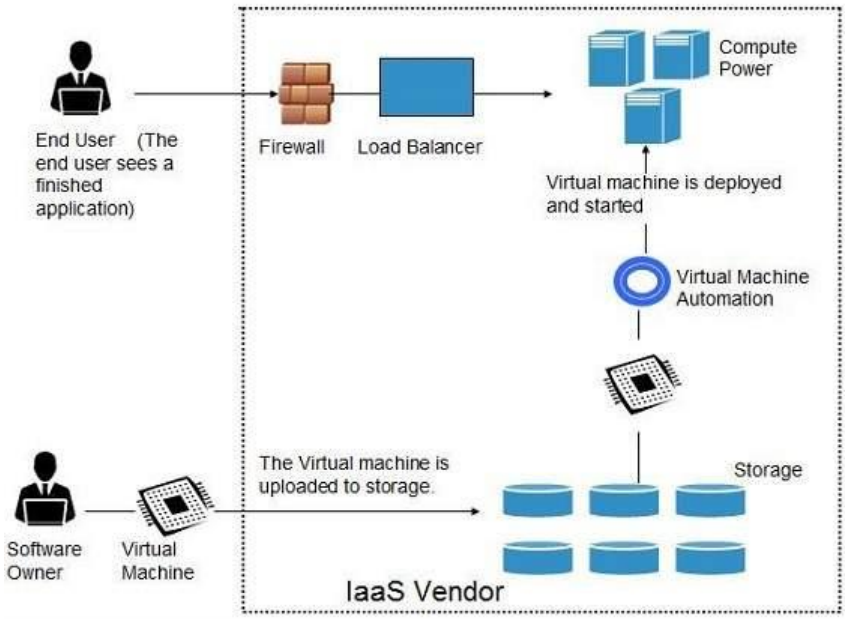
Cloud Computing Platforms and Technologies

Cloud Computing Infrastructure as a Service

Infrastructure-as-a-Service provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc. Apart from these resources, the IaaS also offers:

- Virtual machine disk storage
- Virtual local area network (VLANs)
- Load balancers
- IP addresses
- Software bundles

All of the above resources are made available to end user via **server virtualization.** Moreover, these resources are accessed by the customers as if they own them.



Benefits

IaaS allows the cloud provider to freely locate the infrastructure over the Internet in a cost-effective manner. Some of the key benefits of IaaS are listed below:

- Full control of the computing resources through administrative access to VMs.
- Flexible and efficient renting of computer hardware.
- Portability, interoperability with legacy applications.

Full control over computing resources through administrative access to VMs

IaaS allows the customer to access computing resources through administrative access to virtual machines in the following manner:

- Customer issues administrative command to cloud provider to run the virtual machine or to save data on cloud server.
- Customer issues administrative command to virtual machines they owned to start web server or to install new applications.

Flexible and efficient renting of computer hardware

IaaS resources such as virtual machines, storage devices, bandwidth, IP addresses, monitoring services, firewalls, etc. are made available to the customers on rent. The payment is based upon the amount of time the

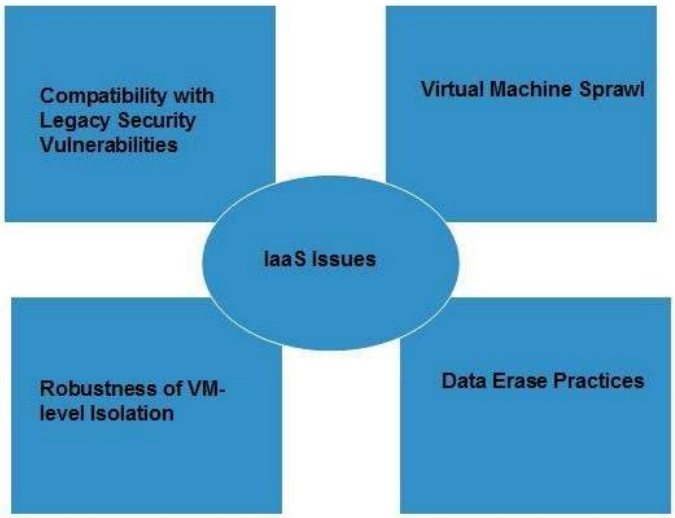
customer retains a resource. Also with administrative access to virtual machines, the customer can run any software, even a custom operating system.

Portability, interoperability with legacy applications

It is possible to maintain legacy between applications and workloads between IaaS clouds. For example, network applications such as web server or e-mail server that normally runs on customer-owned server hardware can also run from VMs in IaaS cloud.

Issues

IaaS shares issues with PaaS and SaaS, such as Network dependence and browser based risks. It also has some specific issues, which are mentioned in the following diagram:



Compatibility with legacy security vulnerabilities

Because IaaS offers the customer to run legacy software in provider's infrastructure, it exposes customers to all of the security vulnerabilities of such legacy software.

Virtual Machine sprawl

The VM can become out-of-date with respect to security updates because IaaS allows the customer to operate the virtual machines in running, suspended and off state. However, the provider can automatically update such VMs, but this mechanism is hard and complex.

Robustness of VM-level isolation

IaaS offers an isolated environment to individual customers through hypervisor. Hypervisor is a software layer that includes hardware support for virtualization to split a physical computer into multiple virtual machines.

Data erase practices

The customer uses virtual machines that in turn use the common disk resources provided by the cloud provider. When the customer releases the resource, the cloud provider must ensure that next customer to rent the resource does not observe data residue from previous customer.

Characteristics

Here are the characteristics of IaaS service model

- Virtual machines with pre-installed software.
- Virtual machines with pre-installed operating systems such as Windows, Linux, and Solaris.

- On-demand availability of resources.
- Allows to store copies of particular data at different locations.
- The computing resources can be easily scaled up and down.

Best-of-Breed Technology

A best of breed system is the best system in its referenced niche or category. Although it performs specialized functions better than an integrated system, this type of system is limited by its specialty area.

To fulfill varying requirements, organizations often use best of breed systems from separate vendors. However, maintaining multiple systems provides little cross connectivity, which creates maintenance and integration challenges.

