Cloud Computing

Cloud computing refers to a technology that uses remote servers to store, manage and retrieve data from anywhere through out the world via internet rather than using local drives.

It does the following operations :

- Backup , Store and retrieve the data
- Streaming of audio and video
- Hosting blogs and websites
- Delivery of software on demand

Why cloud computing?

Generally, when an IT company is formed the company makes sure that it maintains a server room. Mostly the server room consists of the database servers, routers ,modems, mail servers and QPS(Query per second),high net speed and at last the maintenance engineers.

All this requires a lot of money to setup. To avoid all these we can use cloud computing services.

Characteristics of Cloud computing

- The chance of server failure is minimum.
- It offers various resources on demand to the users without having engineers at peak load.
- Multiple users and applications can work efficiently without any issue.
- Cloud computing enables users to access the resources from anywhere through out the world via internet.

Advantages of Cloud computing

- Once the data is stored in the cloud, it can be accessed easily from anywhere through out the world.
- Cloud applications provide collaborations of users where multiple users can share and retrieve the same data very easily.
- It reduces the software and hardware maintenance cost for the companies.

- Offers huge amount of storage capacity to the users to store all types of data.
- Cloud ensures that the data is stored with high security.

Disadvantages of Cloud computing

- Whenever we want to access the data in the cloud we definitely require a smooth internet connectivity. Otherwise it becomes difficult to upload or download the data.
- cloud infrastructure is completely owned, managed, and monitored by the service provider, so the cloud users have less control over the function and execution of services within a cloud infrastructure.
- Although cloud service providers implement the best security standards to store important information. But, before adopting cloud technology, you should be aware that you will be sending all your organization's sensitive information to a third party, i.e., a cloud computing service provider. While sending the data on the cloud, there may be a chance that your organization's information is hacked by Hackers.

History of Cloud Computing

Before the cloud computing technology was emerged there was client/server computing.

It is a centralized storage and all the data and controls store in the server side.

Whenever a user wants to interact with the server he/she gains a proper access over the server and then use it for their needs.

This is how the client/server computing worked before cloud computing came into the picture.

In 1962, John MacCharty suggested in a speech at MIT that computing can be sold for the users just like how the water and electricity is being sold daily.

It was a brilliant idea but the idea was ahead of its time, and after few decades the cloud computing technology was understood and came into existing technology int 1999.

In 1999,Salesforce.com was the first company which offered the applications to the users in a single website.

Later, Amazon in the year 2002 started AWS(Amazon Web Services) and became very successful.

In 2009,Google Apps started their cloud computing services.

Cloud computing Architecture

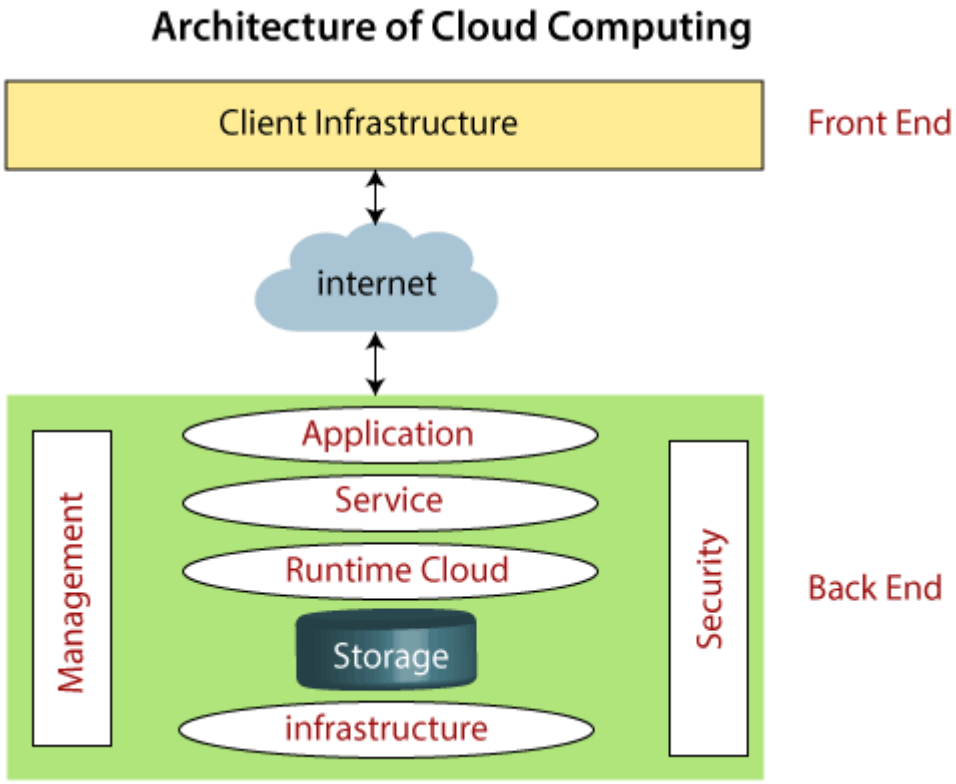
Generally, cloud computing technology is used by both small and large organizations.

