data centers and user devices.
- This ensures fast and reliable data transfer.

User Access:

- Users access cloud services through **web browsers** or APIs.
- They interact with cloud-based applications, servers, storage, and data.

This combination of virtualization, service models, deployment options, and robust infrastructure lets users access scalable, cost-effective computing resources whenever needed.



6. Research the history and development of the three major cloud providers.

The three major cloud providers - Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) - have unique histories and developmental paths shaping the modern cloud computing industry. Here's an overview of their development and impact on cloud technology:

Amazon Web Services (AWS)

- **Launch**: 2006, first to market.
- **Focus**: Broad range of services, popular for its scalability and pay-as-you-go model.
- **Strengths**: Large service variety, global infrastructure, dominance in the cloud market.
- **Broad Service Portfolio**: From storage and databases to machine learning and quantum computing, AWS leads in service variety and innovation.

Microsoft Azure

- **Launch**: 2010.
- **Focus**: Enterprise-friendly with hybrid cloud solutions.
- **Strengths**: Strong integration with Microsoft products like Windows and Office 365, hybrid and on-premises business solutions.
- **Hybrid Cloud Focus**: Azure emphasizes hybrid cloud solutions, connecting on-premises infrastructure with the cloud.

Google Cloud Platform (GCP)

- **Launch**: 2011.
- **Focus**: Data analytics, machine learning, and multi-cloud.
- **Strengths**: Advanced data tools like BigQuery, strong in AI and Kubernetes, open-source commitment.
- **Kubernetes and Containers**: Google created Kubernetes, an open-source container orchestration tool, which has become the industry standard. Google Kubernetes Engine (GKE) is now a popular service for managing containerized applications

Comparing AWS, Azure, and GCP

Feature	AWS	Azure	GCP
Initial Launch	2006	2010	2011
Market Focus	Broad (startups, enterprises)	Enterprise, Hybrid Cloud	Data & AI-centric, Multi-cloud
Strengths	Service variety, global reach, pay-as-you-go	Enterprise integration, hybrid cloud, Windows support	Data analytics, AI, open-source, Kubernetes
Major Innovations	EC2, S3, Lambda, AWS Outposts	Hybrid cloud, Azure AD, Cognitive Services	BigQuery, Anthos, TensorFlow, GKE
Service Count	~200+	~100+	~60+
Popular Offerings	EC2, S3, RDS, Lambda	Virtual Machines, SQL Database, Azure AD	BigQuery, GKE, Cloud Storage

7. Discuss the differences among these providers, providing a comparative analysis.

Amazon Web Services (AWS)**, Microsoft Azure, and Google Cloud Platform** (GCP) are the three dominant cloud providers offering unique services and strengths. Let's delve into their key differences:

Amazon Web Services (AWS)

- **Market Leader:** AWS is the oldest and most established cloud provider, offering many services.
- **Strengths:**
    - Extensive service catalog
    - Strong developer community
    - Mature infrastructure and reliability
- **Best For:**
    - Enterprises seeking a comprehensive cloud solution
    - Developers who prefer a wide range of tools and services

Microsoft Azure

- **Enterprise Focus:** Azure leverages Microsoft's strong enterprise relationships and software offerings.

- **Strengths:**
  - Integration with Microsoft products (e.g., Office 365, Azure AD)
  - Strong security and compliance features
  - Hybrid cloud capabilities
- **Best For:**
  - Organizations already using Microsoft products
  - Enterprises prioritizing security and compliance

Google Cloud Platform (GCP)

- **Data and AI Focus:** GCP excels in data analytics, machine learning, and artificial intelligence.
- **Strengths:**
  - Powerful data analytics tools (e.g., BigQuery)
  - Advanced machine learning capabilities
  - Strong performance and scalability
- **Best For:**
  - Data-intensive workloads
  - Organizations focused on AI and machine learning

Key Differences Summarized:

Feature	AWS	Azure	GCP
Market Share	Largest	Second Largest	Third Largest
Strength	Comprehensive services	Enterprise focus, hybrid cloud	Data analytics, AI
Best For	General-purpose cloud computing	Enterprises, hybrid cloud	Data-intensive workloads, AI/ML

8. Provide examples of a few services each provider offers (e.g., VM, storage, etc.).

Here are examples of key services offered by each cloud provider, **organized by category**:

1. Compute Services

- AWS:
  - **EC2 (Elastic Compute Cloud)** – Virtual machines with flexible configurations.
  - **Lambda** – Serverless computing for running code without managing servers.
- Azure:
  - **Virtual Machines** – Scalable VMs that support Windows and Linux.
  - **Azure Functions** – Serverless computing for running event-driven code.
- GCP:
  - **Compute Engine** – Customizable virtual machines for computing needs.
  - **Cloud Functions** – Serverless computing for lightweight, event-based code.