Best of breed systems are best applied to one or a few functions, facilitating system maintenance. However, as an organization expands and requirements multiply, best of breed systems may not be able to handle new requirements, forcing the addition of another system. In this type of scenario, the best course of action is to employ an integrated system that can handle most requirements, allowing best of breed systems to handle items requiring focused performance and specialization.

Best of breed system advantages are as follows:

- Updates and building blocks may be rolled out without affecting other systems.
- Because the function of a system is geared to a specific purpose, it is easier to update and able to quickly respond to market changes.
- Specialized functions include more options and solutions and provide specific knowledge regarding specific functions.

Disadvantages are as follows:

- Vendors of best of breed systems are often small organizations that do not understand the requirements of larger organizations.
- Integration with other systems is a highly complex process.
- Sharing data across different systems may be difficult.

Solutions for Best-of-Breed Building Cloud Infrastructure

• Built by integrating multi-vendor infrastructure components

• Enables repurposing the existing infrastructure components

• Requires spending a significant amount of IT staff time on:

  – Evaluating individual and disparate hardware components

  – Installing and integrating infrastructure components

  – Testing hardware, middleware, and software

  – Checking compatibility of all the components

• Enables organizations to choose and switch vendors easily

In an integrated best-of-breed cloud infrastructure components solution, organizations have the flexibility to use and integrate the infrastructure components from different vendors. This solution allows organizations to design their cloud infrastructure by repurposing their existing infrastructure components (in a brownfield deployment option), providing a cost advantage for this solution. This solution enables organizations to select a vendor of their choice for infrastructure components. This solution also enables an organization to easily switch a vendor if the vendor is unable to provide the committed support and not meet the SLAs.

When this method is used to build a cloud infrastructure, an organization may have to spend a significant amount of IT staff time evaluating individual, disparate hardware components, installing hardware, and integrating compute, storage, and network components. The IT staff may also have to spend effort integrating and testing hardware, middleware, and software. They also need to check the compatibility of all the components to ensure that the combined components interoperate and function as expected. This may delay the deployment of cloud services. Further, scaling of such an infrastructure takes longer because each component that is scaled requires integration with the existing infrastructure and testing for compatibility. Finally, this solution requires acquiring cloud infrastructure management tools and deploying them on the infrastructure.

Cloud Ready Converged Infrastructure

Converged infrastructure is a way of structuring an information technology (IT) system which groups multiple components into a single optimized computing package. Components of a converged infrastructure may include servers, data storage devices, networking equipment and software for IT infrastructure management, automation and orchestration.

IT organizations use converged infrastructure to centralize the management of IT resources, to consolidate systems, to increase resource-utilization rates, and to lower costs. Converged infrastructures foster these objectives by implementing pools of computers, storage and networking resources that can be shared by multiple applications and managed in a collective manner using policy-driven processes.[1]

IT vendors and IT industry analysts use various terms to describe the concept of a converged infrastructure. These include "converged system", "unified computing", "fabric-based computing", and "dynamic infrastructure".

Benefits

Converged infrastructure provides both technical and business efficiencies, according to industry researchers and observers.[3] These gains stem in part from the pre-integration of technology components, the pooling of IT resources and the automation of IT processes. Converged infrastructure further contributes to efficient data centers by enhancing the ability of cloud computing systems to handle enormous data sets, using only a single integrated IT management system [4]

Writing in *CIO magazine*, Forrester Research analyst Robert Whiteley noted that converged infrastructures, combining server, storage, and networks into a single framework, help to transform the economics [of] running the datacenter thus accelerating the transition to IP storage to help build infrastructures that are "cloud-ready".[5] The combination of storage and compute into a single entity is known as converged storage.[6]

Decreased complexity, through the use of pre-integrated hardware with virtualization and automation management tools, is another important value proposition for converged infrastructure as noted in an IDC study.[7]

In April 2012, the open source analyst firm Wikibon released the first market forecast for converged infrastructure,[8] with a projected $402 billion total available market (TAM) by 2017 of which, nearly 2/3 of

the infrastructure that supports enterprise applications will be packaged in some type of converged solution by 2017.

InformationWeek[9] highlighted the promise of two long-term advantages of a unified data center infrastructure:

1. Lower costs as the result of both:

- lower capital expenses resulting from higher utilization, less cabling, and fewer network connections
- lower operating costs resulting from reduced labor via automated data center management and a consolidating storage and network management infrastructure teams

2. Increased IT agility by:

- virtualizing IP and Fibre Channel storage networking
- allowing for single console management.

Data centers around the world are reaching limits in power, cooling and space.[10] At the same time, capital constraints are requiring organizations to rethink data center strategy. Converged infrastructure offers a solution to these challenges.

Anatomy of Cloud Computing

Provisioning and Configuration Module:

It is the lowest level of cloud and typically resides on bare hardware (as a firmware) or on the top of the hypervisor layer. Its function is to abstract the underlying hardware and provide a standard mechanism to spawn instance of virtual machine on demand. It also handles the post-configuration of the operating systems and applications residing on the VM

Monitoring and Optimization:

This layer handles the monitoring of all services, storage, networking and applications components in cloud. Based on the statistics, it could perform routine functions that optimize the behavior of the infrastructure components and provide relevant data to the cloud administrator to further optimize the configuration for maximum utilization and performance,

Metering and Chargeback:

This layer provides functions to measure the usage of resources in cloud. The metering module collects all the utilization data per domain per use. This module gives the cloud administrator enough data to measure ongoing utilization of resources and to create invoices based on the usage on a periodic basis.

Orchestration:

Orchestration is a central to cloud operations. Orchestration converts requests from the service management layer and the monitoring, chargeback modules to appropriate action item which are then submitted to provisioning and configuration module for final closure. Orchestration updates the CMDB in the process.

Configuration Management Database (CMDB):

It is a central configuration repository wherein all the meta data and configuration of different modules, resources are kept and updated in the real-time basis. The repository can then be accessed using standards protocols like SOAP by third-party software and integration components. All updates in CMDB happen in real time as requests get processed in cloud.

Cloud Life cycle Management Layer (CLM):

This layer handles the coordination of all other layers in cloud. All requests internal and external are

addressed to the CLM layer first. CLM may internally route requests and actions to other layers for further processing.