It is a combinations of service oriented architecture and event driven architecture

The Architecture is divided into two parts:

1.Front end

2.Back end



Front end : The front end is used by the clients, It consists of user interfaces which display all the services and applications provided by the company.Front end includes web browsers, mobile device and computers.

Back end : Back end is managed by the service provider. It consists of the storage, security mechanism, servers, traffic control mechanisms.

Components of Cloud Computing Architecture

1. Client infrastructure : It is the User interface which is displayed to the user when ever the user wants to access the applications provided by particular company.
2. Applications : It is the applications or services provided by the service provider which would be used by the client.
3. Service : A cloud service manages what type of service is being demanded by the user.
   There are three types of cloud services :
   1.Software as a Service(SaaS)
   2.Platform as a Service(PaaS)
   3.Infrastructure as a Service(IaaS)
4. Run time Cloud : It provides execution and runtime environment to the virtual machines.
5. Storage : Storage is one of the main components of cloud computing. It is used to provide storage to the users.
6. Security : Security is an in-built mechanism in cloud computing.
7. Internet : Internet is the medium through which front end and back end interact with each other.

Grid Computing

Imagine you have a big puzzle to solve, but it's so massive that it would take you a really long time to finish it all by yourself. Now, imagine you have a bunch of friends who also want to help you solve this puzzle.

Grid computing is like getting all your friends together to work on different parts of the puzzle at the same time. Each friend has their own skills and abilities, so they can work on their piece of the puzzle independently. When everyone finishes their part, you can put all the pieces together to complete the puzzle much faster than you could have done on your own.

In a similar way, grid computing uses many computers connected over the internet to work on really big tasks. Each computer tackles a small part of the task, and when they're all done, the results are combined to solve the overall

problem faster and more efficiently. It's like teamwork for computers to solve challenging problems faster than a single computer could manage.

Cloud Computing vs Grid Computing

Cloud Computing	Grid Computing
Cloud Computing follows client-server computing architecture.	Grid computing follows a distributed computing architecture.
Scalability is high.	Scalability is normal.
Cloud Computing is more flexible than grid computing.	Grid Computing is less flexible than cloud computing.
Cloud operates as a centralized management system.	Grid operates as a decentralized management system.
In cloud computing, cloud servers are owned by infrastructure providers.	In Grid computing, grids are owned and managed by the organization.
Cloud computing uses services like Iaas, PaaS, and SaaS.	Grid computing uses systems like distributed computing, distributed information, and distributed pervasive.
Cloud Computing is Service-oriented.	Grid Computing is Application-oriented.
It is accessible through standard web protocols.	It is accessible through grid middleware.