2. Storage Services

- AWS:
  - **S3 (Simple Storage Service)** – Scalable object storage.
  - **EBS (Elastic Block Store)** – Block storage for EC2 instances.
- Azure:
  - **Blob Storage** – Object storage for unstructured data.
  - **Azure Disk Storage** – Block storage for VMs.
- GCP:
  - **Cloud Storage** – Unified object storage with multi-regional options.
  - **Persistent Disks** – Block storage for VMs

3. Database Services

- AWS:
  - **RDS (Relational Database Service)** – Managed relational databases (e.g., MySQL, PostgreSQL).
  - **DynamoDB** – Managed NoSQL database service.
- Azure:
  - **Azure SQL Database** – Managed relational database as a service.
  - **Cosmos DB** – Globally distributed, multi-model database.
- GCP:
  - **Cloud SQL** – Managed relational databases (MySQL, PostgreSQL).
  - **Bigtable** – NoSQL database ideal for large-scale analytics

4. Networking Services

- AWS:
  - **VPC (Virtual Private Cloud)** – Customizable virtual networks.
  - **CloudFront** – Content delivery network (CDN) for fast content delivery.
- Azure:

    - **Virtual Network** – Private network within Azure.
    - **Azure Front Door** – Global load balancing and routing.
- GCP:
    - **VPC (Virtual Private Cloud)** – Private networking with global reach.
    - **Cloud CDN** – Content delivery network for caching and delivering content globally.

5. Artificial Intelligence and Machine Learning

- AWS:
    - **SageMaker** – End-to-end machine learning platform.
    - **Rekognition** – Image and video analysis service.
- Azure:
    - **Azure Machine Learning** – Comprehensive ML platform.
    - **Azure Cognitive Services** – Pre-trained AI models for language, vision, and speech.
- GCP:
    - **AI Platform** – Managed services for machine learning.
    - **AutoML** – Custom ML models with minimal expertise needed.

6. Analytics and Big Data

- AWS:
    - **Redshift** – Data warehousing for analytics.
    - **EMR (Elastic MapReduce)** – Managed Hadoop and Spark for big data processing.
- Azure:
    - **Synapse Analytics** – Data warehousing and big data analytics.
    - **HDInsight** – Managed Hadoop, Spark, and more for big data.
- GCP:
    - **BigQuery** – Serverless data warehouse with real-time analytics.
    - **Dataflow** – Managed service for real-time and batch data processing.

7. Security and Identity Management

- AWS:
    - **IAM (Identity and Access Management)** – Access control and security policies.
    - **AWS Shield** – DDoS protection for applications.
- Azure:
    - **Azure Active Directory** – Identity and access management.
    - **Azure Security Center** – Unified security management.
- GCP:
    - **Cloud IAM** – Identity and access management for GCP resources.
    - **Security Command Center** – Security and risk management for GCP.

9. Which cloud provider would you choose and why?

Choosing a cloud provider would depend on several key factors: specific needs of the business, budget, technical expertise, and goals. If there is an option to choose a cloud provider, I prefer **Microsoft Azure**. Here's a quick rundown of why I would choose it:

Reason to Choose Microsoft Azure:

Azure is widely used in enterprise settings, especially by universities and companies already integrated with Microsoft products (like Windows Server, Office 365, and Active Directory). As I am interested in enterprise, IT, or hybrid cloud setups, Azure is an excellent choice for me.

Benefits:

- **Student Benefits**: Azure offers free student accounts with $100 in credit and access to over 25 free services, including AI and machine learning tools.
- Integration with **Microsoft Products**: As I am familiar with Microsoft technologies, Azure is easy to start and integrates well.
- **Certifications**: Azure certifications are valuable, particularly for careers focused on enterprise IT or data science.