Service Catalog:

It is central to the definition of cloud, SC defines what kind of services the cloud is capable of providing and at what cost to the end user. SC is the first thing that is drafted before a cloud is architecture. The service management layer consults SC before it processes any request for a new resource.

Virtual Infrastructure

A virtual infrastructure is a software-based IT infrastructure being hosted on another physical infrastructure and meant to be distributed as a service as in cloud computing's infrastructure as a service (IaaS) delivery model. It provides organizations, particularly smaller ones that cannot afford to build their own physical infrastructure, access to enterprise-grade technology such as servers and applications. The distribution is often done via the cloud, meaning over large networks such as the internet.

The main purpose of a virtual infrastructure is to bring enterprise-level technology to organizations that cannot afford the large capital required to pay for the hardware, software licenses, setup and continual maintenance of an actual data center infrastructure. The technology involves virtualization, which is the utilization of physical server resources to host logical or virtual servers and networking hardware in order to optimize resources and drive costs down by hosting multiple virtual servers in a single host server.

The idea is that no single server is actually taxed enough to the point that its resource limits are reached so it would be more prudent to make use of these resources by running multiple logical servers that, together, can make use of the actual capacity of the host. This lean approach allows for sharing and distributing resources, which, in turn, promotes flexibility, scalability and lower total cost of ownership.

Benefits Of A Virtual Infrastructure:

- **Scalable** – Allows provisioning as many or as few logical servers as required, and users only pay for what they use.
- **Flexible** – Allows for multiple server and networking configurations as compared to a hardwired physical infrastructure, which requires more capital and effort to change.
- **Secure** – Allows more security to be layered on top of whatever security is already present in the virtual infrastructure because all traffic to the virtual infrastructure goes through the actual physical infrastructure.
- **Load balancing** – Allows software-based servers to share workloads easily and distribute them properly so that no single logical server is taxed more than the others.
- **Backup and recovery** – Promotes easier backups because everything can be saved somewhere, allowing for quick recovery in other hosts if a few hosts are down. This is almost impossible with physical servers, which have to be revived before services can resume.

Scheduling algorithms

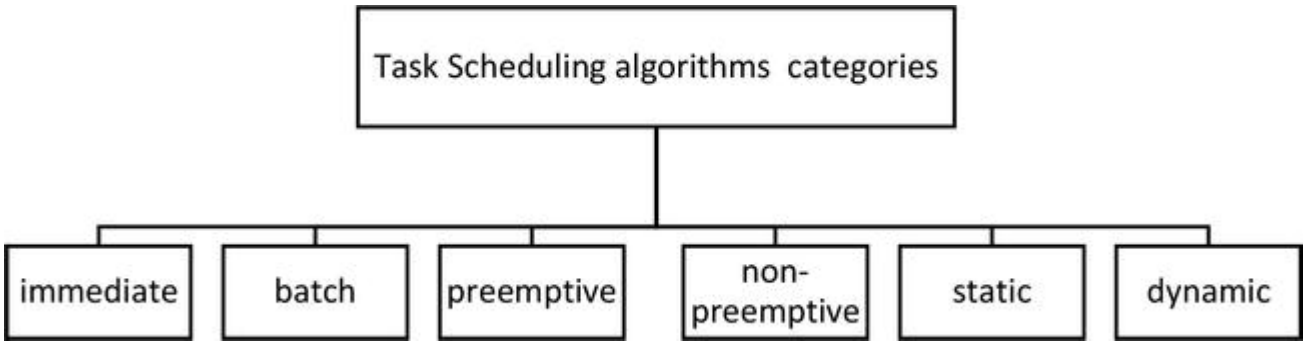
Tasks scheduling algorithms are defined as a set of rules and policies used to assign tasks to the suitable resources (CPU, memory, and bandwidth) to get the highest level possible of performance and resources utilization.

Task scheduling algorithms advantages

- Manage cloud computing performance and QoS.
- Manage the memory and CPU.
- The good scheduling algorithms maximizing resources utilization while minimizing the total task execution time.
- Improving fairness for all tasks.
- Increasing the number of successfully completed tasks.
- Scheduling tasks on a real-time system.
- Achieving a high system throughput.
- Improving load balance.

Tasks scheduling algorithms classifications

Tasks scheduling algorithms classified as in Figure



Tasks scheduling algorithms can be classified as follows

- **Immediate scheduling**: when new tasks arrive, they are scheduled to VMs directly.
- **Batch scheduling**: tasks are grouped into a batch before being sent; this type is also called mapping events.
- **Static scheduling**: is considered very simple compared to dynamic scheduling; it is based on prior information of the global state of the system. It does not take into account the current state of VMs and then divides all traffic equivalently among all VMs in a similar manner such as round robin (RR) and random scheduling algorithms.

- **Dynamic scheduling**: takes into account the current state of VMs and does not require prior information of the global state of the system and distribute the tasks according to the capacity of all available VMs [4, 5, 6].
- **Preemptive scheduling**: each task is interrupted during execution and can be moved to another resource to complete execution [6].
- **Non-preemptive scheduling**: VMs are not re-allocated to new tasks until finishing execution of the scheduled task [6]

Static tasks scheduling algorithms in cloud computing environment

1) FCFS

FCFS: the order of tasks in task list is based on their arriving time then assigned to VMs [3].

Advantages

- Most popular and simplest scheduling algorithm.
- Fairer than other simple scheduling algorithms.
- Depend on FIFO rule in scheduling task.
- Less complexity than other scheduling algorithms.

Disadvantages

- Tasks have high waiting time.
- Not give any priority to tasks. That means when we have large tasks in the begin tasks list, all tasks must wait a long time until the large tasks to finish.
- Resources are not consumed in an optimal manner.
- In order to measure the performance achieved by this method, we will be testing them and then measuring its impact on (fairness, ET, TWT, and TFT).

2) SJF

Tasks are sorted based on their priority. Priority is given to tasks based on tasks lengths and begins from (smallest task ≡ highest priority).

Advantages

- Wait time is lower than FCFS.
- SJF has minimum average waiting time among all tasks scheduling algorithms.

