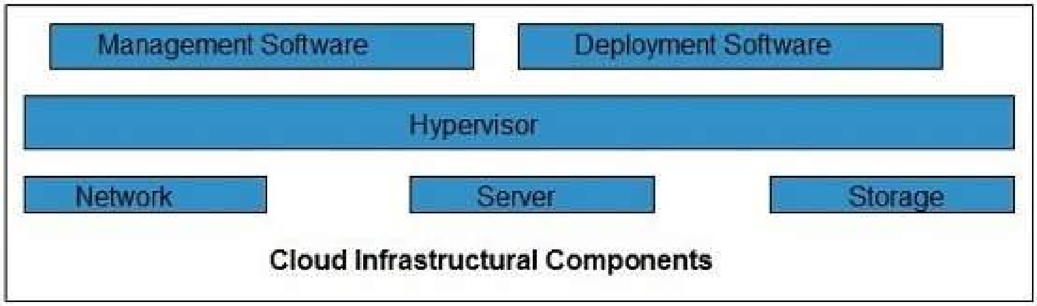
CLOUD COMPUTING TEST QUESTIONS

Test 1

Q1) What are the different cloud infrastructure components?

Ans: Cloud infrastructure consists of servers, storage devices, network, cloud management software, deployment software, and platform virtualization.



Cloud Infrastructural Components

Hypervisor

Hypervisor is a firmware or low-level program that acts as a Virtual Machine Manager. It allows to share the single physical instance of cloud resources between several tenants.

Management Software

It helps to maintain and configure the infrastructure.

Deployment Software

It helps to deploy and integrate the application on the cloud.

Network

It is the key component of cloud infrastructure. It allows to connect cloud services over the Internet. It is also possible to deliver network as a utility over the Internet, which means, the customer can customize the network route and protocol.

Server

The server helps to compute the resource sharing and offers other services such as resource allocation and de-allocation, monitoring the resources, providing security etc.

Storage

Cloud keeps multiple replicas of storage. If one of the storage resources fails, then it can be extracted from another one, which makes cloud computing more reliable.

Q2) Write about the different Cloud deployment models?

Ans: **Public Cloud**

The public cloud makes it possible for anybody to access systems and services. The public cloud may be less secure as it is open to everyone. The public cloud is one in which cloud infrastructure services are provided over the internet to the general people or major industry groups.

Advantages of the Public Cloud Model

- Minimal Investment: Because it is a pay-per-use service, there is no substantial upfront fee, making it excellent for enterprises that require immediate access to resources.
- No setup cost: The entire infrastructure is fully subsidized by the cloud service providers, thus there is no need to set up any hardware.
- Infrastructure Management is not required: Using the public cloud does not necessitate infrastructure management.
- No maintenance: The maintenance work is done by the service provider (not users).
- Dynamic Scalability: To fulfill your company's needs, on-demand resources are accessible.

Disadvantages of the Public Cloud Model

- Less secure: Public cloud is less secure as resources are public so there is no guarantee of high-level security.
- Low customization: It is accessed by many public so it can't be customized according to personal requirements.

Private Cloud

The private cloud deployment model is the exact opposite of the public cloud deployment model. It's a one-on-one environment for a single user (customer). There is no need to share your hardware with anyone else.

It is also called the "internal cloud" & it refers to the ability to access systems and services within a given border or organization. The cloud platform is implemented in a cloud-based secure environment that is protected by powerful firewalls and under the supervision of an organization's IT department.

Advantages of the Private Cloud Model

- Better Control: You are the sole owner of the property. You gain complete command over service integration, IT operations, policies, and user behavior.
- Data Security and Privacy: It's suitable for storing corporate information to which only authorized staff have access. By segmenting resources within the same infrastructure, improved access and security can be achieved.
- Supports Legacy Systems: This approach is designed to work with legacy systems that are unable to access the public cloud.
- Customization: Unlike a public cloud deployment, a private cloud allows a company to tailor its solution to meet its specific needs.

Disadvantages of the Private Cloud Model

- Less scalable: Private clouds are scaled within a certain range as there is less number of clients.
- Costly: Private clouds are more costly as they provide personalized facilities.