How does cloud computing work

Assume that you are an executive at a very big corporation. Your particular responsibilities include to make sure that all of your employees have the right hardware and software they need to do their jobs. To buy computers for everyone is not enough. You also have to purchase software as well as software licenses and then provide these softwares to your employees as they require. Whenever you hire a new employee, you need to buy more software or make sure your current software license allows another user. It is so stressful that you have to spend lots of money.

But, there may be an alternative for executives like you. So, instead of installing a suite of software for each computer, you just need to load one application. That application will allow the employees to log-in into a Web-based service which hosts all the programs for the user that is required for his/her job. Remote servers owned by another company and that will run everything from e-mail to word

processing to complex data analysis programs. It is called cloud computing, and it could change the entire computer industry.

Security risks of cloud computing

Think of cloud computing like storing your important stuff in a shared storage room. While it's convenient, there are some security risks to consider:

1. **Data Breaches:** Just like someone could break into the storage room, hackers might try to access your cloud data without permission.
2. **Loss of Control:** Since your stuff is in someone else's storage room (cloud server), you have less control over its security measures.
3. **Data Loss:** If the storage room (cloud server) has a problem, like a fire or a crash, your stuff could get damaged or lost.
4. **Privacy Concerns:** If the storage room is managed by others, they might be able to see or use your stuff, even if it's unintentional.
5. **Account Hijacking:** If someone gets access to your "key" (account credentials), they could get into your storage room (cloud account) and mess with your stuff.

Types of cloud

- Public cloud
- Private cloud
- Hybrid cloud

Public cloud : It is open to all to store and access the information via internet using pay per usage method.

In this type of cloud all the resources are manages by cloud service provider.

Advantages

1. Can be owned at lower cost when compared to private and hybrid cloud.
2. Cloud is completely maintained by the cloud service provider.
3. Location independent and its services are delivered through internet.
4. There is no limit to the number of users.

Disadvantages

1. It is less secure.
2. Performance depends upon your internet speed.
3. The user has no control of data.

Private cloud : It is owned by an organization or company which is also known as internal cloud or corporate cloud. It is special built based on their requirements.

Advantages

1. Provides high level of security.
2. The organization has full control over the cloud as it is managed by them selves.
3. Can offer better performance with improved speed and accuracy.

Disadvantages

1. Skilled people are required to manage the cloud.
2. Since the cloud is private it can only be accessed with in a particular limit.

Hybrid cloud : It is the combination of public and private cloud.Hybrid cloud is partially secured because the services which are running on public cloud can be accessed by anyone while the services which run in private cloud can be accessed by the organization employees only.

Advantages

1. It reduce the risk
2. It can be used by the organizations which require more security than the public cloud.
3. Hybrid cloud offers flexible resources because of the public cloud and secure resources because of the private cloud.

Disadvantages

1. The security feature is not as good as private cloud.
2. It is more difficult to manage the hybrid cloud.

Community cloud : It allows the systems and services to be accessible by a group of organizations to share and receive the information between the organizations. It is owned and managed by the one or more organizations of that community.

Advantages

1. It is cost effective since the cloud is being shared by several organizations.
2. Provides better security than public cloud.
3. It provides collaborative and distributive environment.

Disadvantages

1. Security feature is not as good as private cloud.
2. It is not suitable if collaboration is not required.

Cloud service models

1.**IaaS** : Infrastructure as a service is also known as Hardware as a service. It is a computing infrastructure managed over the internet. It helps users avoid cost and complexity of buying and setting up the physical servers or storage.

Customers access these resources on the Internet using a pay-as-per use model.

Advantages

1. With Iaas,you don’t need to invest in and maintain the physical servers or storage devices which can be expensive.Instead, you pay for the resources and use them accordingly.
2. Iaas allows easy acalability of resources based on the need. Suppose, if your website has become popular then you can add up more virtual servers on the spot wot handle the traffic and reduce them accordingly.
3. The cloud service provider handles all your servers and storage making your team focus more on other things.
4. This service can be accessed over internet, so it can be accessed anywhere through out the world.

