UNIT 3: Cloud Architecture, Services And Storage: Layered Cloud Architecture Design – NIST Cloud Computing Reference Architecture – Public, Private and Hybrid Clouds – laaS – PaaS – SaaS – Architectural Design Challenges – Cloud Storage – Storage-as-a-Service – Advantages of Cloud Storage – Cloud Storage Providers – S3.

Layered Cloud Architectural Development:

- The architecture of a cloud is developed at three layers: infrastructure, platform, and application, as demonstrated in Figure 4.15. These three development layers are implemented with virtualization and standardization of hardware and software resources provisioned in the cloud.
- The services to public, private, and hybrid clouds are conveyed to users through networking support over the Internet and intranets involved. It is clear that the infrastructure layer is deployed first to support IaaS services. This infrastructure layer serves as the foundation for building the platform layer of the cloud for supporting PaaS services. In turn, the platform layer is a foundation for implementing the application layer for SaaS applications. Different types of cloud services demand application of these resources separately.
- The infrastructure layer is built with virtualized compute, storage, and network resources. The abstraction of these hardware resources is meant to provide the flexibility demanded by users. Internally, virtualization realizes automated provisioning of resources and optimizes the infrastructure management process. The platform layer is for general-purpose and repeated usage of the collection of software resources. This layer provides users with an environment to develop their applications, to test operation flows, and to monitor execution results and performance.
- The platform should be able to assure users that they have scalability, dependability, and security protection. In a way, the virtualized cloud platform serves as a “system middleware” between the infrastructure and application layers of the cloud.

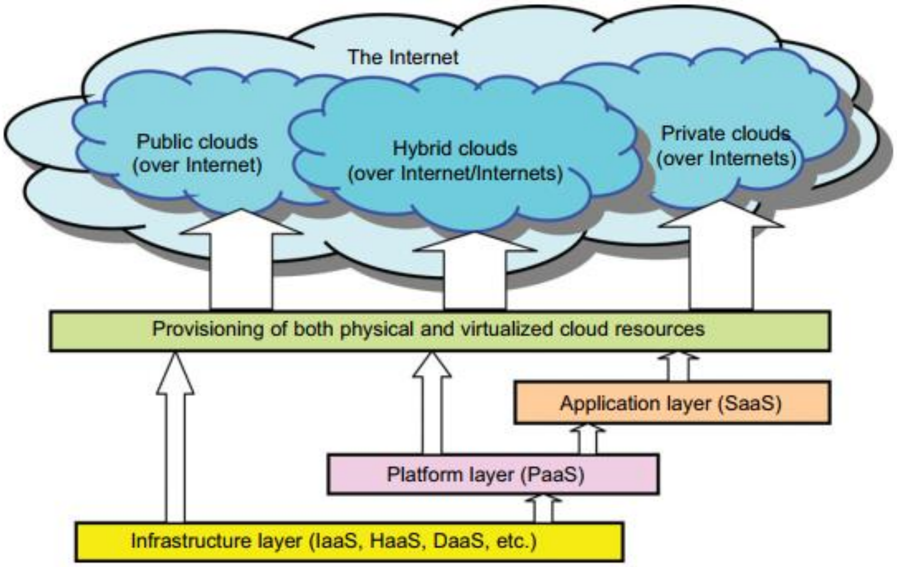
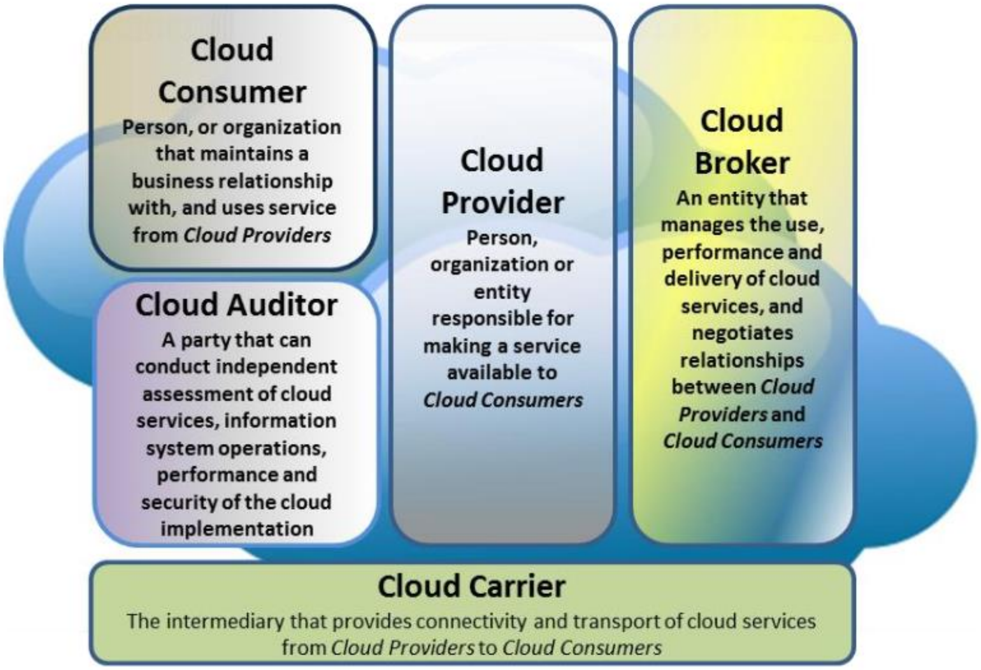