Disadvantages

- Unfairness to some tasks when tasks are assigned to VM, due to the long tasks tending to be left waiting in the task list while small tasks are assigned to VM.
- Taking long execution time and TFT

Service level agreements in Cloud computing

A Service Level Agreement (SLA) is the bond for performance negotiated between the cloud services provider and the client. Earlier, in cloud computing all Service Level Agreements were negotiated between a client and the service consumer. Nowadays, with the initiation of large utility-like cloud computing providers, most Service Level Agreements are standardized until a client becomes a large consumer of cloud services. Service level agreements are also defined at different levels which are mentioned below:

- Customer-based SLA
- Service-based SLA
- Multilevel SLA

Few Service Level Agreements are enforceable as contracts, but mostly are agreements or contracts which are more along the lines of an Operating Level Agreement (OLA) and may not have the restriction of law. It is

fine to have an attorney review the documents before making a major agreement to the cloud service provider. Service Level Agreements usually specify some parameters which are mentioned below:

1. Availability of the Service (uptime)
2. Latency or the response time
3. Service components reliability
4. Each party accountability
5. Warranties

In any case, if a cloud service provider fails to meet the stated targets of minimums then the provider has to pay the penalty to the cloud service consumer as per the agreement. So, Service Level Agreements are like insurance policies in which the corporation has to pay as per the agreements if any casualty occurs. Microsoft publishes the Service Level Agreements linked with the Windows Azure Platform components, which is demonstrative of industry practice for cloud service vendors. Each individual component has its own Service Level Agreements. Below are two major Service Level Agreements (SLA) described:

1. **Windows Azure SLA –**
   Window Azure has different SLA's for compute and storage. For compute, there is a guarantee that when a client deploys two or more role instances in separate fault and upgrade domains, client's internet facing roles will have external connectivity minimum 99.95% of the time. Moreover, all of the role instances of the client are monitored and there is guarantee of detection 99.9% of the time when a role instance's process is not runs and initiates properly.
2. **SQL Azure SLA –**
   SQL Azure clients will have connectivity between the database and internet gateway of SQL Azure. SQL Azure will handle a "Monthly Availability" of 99.9% within a month. Monthly Availability Proportion for a particular tenant database is the ratio of the time the database was available to customers to the total time in a month. Time is measured in some intervals of minutes in a 30-day monthly cycle. Availability is always remunerated for a complete month. A portion of time is marked as unavailable if the customer's attempts to connect to a database are denied by the SQL Azure gateway.

Service Level Agreements are based on the usage model. Frequently, cloud providers charge their pay-as-per-use resources at a premium and deploy standards Service Level Agreements only for that purpose. Clients can also subscribe at different levels that guarantees access to a particular amount of purchased resources. The Service Level Agreements (SLAs) attached to a subscription many times offer various terms and conditions. If client requires access to a particular level of resources, then the client need to subscribe to a service. A usage model may not deliver that level of access under peak load condition.

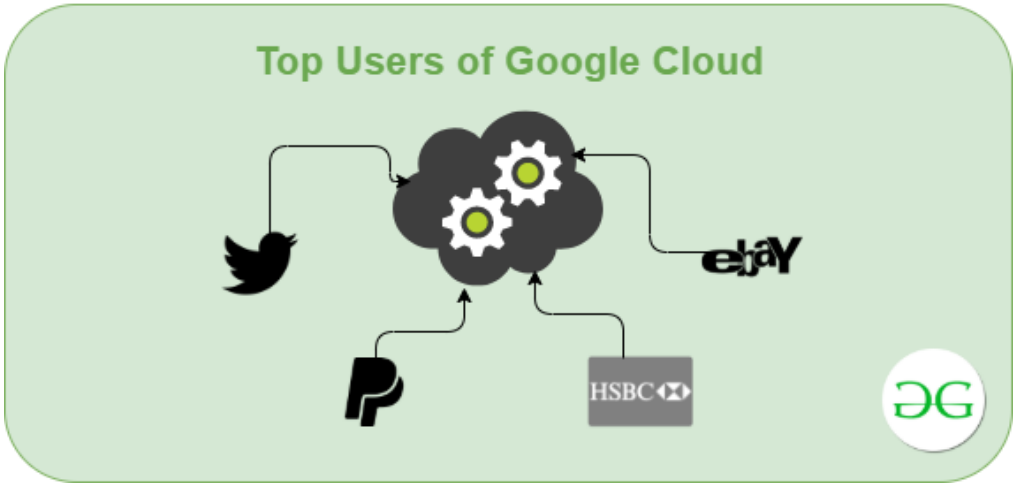
Google Web Services

Google has made our lives more comfortable than ever. Whenever we find ourselves in some problem before we call our mothers we ask Google. One of the significant things Google has excelled upon is keeping our data safe and protected. Back in the days, we used to lose all our cherished data due to one hardware crash. But not today. With Google Cloud, everything can be protected.

Google Cloud Safety: With the increasing number of cybercrimes, one can wonder about his data privacy. Google uses multiple security checks, and Thus, you can relax and store your data on Cloud.

Google Cloud for Trading: With the ever-increasing number of web-enabled devices in this world, the ease of access to the relevant data through the internet is one of the biggest challenges tagging along that the computer scientists are trying to work out. And with Google launching, it's Transfer service, this issue in itself becomes insanely huge to discuss.

Modern Businesses use Cloud computing services to store and manipulate their data sets which can vary from a few GigaBytes to thousands of PetaBytes. Cloud Computing refers to Internet-based computing, providing services like servers, storage, and data handling. Large companies set up their databases using these cloud services because it helps them create and manage a virtual office that contains every bit of their information and files but not physically or on their private computers but on the Cloud, i.e. the Internet itself. This means that the data uploaded can be accessed from anywhere around the globe by the authorized personnel with just some swipes and touches.



Data handling: Handling the amount of data is not an easy task, and that's where the Tech Giants come in. Companies like Google, Amazon, and Microsoft are doing their job exceptionally well by providing the best Cloud Computing services as Business Solutions to the companies who want to adopt this technology. There are hundreds of companies that offer this platform, but multiple surveys say that choosing Google Cloud Computing services might be one of the best decisions one can take for their company.