Disadvantages

1. All your data is sent to the cloud service provider.so, it is still a big security concern for any one because we are sending it to some unknowns and we don’t know what happens there.
2. If there is no proper internet speed then this service might not work properly for the user.

3. With IaaS, you are just renting the hardware from cloud provider.this means you have less control over the underlying hardware control.

2.**PaaS** : It is known as Platform as a service which is designed for the programmer to develop to test, run, manage and develop applications.

PaaS is a cloud service that provides you with all the tools you need to build and run your application. You don't have to worry about buying and setting up servers or software. Instead, you use the tools provided by the PaaS provider.

Advantages

1. PaaS follows a pay-as-you-go model, which means you only pay for the resources you use
2. PaaS provides pre-configured tools and frameworks that simplify the development process. This means developers can focus on writing code and building features rather than setting up and managing the underlying infrastructure.
3. With PaaS, developers can start building and deploying applications quickly. The ready-to-use environment eliminates the need to handle complex setup tasks, allowing for faster development and quicker release of applications.
4. PaaS provides a collaborative environment where multiple team members can work on the same project simultaneously. This enhances teamwork and accelerates development cycles.

Disadvantages

1. Paas offers less control over the environment.
2. While PaaS offerings support a wide range of programming languages and frameworks, you might encounter compatibility issues if your application relies on specialized or older technologies.
3. If you decide to switch to a different PaaS or bring certain services in-house, migrating your application and data can be complex and time-consuming.

3.**SaaS** : It is also known as Software as a service. Imagine you want to watch movies or listen to music. Instead of buying DVDs or CDs and playing them on

your own equipment, you can use streaming services like Netflix or Spotify. You don't need to worry about the technical stuff; you just use the service and enjoy the content.

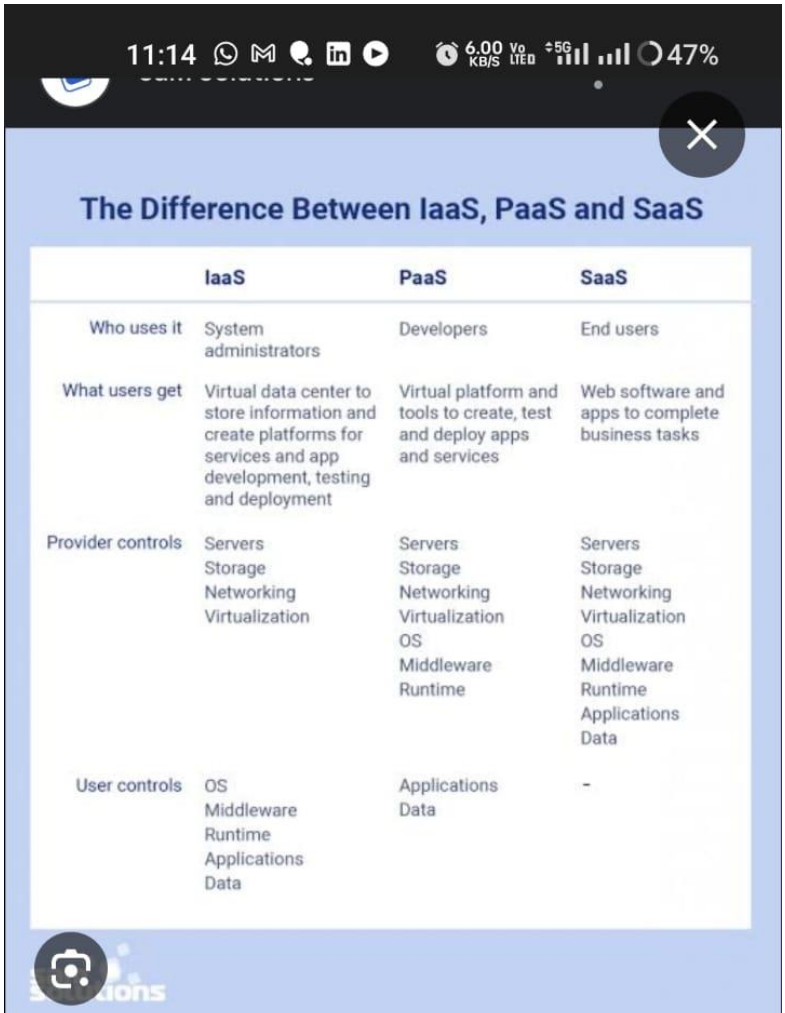
Now, think about software applications you use for work or personal tasks. Instead of installing these applications on your computer, SaaS lets you access and use them over the internet. You don't have to manage the software's installation, updates, or maintenance – the service provider handles all of that.