The Internet
Public clouds (over Internet)
Hybrid clouds (over Internet/Internets)
Private clouds (over Internets)
Provisioning of both physical and virtualized cloud resources
Application layer (SaaS)
Platform layer (PaaS)
Infrastructure layer (IaaS, HaaS, DaaS, etc.)

FIGURE 4.15

Layered architectural development of the cloud platform for IaaS, PaaS, and SaaS applications over the Internet.

- The application layer is formed with a collection of all needed software modules for SaaS applications. Service applications in this layer include daily office management work, such as information retrieval, document processing, and calendar and authentication services. The application layer is also heavily used by enterprises in business marketing and sales, consumer relationship management (CRM), financial transactions, and supply chain management. It should be noted that not all cloud services are restricted to a single layer.
- Many applications may apply resources at mixed layers. After all, the three layers are built from the bottom up with a dependence relationship. From the provider's perspective, the services at various layers demand different amounts of functionality support and resource management by providers. In general, SaaS demands the most work from the provider, PaaS is in the middle, and IaaS demands the least. For example, Amazon EC2 provides not only virtualized CPU resources to users, but also management of these provisioned resources. Services at the application layer demand more work from providers. The best example of this is the Salesforce.com CRM service, in which the provider supplies not only the hardware at the bottom layer and the software at the top layer, but also the platform and software tools for user application development and monitoring.

NIST Cloud Computing Reference Architecture:


Cloud Consumer
Person, or organization that maintains a business relationship with, and uses service from *Cloud Providers*
Cloud Auditor
A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation
Cloud Provider
Person, organization or entity responsible for making a service available to *Cloud Consumers*
Cloud Broker
An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*
Cloud Carrier
The intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*

There are five major actors in NIST cloud computing reference architecture as shown in above figure.

These actors are listed below

- Cloud Consumer.
- Cloud Provider.
- Cloud Carrier.
- Cloud Auditor.
- Cloud Broker.

Each actor is an entity may be a person or an organization that participates in a transaction or process and/or performs tasks in cloud computing.

1. Cloud Consumer

- Cloud consumer is the main participants of cloud computing environment.
- A cloud consumer is a person or organization that use the cloud services such as SaaS, PaaS and IaaS.
- A cloud consumer browses the service catalog provided by a cloud provider, cloud consumer requests the appropriate service.
- Cloud provider sets up cloud environment for the service and make a contracts with the cloud consumer for the use of the service.
- Cloud consumers need cloud **Service Level Agreement(SLA**).

SLA act as a agreement for technical performance requirements provided by a cloud provider. Some terms and conditions regarding the quality of service, security, remedies for performance failures are mentioned in the SLA.

- **Software** as a service applications in the cloud are made accessible via a network to the SaaS consumers.
- The consumers of SaaS may be a organization that gives their employee with access to software applications, end users who directly use software applications, or it may be software application administrators who is responsible for configure applications on the software for the customers.
- Platform as a service can also be employ by the consumer the tools to develop, test, deploy and manage the applications hosted in a cloud environment.
- PaaS consumers can be application developers who design and implement application software in software company.
- PaaS consumer may be application testers who run and test applications in cloud-based environments, application deployers who publish applications into the cloud,
- PaaS may be a application administrators who configure and monitor application performance on a platform.
- Cloud Consumers of Infrastructure as a service have access to different hardware resources like virtual computers, network devices such as router, storage media and other fundamental computing resource.
- The consumers of Infrastructure as a service may be system developers, system administrators and IT managers who creates, install, manage and monitor the services for IT infrastructure operations.