Google has made it remarkably simple for companies to manage their business data through Cloud and at the same time, transfer their data from other cloud services to Google. The former Tech Giant recently announced its transfer services helping big companies move their on-premise data to google cloud. Google claims that the services provided by its Cloud are like the ones used by their servers.

Transfer of data is effortless: Companies will have to select the files they want to transfer and Google will take care of the rest. This deviant method uses the power of Google's Super Computers. We are talking of transfer of data from other cloud services to Google cloud because they come with a number of services in a bulk. Let's discuss them below:

1. **Compute**: Companies can use Google's cloud services in a very scalable way to match their specific and general needs. GCS provides virtual machines and options to deploy our code in different ways.

2. **Storage and Databases**: Even just for storage, multiple options are available such as Cloud SQL, Cloud Bigtable, Google Cloud Datastore, etc.

3. **Big Data:** Similarly multiple services are provided for big data analysis and manipulation like Google Cloud Dataproc, Google Cloud Datalab, Google Cloud Pub/Sub, and Google BigQuery.

4. **Networking:** Google provides multiple networking options that work hand to hand with Google Storage. Google Cloud Load Balancing, Content Delivery Network, and Google Cloud Interconnect are some examples.

5. **Identity and Security:** Cloud Resource Manager, Cloud IAM, and Cloud Security Scanner are some of the services provided by GCP regarding identity and security.

6. **Management Tools:** This tool helps you to manage sensitive data. Also provides a fast and scalable classification for sensitive data elements like credit card numbers, passport numbers, and many more.

7. Cloud AI: A well-managed service that will permit you to work on Machine Learning models based on mainstream frameworks. A Machine Learning product that enables developers to provide their data sets and obtain access to quality trained models by Google's transfer learning and Neural Architecture Search.

8. IOT: This service is a fully managed service which will allow you to easily connect, manage, and absorb data from devices that are connected to the Internet.

The number of services provided by Google is enormous,

Data moved to Google Cloud: Moving data to Cloud comes with several benefits, and some of them are:

- Google's Private data transfer cables and amazingly spread network- Google recently announced that it has invested in the FASTER cable system giving speeds up to 10Tbps between the US and Japan. These cables will be used for Google Cloud and Google App customers.
- Live Migration of Virtual Machines- No other competitor in the field provides this service. There is no noticeable performance degradation while migrating VMs between host machines.
- Best Security- Google comes with the name of security and a promise to protect the user data. Choosing google cloud services means choosing a security model that is laid upon in 15 years.
- Trustworthy back-up- Google claims durability of 99.9% for its storage unit and is based upon four different types: Nearline storage, Coldline Storage, Regional Storage, and Multi-regional Storage. This means no loss of data what so ever.
- Promise to Expand, Google is continuously improving its services and is promising to come up with more. It is new cloud regions that will be strategically placed all over the globe will ensure improved performance and faster services.

With all that's said, we can firmly say that Google has made it very easy to move data to it's Cloud. It is providing a never-ending supply of services for its customers all around the world with the most sophisticated technologies and state of the art supercomputers

Introduction to Amazon Web Services

Amazon Web Services (AWS), a subsidiary of Amazon.com, has invested billions of dollars in IT resources distributed across the globe. These resources are shared among all the AWS account holders across the globe. These account themselves are entirely isolated from each other. AWS provides on-demand IT resources to its account holders on a pay-as-you-go pricing model with no upfront cost. Amazon Web services offers flexibility because you can only pay for services you use or you need. Enterprises use AWS to reduce capital expenditure of building their own private IT infrastructure (which can be expensive depending upon the enterprise's size and nature). AWS has its own Physical fiber network that connects with Availability zones, regions and Edge locations. All the maintenance cost is also bared by the AWS that saves a fortune for the enterprises.

Security of cloud is the responsibility of AWS but Security in the cloud is Customer's Responsibility. The Performance efficiency in the cloud has four main areas:-

- Selection
- Review
- Monitoring
- Tradeoff

AWS Global Infrastructure

The AWS global infrastructure is massive and is divided into geographical regions. The geographical regions are then divided into separate availability zones. While selecting the geographical regions for AWS, three factors come into play

- Optimizing Latency
- Reducing cost
- Government regulations (Some services are not available for some regions)

Each region is divided into at least two availability zones that are physically isolated from each other, which provides business continuity for the infrastructure as in a distributed system. If one zone fails to function, the infrastructure in other availability zones remains operational. The largest region North Virginia (US-East), has six availability zones. These availability zones are connected by high-speed fiber-optic networking.

There are over 100 edge locations distributed all over the globe that are used for the CloudFront (content delivery network). Cloudfront can cache frequently used content such as images and videos(live streaming videos also) at edge locations and distribute it to edge locations across the globe for high-speed delivery and low latency for end-users. It also protects from DDOS attacks.

AWS Management Console

The AWS management console is a web-based interface to access AWS. It requires an AWS account and also has a smartphone application for the same purpose. So When you sign in for first time, you see the console home page where you see all the services provided by AWS. Cost monitoring is also done through the console.

AWS resources can also be accessed through various Software Development Kits (SDKs), which allows the developers to create applications as AWS as its backend. There are SDKs for all the major languages(e.g., JavaScript, Python, Node.js, .Net, PHP, Ruby, Go, C++). There are mobile SDKs for Android, iOS, React Native, Unity, and Xamarin. AWS can also be accessed by making HTTP calls using the AWS-API. AWS also provides a Command Line Interface (CLI) for remotely accessing the AWS and can implement scripts to automate many processes. This Console is also available as an app for Android and iOS. For mobile apps, you can simply download AWS console app.

AWS Cloud Computing Models

There are three cloud computing models available on AWS.