Hybrid Cloud

By bridging the public and private worlds with a layer of proprietary software, hybrid cloud computing gives the best of both worlds. With a hybrid solution, you may host the app in a safe environment while taking advantage of the public cloud's cost savings. Organizations can move data and applications between different clouds using a combination of two or more cloud deployment methods, depending on their needs.

Advantages of the Hybrid Cloud Model

- Flexibility and control: Businesses with more flexibility can design personalized solutions that meet their particular needs.
- Cost: Because public clouds provide scalability, you'll only be responsible for paying for the extra capacity if you require it.
- Security: Because data is properly separated, the chances of data theft by attackers are considerably reduced.

Disadvantages of the Hybrid Cloud Model

- Difficult to manage: Hybrid clouds are difficult to manage as it is a combination of both public and private cloud. So, it is complex.
- Slow data transmission: Data transmission in the hybrid cloud takes place through the public cloud so latency occurs.

Community Cloud

It allows systems and services to be accessible by a group of organizations. It is a distributed system that is created by integrating the services of different clouds to address the specific needs of a community, industry, or business. The infrastructure of the community could be shared between the organization which has shared concerns or tasks. It is

generally managed by a third party or by the combination of one or more organizations in the community.

Advantages of the Community Cloud Model

- **Cost Effective: It is cost-effective because the cloud is shared by multiple organizations or communities.**
- **Security: Community cloud provides better security.**
- **Shared resources: It allows you to share resources, infrastructure, etc. with multiple organizations.**
- **Collaboration and data sharing: It is suitable for both collaboration and data sharing.**

Disadvantages of the Community Cloud Model

- **Limited Scalability: Community cloud is relatively less scalable as many organizations share the same resources according to their collaborative interests.**
- **Rigid in customization: As the data and resources are shared among different organizations according to their mutual interests if an organization wants some changes according to their needs they cannot do so because it will have an impact on other organizations.**

Q3) What is Hypervisor? How does it work?
Ans: Hypervisor is a firmware or low-level program that acts as a Virtual Machine Manager. It allows to share the single physical instance of cloud resources between several tenants.

Q4) What are the benefits of Hypervisor?

Ans: Using a hypervisor to host several virtual machines has many advantages:

- **Speed:** The hypervisors allow virtual machines to be built instantly unlike bare-metal servers. This makes provisioning resources for complex workloads much simpler.
- **Efficiency:** Hypervisors that run multiple virtual machines on the resources of a single physical machine often allow for more effective use of a single physical server.
- **Flexibility:** Since the hypervisor distinguishes the OS from the underlying hardware, the program no longer relies on particular hardware devices or drivers, bare-metal hypervisors enable operating systems and their related applications to operate on a variety of hardware types.
- **Portability:** Multiple operating systems can run on the same physical server thanks to hypervisors (host machine). The hypervisor's virtual machines are portable because they are separate from the physical computer.

Q5) Write about the risks in Cloud computing.

Ans: Some most common Security Risks of Cloud Computing are given below-

Data Loss

Data loss is the most common cloud security risks of cloud computing. It is also known as data leakage. Data loss is the process in which data is being deleted, corrupted, and unreadable by a user, software, or application. In a cloud computing environment, data loss occurs when our sensitive data is somebody else's hands, one or more data elements can not be utilized by the data owner, hard disk is not working properly, and software is not updated.

Hacked Interfaces and Insecure APIs

As we all know, cloud computing is completely depends on Internet, so it is compulsory to protect interfaces and APIs that are used by external users. APIs are the easiest way to communicate with most of the cloud services. In cloud computing, few services are available in the public domain. These services can be accessed by third parties, so there may be a chance that these services easily harmed and hacked by hackers.

Data Breach

Data Breach is the process in which the confidential data is viewed, accessed, or stolen by the third party without any authorization, so organization's data is hacked by the hackers.

Vendor lock-in

Vendor lock-in is the of the biggest security risks in cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving one cloud to another.

Increased complexity strains IT staff

Migrating, integrating, and operating the cloud services is complex for the IT staff. IT staff must require the extra capability and skills to manage, integrate, and maintain the data to the cloud.