Advantages

1. With Saas, you can access the applications from anywhere through out the world using internet.
2. The service provider takes care about the complete application so there is no need to look up on the application i.e less maintainance is required.
3. With Saas, you can immediately start using the service once you have subscribed to the service.

Disadvantages

1. Storing sensitive data in the cloud might raise security and privacy concerns, especially for industries with strict regulations.
2. SaaS requires a reliable internet connection. If your connection is slow or goes down, it can affect your ability to use the software.
3. Since the software runs on the provider's servers, the performance might vary based on their infrastructure load and the number of users.
4. Your ability to use the software depends on the availability and reliability of the SaaS provider's servers. Downtime on their end can impact your access.



The Difference Between IaaS, PaaS and SaaS

	IaaS	PaaS	SaaS
Who uses it	System administrators	Developers	End users
What users get	Virtual data center to store information and create platforms for services and app development, testing and deployment	Virtual platform and tools to create, test and deploy apps and services	Web software and apps to complete business tasks
Provider controls	Servers Storage Networking Virtualization	Servers Storage Networking Virtualization OS Middleware Runtime	Servers Storage Networking Virtualization OS Middleware Runtime Applications Data
User controls	OS Middleware Runtime Applications Data	Applications Data	-

IaaS vs. PaaS vs. SaaS. Advantages and Disadvantag...

Visit

Images may be subject to copyright. Learn more

Citrusbug

Discover Search Saved

Virtual Private Cloud

In a public park, many people can visit and use the space. But if you want a special, private area just for your family and friends, you can put up a fence around a section of the park. Inside that fenced area, you have your own space, and others can't easily see or access it.

Similarly, in cloud computing, a VPC is like your fenced-off area within a cloud provider's big computer network. It's a way to create your own private space in the cloud where you can put your digital stuff like websites, databases, and applications. This space is separate from what other people are doing in the cloud, and you have control over who can enter or exit it.

So, a VPC helps you keep your digital things private and secure while using cloud services.

Public IP in cloud computing

In the context of cloud computing, think of a public IP address like a phone number for your computer or server that's connected to the internet. Just as you need a phone number for people to call you, your computer or server needs a public IP address so that other computers on the internet can connect to it.

Accessibility: A public IP address allows your cloud-based computer or server to be reached from anywhere on the internet. It's like having a phone that anyone can call from anywhere in the world.

Uniqueness: Just as each phone number is unique, public IP addresses are also unique. No two devices on the internet can have the same public IP address at the same time.

Private IP in the context of cloud computing

In the context of cloud computing, a private IP address is like an address within a secret club or a private neighborhood. It's used to communicate between computers or servers within your own private space in the cloud, and it's not meant to be accessible from the wider internet.

Here are some simple points about private IP addresses in cloud computing:

1. **Internal Communication:** Private IP addresses are used for computers or servers to talk to each other within your private cloud network. It's like having a secret language that only your friends in the club understand.
2. **Isolation:** Just as a secret club is separate from the public, your private cloud network is separate from the public internet. This means that the resources with private IPs can't be directly reached from outside your private network, adding an extra layer of security.
3. **Security:** Because private IPs are not directly accessible from the internet, they help keep your internal resources safe from potential threats or unauthorized access. It's like having a locked gate to keep out unwanted visitors.