1. **Infrastructure as a Service (IaaS)**: It is the basic building block of cloud IT. It generally provides access to data storage space, networking features, and computer hardware(virtual or dedicated hardware). It is highly flexible and gives management controls over the IT resources to the developer. For example, VPC, EC2, EBS.
2. **Platform as a Service (PaaS):** This is a type of service where AWS manages the underlying infrastructure (usually operating system and hardware). This helps the developer to be more efficient as they do not have to worry about undifferentiated heavy lifting required for running the applications such as capacity planning, software maintenance, resource procurement, patching, etc., and focus more on deployment and management of the applications. For example, RDS, EMR, ElasticSearch.
3. **Software as a Service(SaaS):** It is a complete product that usually runs on a browser. It primarily refers to end-user applications. It is run and managed by the service provider. The end-user only has to worry about the application of the software suitable to its needs. For example, Saleforce.com, Web-based email, Office 365 .

Microsoft Cloud services

What is Azure?

Azure is Microsoft's cloud platform, just like Google has it's Google Cloud and Amazon has it's Amazon Web Service or AWS.000. Generally, it is a platform through which we can use Microsoft's resource. For example, to set up a huge server, we will require huge investment, effort, physical space and so on. In such situations, Microsoft Azure comes to our rescue. It will provide us with virtual machines, fast processing of data, analytical and monitoring tools and so on to make our work simpler. The pricing of Azure is also simpler and cost-effective. Popularly termed as "Pay As You Go", which means how much you use, pay only for that.

Azure History

Microsoft unveiled Windows Azure in early October 2008 but it went to live after February 2010. Later in 2014, Microsoft changed its name from Windows Azure to Microsoft Azure. Azure provided a service platform for .NET services, SQL Services, and many Live Services. Many people were still very skeptical about "the cloud". As an industry, we were entering a brave new world with many possibilities. Microsoft Azure is getting bigger and better in coming days. More tools and more functionalities are getting added. It has two releases as of now. It's famous version Microsoft Azure v1 and later Microsoft Azure v2. Microsoft Azure v1 was more like JSON script driven then the new version v2, which has interactive UI for simplification and easy learning. Microsoft Azure v2 is still in the preview version.

How Azure can help in business?

Azure can help in our business in the following ways-

- **Capital less**: We don't have to worry about the capital as Azure cuts out the high cost of hardware. You simply pay as you go and enjoy a subscription-based model that's kind to your cash flow. Also, to set up an Azure account is very easy. You simply register in Azure Portal and select your required subscription and get going.
- **Less Operational Cost**: Azure has low operational cost because it runs on its own servers whose only job is to make the cloud functional and bug-free, it's usually a whole lot more reliable than your own, on-location server.
- **Cost Effective**: If we set up a server on our own, we need to hire a tech support team to monitor them and make sure things are working fine. Also, there might be a situation where the tech support team is taking too much time to solve the issue incurred in the server. So, in this regard is way too pocket-friendly.
- **Easy Back Up and Recovery** options: Azure keep backups of all your valuable data. In disaster situations, you can recover all your data in a single click without your business getting affected. Cloud-based backup and recovery solutions save time, avoid large up-front investment and roll up third-party expertise as part of the deal.
- **Easy to implement**: It is very easy to implement your business models in Azure. With a couple of on-click activities, you are good to go. Even there are several tutorials to make you learn and deploy faster.
- **Better Security**: Azure provides more security than local servers. Be carefree about your critical data and business applications. As it stays safe in the Azure Cloud. Even, in natural disasters, where the resources can be harmed, Azure is a rescue. The cloud is always on.
- **Work from anywhere**: Azure gives you the freedom to work from anywhere and everywhere. It just requires a network connection and credentials. And with most serious Azure cloud services offering mobile apps, you're not restricted to which device you've got to hand.
- **Increased collaboration:** With Azure, teams can access, edit and share documents anytime, from anywhere. They can work and achieve future goals hand in hand. Another advantage of the Azure is that it preserves records of activity and data. Timestamps are one example of the Azure's record

keeping. Timestamps improve team collaboration by establishing transparency and increasing accountability.

Microsoft Azure Services

Some following are the services of Microsoft Azure offers:

1. **Compute**: Includes Virtual Machines, Virtual Machine Scale Sets, Functions for serverless computing, Batch for containerized batch workloads, Service Fabric for microservices and container orchestration, and Cloud Services for building cloud-based apps and APIs.
2. **Networking**: With Azure you can use variety of networking tools, like the Virtual Network, which can connect to on-premise data centers; Load Balancer; Application Gateway; VPN Gateway; Azure DNS for domain hosting, Content Delivery Network, Traffic Manager, ExpressRoute dedicated private network fiber connections; and Network Watcher monitoring and diagnostics
3. **Storage**: Includes Blob, Queue, File and Disk Storage, as well as a Data Lake Store, Backup and Site Recovery, among others.
4. **Web + Mobile**: Creating Web + Mobile applications is very easy as it includes several services for building and deploying applications.
5. **Containers**: Azure has a property which includes Container Service, which supports Kubernetes, DC/OS or Docker Swarm, and Container Registry, as well as tools for microservices.
6. **Databases**: Azure has also includes several SQL-based databases and related tools.
7. Data + Analytics: Azure has some big data tools like HDInsight for Hadoop Spark, R Server, HBase and Storm clusters
8. **AI + Cognitive** Services: With Azure developing applications with artificial intelligence capabilities, like the Computer Vision API, Face API, Bing Web Search, Video Indexer, Language Understanding Intelligent.
9. **Internet of Things:** Includes IoT Hub and IoT Edge services that can be combined with a variety of machine learning, analytics, and communications services.
10. **Security + Identity**: Includes Security Center, Azure Active Directory, Key Vault and Multi-Factor Authentication Services.
11. **Developer Tools:** Includes cloud development services like Visual Studio Team Services, Azure DevTest Labs, HockeyApp mobile app deployment and monitoring, Xamarin cross-platform mobile development and more.

Practical Issues:-

1) Interoperability:

It is defined as the capacity of at least two systems or applications to trade with data and utilize it. On the other hand, cloud interoperability is the capacity or extent at which one cloud service is connected with the other by trading data as per strategy to get results.

The two crucial components in Cloud interoperability are usability and connectivity, which are further divided into multiple layers.

1. Behaviour
2. Policy
3. Semantic
4. Syntactic
5. Transport
6. Portability

Categories of Cloud Computing Interoperability

1. **Application Interoperability –**
It is the interoperability between deployed components of an application deployed in a system.

Generally, applications that are built on the basis of design principles show better interoperability than those which are not.