Spectre & Meltdown

Spectre & Meltdown allows programs to view and steal data which is currently processed on computer. It can run on personal computers, mobile devices, and in the cloud. It can store the password, your personal information such as images, emails, and business documents in the memory of other running programs.

Denial of Service (DoS) attacks

Denial of service (DoS) attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover the lost data, DoS attackers charge a great deal of time and money to handle the data.

Q6) What are the different types of Virtualization?

Ans: **Virtualization** is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".

The machine on which the virtual machine is going to create is known as **Host Machine** and that virtual machine is referred as a **Guest Machine**

Types of Virtualization:

1. Hardware Virtualization.
2. Operating system Virtualization.
3. Server Virtualization.
4. Storage Virtualization.

1) Hardware Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the hardware system* is known as hardware virtualization.

The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.

After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage:

Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

2) Operating System Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is installed on the Host operating system* instead of directly on the hardware system is known as operating system virtualization.

Usage:

Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

3) Server Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the Server system* is known as server virtualization.

Usage:

Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

4) Storage Virtualization:

Storage virtualization is the *process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device*.

Storage virtualization is also implemented by using software applications.

Usage:

Storage virtualization is mainly done for back-up and recovery purposes.

Test 2

1) What is SDN? Why is it important?

Ans: Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

Importance:

- **Better Network Connectivity:** SDN provides very better network connectivity for sales, services, and internal communications. SDN also helps in faster data sharing.
- **Better Deployment of Applications:** Deployment of new applications, services, and many business models can be speed up using Software Defined Networking.
- **Better Security:** Software-defined network provides better visibility throughout the network. Operators can create separate

zones for devices that require different levels of security. SDN networks give more freedom to operators.

- **Better Control with High Speed:** Software-defined networking provides better speed than other networking types by applying an open standard software-based controller.

2) Write about the working principle of SDN.

Ans: SDN, or Software-Defined Networking, is a networking architecture that separates the control plane from the data plane in a network, enabling centralized management and programmability.

A typical SDN architecture consists of three layers.

- Application layer: It contains the typical network applications like intrusion detection, firewall, and load balancing.
- Control layer: It consists of the SDN controller which acts as the brain of the network. It also allows hardware abstraction to the applications written on top of it.
- Infrastructure layer: This consists of physical switches which form the data plane and carries out the actual movement of data packets.

The layers communicate via a set of interfaces called the north-bound APIs(between the application and control layer) and southbound APIs(between the control and infrastructure layer).

The SDN controller is responsible for configuring and managing the network devices in the data plane by communicating with them through a standardized protocol, such as OpenFlow.

The SDN controller maintains a global view of the network topology and traffic flow, and can make intelligent decisions about how packets are forwarded based on policies defined by the network administrator or operator.

When a packet arrives at a network device, such as a switch, the device sends a message to the SDN controller requesting instructions on how to handle the packet. The SDN controller then examines the packet and the network topology to determine the appropriate action and sends instructions back to the switch on how to forward the packet. This process is known as the "control plane signaling" and allows for fine-grained control over network traffic.

Q3) Explain OpenFlow architecture in detail.

Ans: OpenFlow. It is a multivendor standard defined by the Open Networking Foundation (ONF) for implementing SDN in networking equipment. The OpenFlow protocol defines the interface between an OpenFlow Controller and an OpenFlow switch, see Figure 1 below. The OpenFlow protocol allows the OpenFlow Controller to instruct the OpenFlow switch on how to handle incoming data packets.

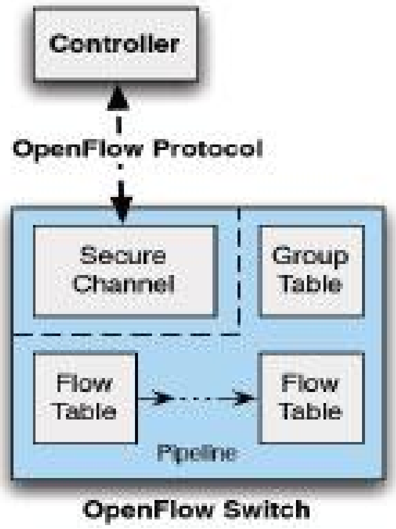


Figure 1 – The OpenFlow Protocol. Source: ONF OpenFlow 1.3.0 Switch Specification