Infrastructure as Code

Infrastructure as Code (IaC) in cloud computing is like creating a recipe for building and managing your computer servers and other resources using code, just like a chef follows a recipe to cook a meal.

Here's a simple explanation of IaC and its use:

1. **Building and Managing Infrastructure with Code:** Instead of setting up servers and networks manually, IaC lets you write code that describes how your cloud infrastructure should be created and configured. It's like writing down the steps for building a LEGO castle.
2. **Automation:** Once you have this code (your "recipe"), you can use automation tools to build, change, and manage your cloud resources. It's like having a robot chef follow your recipe to cook your meals automatically.
3. **Consistency:** IaC ensures that your infrastructure is always set up the same way every time you need it. It's like always getting the same delicious pizza from your favorite pizza place because they follow the same recipe.

4. **Scalability:** You can easily scale your infrastructure up or down by changing your code. It's like deciding to cook dinner for one or for a big party, and your recipe adjusts accordingly.

How can you ensure the security of resources deployed in the cloud?

Ensuring the security of resources deployed in the cloud is a critical aspect of cloud computing. Cloud security is a shared responsibility between the cloud service provider (CSP) and the cloud customer. Here are several important practices to help secure your resources in the cloud:

Identity and Access Management (IAM):

- Use strong authentication methods like multi-factor authentication (MFA) for user accounts.

Data Encryption:

Encrypt data both in transit and at rest using encryption protocols and services provided by the cloud provider.

Network Security:

- Create a Virtual Private Cloud (VPC) or similar network segmentation to isolate resources and control traffic flow.
- Implement security groups, network access control lists (NACLs), and firewalls to control inbound and outbound traffic.

Security Monitoring and Logging:

Implement monitoring tools to detect and alert on suspicious activities or security incidents.

Employee Training and Awareness:

Train your employees and teams on security best practices, including phishing awareness and safe cloud resource usage.

Foster a culture of security awareness within your organization.

Data Backup and Recovery:

Regularly back up critical data and test data recovery processes to ensure data integrity and availability in case of data loss.

Continuous Improvement:

Stay informed about evolving security threats and best practices in cloud security.

Continuously assess and improve your security measures to adapt to changing risks and technologies.

Cloud based solutions

1. **Load Balancers**:
    - **What they do**: Load balancers distribute incoming web traffic or requests across multiple servers to ensure that no single server gets overwhelmed, improving the overall performance and reliability of a web application.
    - **How they work**: Imagine a restaurant with multiple waiters. When customers arrive, a host (the load balancer) directs each customer to an available waiter (server). This way, no single waiter becomes too busy, and customers get faster service.
2. **Auto-Scaling**:
    - **What it does**: Auto-scaling automatically adjusts the number of servers or resources in your cloud infrastructure to handle changes in traffic or demand, ensuring your application stays responsive and cost-effective.
    - **How it works**: Think of it like a thermostat in your home. When it gets colder, the thermostat turns on the heat, and when it gets warmer, it turns it off. Auto-scaling monitors your website's traffic, and when it sees more visitors, it adds more servers. When traffic decreases, it removes unnecessary servers to save money.
3. **Content Delivery Network (CDN)**:
    - **What it does**: CDNs are networks of servers distributed worldwide that store and deliver website content (like images, videos, and web pages) to users from a server location closest to them. This speeds up content delivery and reduces server load.

- **How it works**: Think of it as a chain of post offices. Instead of mailing a letter directly to someone far away, you drop it at your local post office. The post office closest to the recipient forwards the letter quickly. Similarly, CDNs store your website's content on servers around the world. When a user accesses your site, the CDN serves content from the nearest server, reducing the time it takes to load your web pages.