2. **Platform Interoperability –**
   It is the interoperability between deployed components of platforms deployed in a system. It is an important aspect, as application interoperability can't be achieved without platform interoperability.
3. **Management Interoperability –**
   Here, the Cloud services like SaaS, PaaS or IaaS and applications related to self-service are assessed. It would be pre-dominant as Cloud services are allowing enterprises to work-in-house and eradicate dependency from third parties.
4. **Publication and Acquisition Interoperability –**
   Generally, it is the interoperability between various platforms like PaaS services and the online marketplace.

2)Portability

It is the process of transferring the data or an application from one framework to others, making it stay executable or usable. Portability can be separated into two types: Cloud data portability and Cloud application portability.

- Cloud data portability –
  It is the capability of moving information from one cloud service to another and so on without expecting to re-enter the data.
- Cloud application portability –
  It is the capability of moving an application from one cloud service to another or between a client's environment and a cloud service.

Categories of Cloud Computing portability :-

1. Data Portability –
   Data portability, which is also termed as cloud portability, refers to the transfer of data from one source to another source or from one service to another service, i.e. from one application to another application or it may be from one cloud service to another cloud service in the aim of providing a better service to the customer without affecting it's usability. Moreover, it makes the cloud migration process more easier.
2. Application Portability –
   It enables re-use of various application components in different cloud PaaS services. If the components are independent in their cloud service provider, then application portability can be a difficult task for the enterprise. But if components are not platform specific, porting to another platform is easy and effortless.
3. Platform Portability –
   There are two types of platform portability- platform source portability and machine image portability. In the case of platform source portability, e.g. UNIX OS, which is mostly written in C language, can be implemented by re-compiling on various different hardware and re-writing sections that are hardware-dependent which are not coded in C. Machine image portability binds application with platform by porting the resulting bundle which requires standard program representation.

3) Integration

1.Security:-

The cloud is likely more secure than on-premises, but businesses still need to take precautions to manage cloud risk and compliance. A robust cloud security solution must include functionality for user authentication and authorization, data encryption, and data backup and recovery. Depending on your industry, you may need to choose a tool such as Integrate.io that is compliant with standards such as HIPAA and SOC 2, which ensure that companies meet data security best practices.

2. Network Latency:-

Cloud environments are often preferred to on-premises because of their scalability: you can easily increase or decrease your usage of compute and storage resources in just a few minutes. But scaling your cloud environment will have a limited effect if your network latency is too high, which puts a firm cap on the data integration workloads you can run.

Hybrid clouds make use of wide-area networks (WANs) instead of local area networks (LANs). But WANs may become clogged by transmitting too many small, uncompressed data packets over a remote database connection, overburdening the network.

3. Choosing the Right Architecture:-

Choosing the right architecture for your cloud environment is essential. Most organizations have three options to choose from:

- A **public cloud** is offered by a third-party cloud provider, such as Amazon Web Services or Microsoft Azure.
- A **private cloud** is used only by a single organization.
- A **hybrid cloud** combines aspects of both public and private clouds.

What's more, many businesses pursue a "multi-cloud" strategy, in which they make use of services from multiple cloud vendors (e.g., different vendors for cloud computing, storage, and software). Public, private, hybrid, and multi-cloud all combine to offer a dizzying array of possibilities.

4. Data Governance Questions:-

Cloud integrations exchange massive quantities of data. How can you ensure that data quality remains high while maintaining compliance with IT protocols and procedures? "Data governance" is the term for the data management policies that ensure the high availability, integrity, and usability of your organization's data. Unfortunately, as they move to the cloud, many organizations fail to implement a solid plan for data governance. As a result, each new integration between different systems may introduce new issues and points of failure. Furthermore, as the size of your cloud environment grows, manually monitoring these integration points becomes increasingly infeasible.

5. Cloud Integration Anti-Patterns

In software development, an "anti-pattern" is a solution to a common problem that is usually ineffective and often actively counterproductive. Cloud integration, too, suffers from anti-patterns that can negatively impact performance and data quality.

According to Oracle, some of the most frequent cloud integration anti-patterns are:

- Scheduling jobs that execute for too long, starving other jobs of the resources they need.

- Developers who are creating their own connections to an application, which wastes time and makes the integration exponentially more difficult to manage.
- Reading very large files in memory.
- Failing to adjust integrations and workflows over time as your business requirements evolve.

6. On-Premise Integrations:-

Beyond choosing the right cloud architecture (see above), you also need to choose the right balance between cloud and on-premises. Even businesses that want to fully commit to the cloud may find that they need to leave some legacy systems behind on-premises.

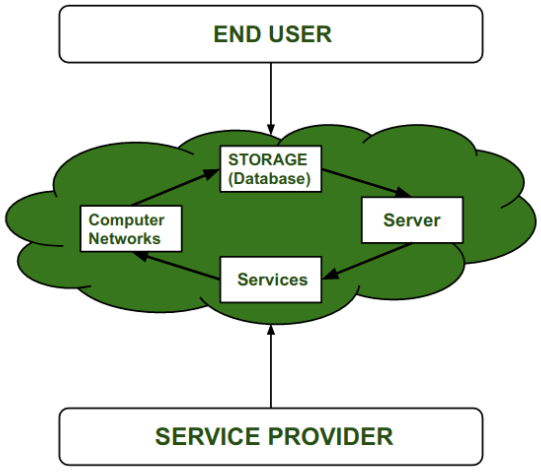
Solution: As with the issue of different cloud architectures, the challenge of integrating between cloud and on-premises needs to be addressed well before the project begins. Choose a cloud integration solution such as Integrate.io that can run on the public cloud, private cloud, and on-premises infrastructure. Make sure that you have a secure, well-built solution for user authentication and access so that employees can pass between the two environments without a hitch.

7. Deciding Between Custom and Pre-Built Solutions

With 84 percent of organizations using a multi-cloud strategy, the question is less about whether you need to think about cloud integration challenges and more about what solutions you'll use to address them.