The OpenFlow switch may be programmed to:
(1) identify and categorize packets from an ingress port based on a various packet header fields;
(2) Process the packets in various ways, including modifying the header; and,
(3) Drop or push the packets to a particular egress port or to the OpenFlow Controller.
The OpenFlow instructions transmitted from an OpenFlow Controller to an OpenFlow switch are structured as “flows”. Each individual flow contains packet match fields, flow priority, various counters, packet processing instructions, flow timeouts and a cookie. The flows are organized in tables. An incoming packet may be processed by flows in multiple “pipelined” tables before exiting on an egress port. The OpenFlow protocol standard is evolving quickly with release 1.6 as the current revision at the time of this blog being published.

The OpenFlow Network Architecture consists of three layers:

(1) One or more OpenFlow virtual and/or physical switches;
(2) One or two OpenFlow controller(s); and,
(3) One or more OpenFlow application(s). For an illustration, see figure 2 below.

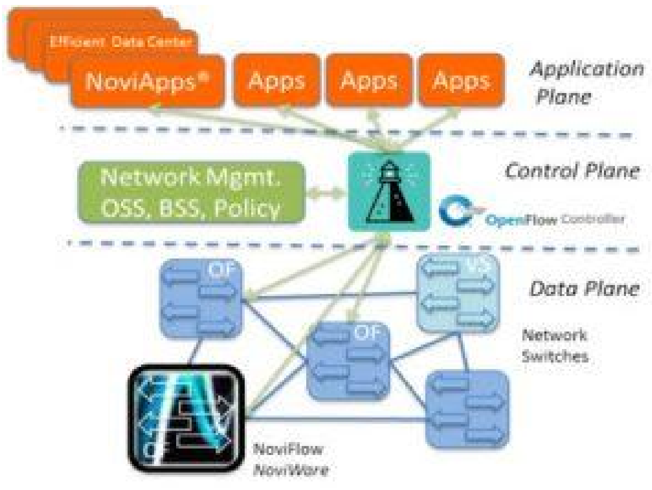


Figure 2 - The OpenFlow Architecture
Source: NoviFlow, Inc.

The OpenFlow controller maintains the OpenFlow protocol communications channels to the OpenFlow switches, maintains a local state graph of the OpenFlow switches and exposes a northbound API to the OpenFlow applications. The northbound API may be viewed as an abstraction of the network and allows the OpenFlow applications to read the state of the network and to instruct the network to perform various tasks.

A real world OpenFlow capable network may consist of only OpenFlow switches or a mixture of OpenFlow switches and traditional switches and routers. The latter network type is called an overlay network. Some OpenFlow applications will require only partial deployment of OpenFlow switches whereas others require a network consisting of only OpenFlow switches.

Q4) Explain the different models of SDN.

Ans: There are different models of SDN.

- Open SDN: Network administrators use a protocol like OpenFlow to control the behavior of virtual and physical switches at the data plane level.
- SDN by APIs: Instead of using an open protocol, application programming interfaces control how data moves through the network on each device.
- SDN Overlay Model: Another type of software-defined networking runs a virtual network on top of an existing hardware infrastructure, creating dynamic tunnels to different on-premise and remote data centers. The virtual network allocates bandwidth over a variety of channels and assigns devices to each channel, leaving the physical network untouched.
- Hybrid SDN: This model combines software-defined networking with traditional networking protocols in one environment to support different functions on a network. Standard networking protocols continue to direct some traffic, while SDN takes on responsibility for other traffic, allowing network administrators to introduce SDN in stages to a legacy environment.

Q5) What are the different resource scheduling algorithms?

Ans:

Test 3

Q1) What are the unique challenges in Cloud Security?