Ideal For: Since I am taking a Cloud Computing course, I have gained hands-on experience with various Azure services, including SQL, App Service, Blob Storage, Virtual Machines, Backup, Payment Plan, and more.

10. Artificial Intelligence and Cloud Computing.

Artificial Intelligence

Artificial Intelligence (AI) is the **simulation of human intelligence by machines**, particularly computers, to perform tasks that typically require human thought. These tasks include recognizing speech, interpreting images, making decisions, and even understanding natural language. AI systems learn from data, identify patterns, and make predictions or decisions with minimal human intervention.

AI is **used** across many industries to improve efficiency, decision-making, and innovation. Key applications include:

1. **Healthcare**: AI helps with diagnostics, drug discovery, personalized medicine, and robotic surgeries.
2. **Finance**: AI powers algorithmic trading, fraud detection, and credit scoring.
3. **Transportation**: AI enables self-driving cars, route optimization, and traffic management.
4. **Retail**: AI enhances product recommendations, inventory management, and customer service.
5. **Manufacturing**: AI predicts maintenance needs, automates tasks and ensures quality control.
6. **Entertainment**: AI is used for content recommendations, game development, and creating deepfakes.
7. **Education**: AI personalizes learning, automates grading, and provides tutoring.
8. **Security**: AI supports surveillance, cybersecurity, and fraud detection.
9. **Agriculture**: AI optimizes farming techniques, crop yields, and livestock monitoring.
10. **Energy**: AI improves energy efficiency, smart grids, and renewable energy management.

Advantages: AI enhances automating tasks, data analysis, personalization, and innovation while reducing costs and enabling new possibilities.

Disadvantages: It can lead to job losses, biases, privacy risks, high costs, and ethical concerns. Balancing AI's benefits with responsible use is key to maximizing its positive impact.

Cloud computing

Cloud computing **provides the infrastructure and tools** needed to develop and deploy AI applications, while AI enhances cloud platforms by improving automation, security, and resource management. This symbiotic relationship drives innovation in numerous industries, providing smarter solutions and improving overall efficiency.

AI Benefits from Cloud Computing:

- **Scalability**: AI and machine learning (ML) models often require large datasets and substantial computational resources. Cloud platforms like AWS, Azure, and Google Cloud provide scalable resources that can adjust to the demands of AI workloads.
- **Compute Power**: AI models, especially deep learning models, require significant computational resources such as GPUs or TPUs. Cloud providers offer these as part of their computing services (e.g., AWS EC2, Azure GPU instances, Google Cloud AI Platform), allowing developers to leverage high-performance hardware without owning it.
- **Data Storage**: AI applications require vast amounts of data for training models. Cloud storage services like AWS S3, Azure Blob Storage, and Google Cloud Storage provide cost-effective, scalable storage solutions for big data, enabling AI models to access and process the data efficiently.

Cloud Computing Benefits from AI:

- **Automation and Optimization**: AI can automate cloud resource management, such as scaling applications up or down based on demand or optimizing workloads for cost and performance. AI-driven automation tools help manage cloud environments more efficiently.
- **Predictive Analytics**: AI-powered predictive models can analyze usage patterns in the cloud, helping businesses predict resource consumption and optimize infrastructure accordingly. This reduces costs and increases efficiency.
- **Enhanced Security**: AI and machine learning algorithms are used to detect and respond to threats in real time. By analyzing network traffic, identifying anomalies, and

recognizing potential security breaches, AI can provide enhanced security for cloud environments.

- **Natural Language Processing (NLP)**: Cloud platforms often integrate AI-powered NLP to enable voice and text-based interactions for cloud services, making it easier for users to query data and interact with the system.

Artificial Intelligence (AI) and Cloud Computing complement each other to make advanced data processing and machine learning more accessible and scalable. The synergy between AI and cloud computing allows for more robust, agile, and cost-effective AI solutions, enabling rapid innovation across industries. The integration of **Artificial Intelligence** and **Cloud Computing** enables businesses to unlock new capabilities, scale AI models quickly, and manage large datasets efficiently.