The two basic options at your fingertips are custom-built and pre-built cloud data integrations. But it's not necessarily an either/or choice. You might use both possibilities for different integrations within a single cloud environment

4) Security :-



In this, we will discuss the overview of cloud computing, its need, and mainly our focus to cover the security issues in Cloud Computing. Let’s discuss it one by one.

- **Cloud Computing :**
  Cloud Computing is a type of technology that provides remote services on the internet to manage, access, and store data rather than storing it on Servers or local drives. This technology is also known as Serverless technology. Here the data can be anything like Image, Audio, video, documents, files, etc.

- **Need of Cloud Computing :**
  Before using Cloud Computing, most of the large as well as small IT companies use traditional methods i.e. they store data in Server, and they need a separate Server room for that. In that Server Room, there should be a database server, mail server, firewalls, routers, modems, high net speed devices, etc. For that IT companies have to spend lots of money. In order to reduce all the problems with cost Cloud computing come into existence and most companies shift to this technology.

Security Issues in Cloud Computing :

There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

Data Loss –
Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know

that our sensitive data is in the hands of Somebody else, and we don't have full control over our database. So if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

1. **Interference of Hackers and Insecure API's –**
   As we know if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain. An is the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So it may be possible that with the help of these services hackers can easily hack or harm our data.

2. **User Account Hijacking –**
   Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by Hacker. Then the hacker has full authority to perform Unauthorized Activities.

3. **Changing Service Provider –**
   Vendor lock In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they ace various problem's like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

4. **Lack of Skill –**
   While working, shifting to another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn't have skilled Employee. So it requires a skilled person to work with cloud Computing.

5. **Denial of Service (DoS) attack –**
   This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs data is lost. So in order to recover data, it requires a great amount of money as well as time to handle it.

Standards Organizations and Groups:-

At the recently concluded IEEE P2302 Inter-Cloud Interoperability Working Group meeting, it was noted that there are many SDOs working on cloud computing whitepapers, standards and specifications. The P2302 WG is interested in those that are addressing inter-cloud aspects including communications, policy, protocols, or security for potential collaboration. Inter-cloud scenarios include: public to public, public to private (and vice-versa), private to private cloud interconnections for both computing and storage.

Here is an incomplete list of Cloud Computing SDOs along with their output documents and work in progress:

1)NIST National Institute of Standards and Technology

Cloud Computing Project: NIST's role in cloud computing is to promote the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards.

Outputs:

-NIST definition of Cloud Computing v15 2009-10

-NIST Cloud Computing Standards Roadmap Working draft – 12th 2011.05-24

2)ISO/IEC JTC1 SC38

Distributed Application Platforms and Services: Study group on Cloud Computing is addressing:

-Terms of Reference of Study Group on Cloud computing :

-Provide a taxonomy, terminology and value proposition for Cloud Computing

-Assess the current state of standardization in Cloud Computing within JTC 1 and in other SDOs and consortia -beginning with document JTC 1 N 9687.

-Document standardization market/business/user requirements and the challenges to be addressed.

-Liaise and collaborate with relevant SDOs and consortia related to Cloud Computing

-Hold open meetings to gather requirements as needed from a wide range of interested organizations.

-Provide a report of activities and recommendations to SC 38 including: reviewing current concepts, characteristics, definitions, use cases, reference architecture, types and components used in Cloud Computing; a comparison of Cloud Computing to related technologies; analysing standardization activities for Cloud Computing in other standards organizations.

Output: Draft Study Group on Cloud Computing report V.2 2011-05

3)Cloud Computing Use Case Discussion Group

This open discussion group exists to define use cases for cloud computing. Theyare considering: Definitions and Taxonomy, Use Case Scenarios, Customer Scenarios, Developer Requirements, Security Scenarios & use cases and recommendations for SLAs.

Output: Cloud Computing Use Case whitepaper v4 July 2010

4)Global Inter-Cloud Technology Forum (GICTF)

This Japan based forum is trying to promote standardization of network protocols and the interfaces through which cloud systems inter-work with each other, and to enable the provision of more reliable cloud services

Output: Use cases and Functional Requirements for Inter-Cloud Computing White paper v1 2010-08

5)ETSI Cloud

In June 2006 ETSI technical committee GRID was created and held its first meeting in September.
TC GRID's task is to address issues associated with the convergence of Information Technology (IT) and telecommunications, paying particular attention initially to the lack of interoperable Grid solutions in situations which involve contributions from both the IT and telecommunications industries.

In 2008, TC GRID undertook a survey of existing stakeholders in the Grid domain, for which the European Commission (EC) provided financial support. A test frame for Grid standards is being developed in collaboration with ETSI's Centre for Testing & Interoperability (CTI).

There is also an increasing interest in addressing the convergence between ETSI technical committees GRID and TISPAN (Telecommunication and Internet converged Services and Protocols for Advanced Networking).

Outputs:

-Use Cases for Cloud Service Scenarios Technical Report (TR) v1 2010-2011

-Standardization requirements for cloud services (ETSI TR102 997) TR v1 2010-2011

6)Distributed Management Task Force (DMTF)

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. One of the key standards it maintained is the Common Information Model (CIM) .

Outputs:
-Use cases and interactions for Managing Clouds DSP-IP0103 2010-6-18

-Interoperable Clouds (DSP-IS0101) White paper v1.0.0 2009-11-11

-Architecture for Managing Clouds(DSP-IS0102) White paper v1.0.0 2010-6-18
-Cloud Management Interface Requirements on Protocol, Operations, Security & Message Specification v1.0.0

-Cloud Service Management Models Specification v.1.0.0 At the latest by 2011-12-31

-Open Virtualization Format (DSP0243) Standard v1.0 2009- Feb

-August 2010, DeltaCloud API specification for **Apache Delta cloud has been submitted to the DMTF to be an candidate standard for inter-cloud operations**.

7)CSA Cloud Security Alliance

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

Outputs:

-Top Threats to Cloud Computing White paper v1.0 2010-03

-Security Guidance for Critical Areas of Focus in Cloud Computing White paper v3 Q4 2011

-CSA Cloud Control Matrix Trusted Cloud Initiative Controls framework v1.1 2011-2

-Trusted Cloud Initiative Certification v1 Q4 2010

-Cloud audit / cloud trust protocols white paper v1 Q4 2011