Ans:

1) Misconfiguration: Cloud misconfigurations can expose data and applications to unauthorized access, data leakage, and other security risks. Customers must ensure that their cloud resources are configured securely.
2) Compliance: Organizations need to comply with various regulations and standards, such as HIPAA, GDPR, and PCI DSS. Cloud providers often offer compliance certifications, but customers must ensure that their own use of the cloud complies with these regulations.
3) Multi-tenancy: Cloud providers offer shared resources to multiple customers, which can lead to security risks such as unauthorized access, data leakage, and cross-site scripting attacks.
4) Vendor lock-in: Customers may become dependent on a single cloud provider, making it difficult to switch to a different provider if necessary. This can create security risks if the provider experiences a security breach or outage.
5) Data breaches: Cloud providers are responsible for securing their infrastructure, but customers are responsible for securing their data. Data breaches can occur due to weak authentication and authorization practices, unsecured APIs, and inadequate data encryption.
6) Lack of visibility: Cloud customers may not have complete visibility into the security practices of their cloud provider, which can make it difficult to assess and manage security risks.

Q2) Why is cloud security important?

Ans: Here are the top security benefits of cloud computing:

1. Lower upfront costs

One of the biggest advantages of using cloud computing is that you don't need to pay for dedicated hardware. Not having to invest in dedicated hardware helps you initially save a significant amount of moneyand can also help you upgrade your security. CSPs will handle your security needs proactively once you've hired them. This helps you save on costs and reduce the risks associated with having to hire an internal security team to safeguard dedicated hardware.

2. Reduced ongoing operational and administrative expenses

Cloud security can also lower your ongoing administrative and operational expenses. A CSP will handle all your security needs for you, removing the need to pay for staff to provide manual security updates and configurations. You can also enjoy greater security, as the CSP will have expert staff able to handle any of your security issues for you.

3. Increased reliability and availability

You need a secure way to immediately access your data. Cloud security ensures your data and applications are readily available to authorized users. You'll always have a reliable method to access your cloud applications and information, helping you quickly take action on any potential security issues.

4. Centralized security

Cloud computing gives you a centralized location for data and applications, with many endpoints and devices requiring security. Security for cloud computing centrally manages all your applications, devices, and data to ensure everything is protected. The centralized location allows cloud security companies to more easily perform tasks, such as implementing disaster recovery plans, streamlining network event monitoring, and enhancing web filtering.

5. Greater ease of scaling

Cloud computing allows you to scale with new demands, providing more applications and data storage whenever you need it. Cloud security easily scales with your cloud computing services. When your needs change, the centralized nature of cloud security allows you to easily integrate new applications and other features without sacrificing your data's safety. Cloud security can also scale during high traffic periods, providing more security when you upgrade your cloud solution and scaling down when traffic decreases.

6. Improved DDoS protection

Distributed Denial of Service (DDoS) attacks are some of the biggest threats to cloud computing. These attacks aim a lot of traffic at servers at once to cause harm. Cloud security protects your servers from these attacks by monitoring and dispersing them.

Q3) How does cloud security work?

Ans: Cloud security in cloud computing involves securing the cloud infrastructure, platforms, applications, and data from cyber threats and attacks. Here are the key ways in which cloud security works in cloud computing:

- Identity and access management (IAM): Cloud security in cloud computing starts with identifying who has access to cloud resources and data. IAM solutions are used to manage user identities, control access to resources, and enforce security policies.
- Encryption: Cloud security in cloud computing involves encrypting data both in transit and at rest to protect it from unauthorized access. Encryption keys should be properly managed and rotated regularly to prevent data loss or theft.
- Network security: Cloud security in cloud computing involves securing the network infrastructure used to host cloud resources. This includes implementing firewalls, intrusion detection systems, and other security measures to protect against cyber threats and attacks.
- Application security: Cloud security in cloud computing involves securing the applications that are hosted in the cloud. This includes implementing secure coding practices, testing for vulnerabilities, and deploying security patches to ensure that applications remain secure.
- Data protection: Cloud security in cloud computing involves protecting data from loss or theft. This includes implementing backup and recovery solutions, as well as disaster recovery plans, to ensure that data can be recovered in the event of a data breach or disaster.
- Compliance: Cloud security in cloud computing involves complying with a range of regulations and standards, such as data privacy laws and industry-specific regulations. Cloud providers need to implement processes and procedures to ensure that they are meeting these requirements.

Q4) Write a note on SAP systems.

Ans: SAP, or Systems Applications and Products, is a widely-used enterprise resource planning (ERP) software SAP creates a centralized system for businesses that enables every department to access and share common data to create a better work environment for every employee in the company. SAP is the most-used ERP software on the market and contains hundreds of fully integrated modules that cover nearly every aspect of business management.