AWS Lambda

What is AWS Lambda? AWS Lambda is like a magical computer that automatically does tasks for you when you need them, without you having to worry about setting up or maintaining the computer.

When would you use AWS Lambda? You would use AWS Lambda when you have small pieces of code, called "functions," that need to run in response to specific events or triggers. Here are some examples:

1. **Auto-Scaling**: When your website or application gets more visitors, Lambda can automatically add more computing power to handle the increased load.
2. **File Processing**: If you want to resize images when they're uploaded to a storage service like Amazon S3, Lambda can do it for you as soon as the file is added.
3. **Real-time Data Processing**: Lambda can process data from streaming sources like IoT devices, sensors, or logs, and take actions based on that data.
4. **Scheduled Tasks**: You can schedule Lambda functions to run at specific times or intervals. For example, you could use it to regularly clean up old data or send out automated emails.

How would you monitor the performance of a cloud application? Mention some monitoring tools or services.

Application-Level Monitoring:

- Logs: Monitor application logs for errors, warnings, and performance-related information. Services like AWS CloudWatch Logs, Loggly, or the

ELK Stack (Elasticsearch, Logstash, Kibana) are popular for log management.

- Metrics: Collect and analyze application-specific metrics such as response times, error rates, and resource utilization. Tools like AWS CloudWatch, Prometheus, or Datadog can help with this.

End-User Experience Monitoring:

Real User Monitoring (RUM): Track how actual users experience your application, including page load times and interactions. Tools like New Relic, Dynatrace, and Google Analytics can provide RUM capabilities.

Security Monitoring:

- **Security Logs**: Monitor security logs for unauthorized access attempts and potential breaches. AWS GuardDuty, Azure Security Center, and tools like Security Information and Event Management (SIEM) solutions help with this.

Cost Monitoring: - Keep an eye on your cloud resource costs using cloud cost management tools like AWS Cost Explorer, Azure Cost Management, and Google Cloud Cost Management.

What strategies would you implement to ensure high availability and disaster recovery in a cloud environment?

High Availability (HA):

1. Multi-Region Deployment: Deploy your application across multiple geographical regions of your cloud provider. This ensures redundancy and resilience in case one region experiences an outage.
2. Load Balancing: Use load balancers to distribute traffic across multiple instances or servers. This prevents overloading a single server and provides redundancy.
3. Auto-Scaling: Implement auto-scaling to dynamically adjust resources based on traffic or demand. This ensures your application can handle increased loads without manual intervention.
4. Database Replication: Set up database replication across different availability zones or regions. This ensures data availability even if one database instance fails.

Disaster Recovery (DR):

1. Data Backup and Versioning: Regularly back up your data and retain multiple versions. Use object storage like AWS S3 or Azure Blob Storage for durability.
2. Cross-Region Replication: Replicate critical data and resources to a different region or cloud provider to safeguard against regional failures.
3. Backup and Restore Testing: Periodically test your backup and restore processes to ensure they work as expected.
4. Geographic Diversity: Choose disaster recovery sites in regions with a low likelihood of experiencing simultaneous disasters to minimize the risk of dual failures.

How can you optimize costs when using cloud resources?

1. **Rightsize Resources**:
    a. Choose cloud resources (e.g., instances, storage) with the right amount of compute power and capacity for your workload. Avoid over-provisioning or under-provisioning.
2. **Utilize Auto-Scaling**:
    a. Implement auto-scaling to adjust resources dynamically based on demand. This prevents overpaying for idle resources during periods of low activity.

Monitor and Analyze Costs: Regularly monitor your cloud costs using cloud provider cost management tools or third-party solutions. Identify cost outliers and investigate unexpected spikes.

Budgeting and Alerts:

- Set up budgets and cost alerts to notify you when spending exceeds predefined thresholds. This helps you stay within budget and take action if costs rise unexpectedly.