SAP collects and processes data from all functions in a business on one platform. SAP is essential for many businesses because it allows every department to communicate with each other easily. The success of any organization relies on effective communication and data exchange between its functions, and SAP is an effective way to support those efforts.

Q5) How can you deploy an SAP system using cloud technology? Explain.

EXTRA QUESTIONS

Q) What is cloud security ?

Ans: Cloud security refers to the technologies and protocols that protect cloud computing environments, applications running in the cloud, and data held in the cloud.

The full scope of cloud security is designed to protect the following, regardless of your responsibilities:

Physical networks
Data storage
Data servers
Computer virtualization frameworks
Operating systems (OS)
Middleware
Runtime environments
Data
Applications
End-user hardware

Q) How does Cloud Security work?

Ans: Cloud security involves various aspects to protect data and systems in the cloud.

Data security focuses on safeguarding sensitive data. Encryption is a powerful tool that scrambles data, making it unreadable without an encryption key. Transit protections, like virtual private networks (VPNs), secure data during transmission.

Identity and access management (IAM) controls user access to resources. It includes authentication (verifying user identity) and authorization (granting appropriate privileges). Password management and multi-factor authentication are examples of IAM measures.

Governance involves policies and practices for threat prevention, detection, and response. Organizations prioritize threat intelligence to identify and address potential risks. User behavior policies and training also contribute to a secure environment.

Data retention (DR) and business continuity (BC) planning ensure data backup and recovery. Redundancy measures, such as regular backups, help protect against data loss. Business continuity plans outline actions to maintain operations during disruptions.

Legal compliance focuses on adhering to privacy regulations. Organizations must protect user information and follow legislative requirements. Data masking techniques, such as encryption, can obscure sensitive data.

Q) What makes Cloud security different ?

Ans: Cloud security differs from traditional IT security in several ways:

1. Data storage: Cloud models rely on offsite data storage, reducing the need for costly in-house infrastructure but also reducing control over security measures.

2. Scaling speed: Cloud systems can quickly scale to meet organizational needs, but this rapid expansion can outpace security measures if not properly managed.

3. End-user system interfacing: Cloud systems interface with various other systems and services, requiring attention to access permissions and vulnerabilities at the device, software, and network levels.

4. Proximity to networked data and systems: Cloud providers are connected to a vast network of users, increasing the potential for security threats and placing additional responsibilities on the providers to protect their infrastructure and data.

5. Dynamic nature: Cloud environments are dynamic and constantly changing, which can make it challenging to apply security controls consistently.

Q) Explain any two task scheduling algorithms of Cloud computing.

Ans: Immediate scheduling and batch scheduling algorithms in task scheduling in cloud computing:

Immediate Scheduling:

Immediate scheduling, also known as online scheduling, focuses on scheduling tasks as soon as they arrive or are submitted to the system.
It aims to quickly allocate available resources to incoming tasks without delay.
This type of scheduling algorithm is suitable for scenarios where tasks have short execution times or strict latency requirements.
Immediate scheduling algorithms prioritize tasks based on certain criteria such as deadlines, priority levels, or resource availability.
These algorithms make quick decisions on task placement and resource allocation, often based on real-time information, to achieve efficient utilization of cloud resources.
Examples of immediate scheduling algorithms include First-Come, First-Served (FCFS), Shortest Job Next (SJN), and Round Robin (RR).
Batch Scheduling:

Batch scheduling focuses on grouping tasks into batches or jobs and scheduling them together.
Instead of immediately allocating resources to individual tasks, batch scheduling waits for a sufficient number of tasks to arrive before scheduling them.
It aims to achieve better overall resource utilization and minimize the scheduling overhead by considering a larger set of tasks at once.

Batch scheduling algorithms often optimize for factors such as energy efficiency, load balancing, or maximizing throughput.
These algorithms consider the characteristics of tasks, resource availability, and system constraints to make scheduling decisions.
Examples of batch scheduling algorithms include backfilling, gang scheduling, and partitioning-based approaches like space-sharing and time-sharing.