Cloud Provider

- A cloud provider is responsible for making a service available to the cloud consumer. Cloud provider may be a person , team or an organization.
- A Cloud Provider maintain and manages the different cloud computing services for the consumer and makes arrangement to deliver the cloud services to the Cloud Consumers suing network access or internet.
- In context to **Software as a Service** Cloud provider is responsible for deploys, configuring, maintaining and updating the operation of the software applications on a cloud infrastructure so that the services are provisioned as per the required levels by the cloud consumers.
- The major responsibilities of cloud provider in context to software as a service are to manage , control the applications and overall infrastructure.
- In context to **Platform as a Service**, the Cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform. These components may be software execution stack, databases and some other components that act as middleware.
- The PaaS Cloud Provider generally supports the development, deployment and management process of the Platform as a Service.
- Some integrated tools like IDE, SDK, development version of cloud software, deployment and management are also the part of Platform as a Service.
- Physical computing resources such as servers, networks, storage and hosting infrastructure are also maintain and manage by the cloud provider for the consumer of **Infrastructure as a Service**.

- The Cloud Provider implement the cloud software so that computing resources become available to the Cloud Consumer who use the infrastructure as service through a set of service interface and virtual network interfaces that helps in resource abstraction.

3. Cloud Auditor

- A cloud auditor is a dedicated team of technically skilled person that can perform an independent examination or review of cloud service controls with the intent to express strength and weakness of the process and some suggestion or improvement.
- Audits are performed to verify the standards of services after checking the evidence.
- Major role of a cloud auditor is to evaluate the services provided by a cloud provider against the parameters such as security controls, privacy impact and performance etc.
- To perform the audit of security a cloud auditor do the assessment of the security controls in the information system to determine the extent to which the controls are implemented accurately and operating as per expectation and producing the desired outcome with respect to the security requirements for the system.

4. Cloud Broker

Some time services integrations becomes more complex due to which it becomes difficult for the cloud consumer to manage the cloud service.

In such situation cloud consumer request cloud services from cloud broker. Cloud Broker acts as mediator between consumer and provider.

- A cloud broker manages the delivery of cloud services , their performance and use.
- A cloud broker negotiates relationships between cloud providers and cloud consumers.

In general, a cloud broker involves in three types of activities which are as follow

Service Intermediation

- A cloud broker may enhances a given service by improving some specific capability and providing value-added services to cloud consumers.
- The improvement may be related to managing the access to cloud services, identity management, performance reporting, enhanced security, etc.

Service Aggregation

- Services aggregation can be seems as combining and integrating multiple services into one or some more new services.
- The broker ensures the data movement between the cloud consumer and multiple cloud providers in secure manner.
- A cloud broker also provides the data integration.

Service Arbitrage

- Service arbitrage is very similar to service aggregation but there is a little bit difference also.
- In service arbitrage the services to be aggregated are not fixed in advance.
- In Service arbitrage a broker has the flexibility to select the services from multiple agencies.
- The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

5. Cloud Carrier

Cloud Carrier is another important actors in NIST cloud computing reference architecture.

- Role of cloud carrier is to provide the connectivity and transport of cloud services between cloud consumers and cloud providers.
- Cloud carriers provide access to consumers through network, telecommunication and other access devices.

For example- cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices.

Public, Private and Hybrid Clouds:

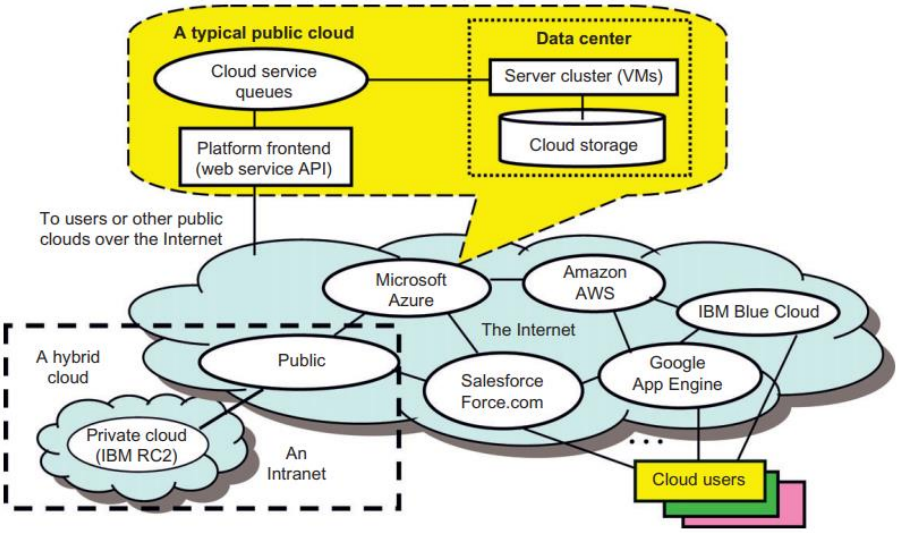


FIGURE 4.1

Public, private, and hybrid clouds illustrated by functional architecture and connectivity of representative clouds available by 2011.

As Figure 4.1 shows, both public clouds and private clouds are developed in the Internet. As many clouds are generated by commmercial providers or by enterprises in a distributed manner, they will be interconnected over the Internet to achieve scalable and efficient computing services. Commercial cloud providers such as Amazon, Google, and Microsoft created their platforms to be distributed geographically.

PUBLIC CLOUD:

- A public cloud is built over the Internet and can be accessed by any user who has paid for the service. Public clouds are owned by service providers and are accessible through a subscription. The callout box in top of Figure 4.1 shows the architecture of a typical public cloud.
- Many public clouds are available, including Google App Engine (GAE), Amazon Web Services (AWS), Microsoft Azure, IBM Blue Cloud, and Salesforce.com's Force.com. The providers of the aforementioned clouds are commercial providers that offer a publicly accessible remote interface for creating and managing VM instances within their proprietary infrastructure.
- A public cloud delivers a selected set of business processes. The application and infrastructure services are offered on a flexible price-per-use basis.

Advantages of Public Cloud

There are the following advantages of Public Cloud -

- Public cloud is owned at a lower cost than the private and hybrid cloud.
- Public cloud is maintained by the cloud service provider, so do not need to worry about the maintenance.
- Public cloud is easier to integrate. Hence it offers a better flexibility approach to consumers.
- Public cloud is location independent because its services are delivered through the internet.
- Public cloud is highly scalable as per the requirement of computing resources.
- It is accessible by the general public, so there is no limit to the number of users.

Disadvantages of Public Cloud

- Public Cloud is less secure because resources are shared publicly.
- Performance depends upon the high-speed internet network link to the cloud provider.
- The Client has no control of data.

Private Clouds:

- A private cloud is built within the domain of an intranet owned by a single organization. Therefore, it is client owned and managed, and its access is limited to the owning clients and their partners. Its deployment was not meant to sell capacity over the Internet through publicly accessible interfaces.
- Private clouds give local users a flexible and agile private infrastructure to run service workloads within their administrative domains. A private cloud is supposed to deliver more efficient and convenient cloud services. It may impact the cloud standardization, while retaining greater customization and organizational control.

Advantages of Private Cloud

There are the following advantages of the Private Cloud -

- Private cloud provides a high level of security and privacy to the users.
- Private cloud offers better performance with improved speed and space capacity.

- It allows the IT team to quickly allocate and deliver on-demand IT resources.
- The organization has full control over the cloud because it is managed by the organization itself. So, there is no need for the organization to depends on anybody.
- It is suitable for organizations that require a separate cloud for their personal use and data security is the first priority.

Disadvantages of Private Cloud

- Skilled people are required to manage and operate cloud services.
- Private cloud is accessible within the organization, so the area of operations is limited.
- Private cloud is not suitable for organizations that have a high user base, and organizations that do not have the prebuilt infrastructure, sufficient manpower to maintain and manage the cloud.

Hybrid Clouds:

- A hybrid cloud is built with both public and private clouds, as shown at the lower-left corner of Figure 4.1. Private clouds can also support a hybrid cloud model by supplementing local infrastructure with computing capacity from an external public cloud.
- For example, the Research Compute Cloud (RC2) is a private cloud, built by IBM, that interconnects the computing and IT resources at eight IBM Research Centers scattered throughout the United States, Europe, and Asia. A hybrid cloud provides access to clients, the partner network, and third parties.
- In summary, public clouds promote standardization, preserve capital investment, and offer application flexibility. Private clouds attempt to achieve customization and offer higher efficiency, resiliency, security, and privacy. Hybrid clouds operate in the middle, with many compromises in terms of resource sharing.

Advantages of Hybrid Cloud

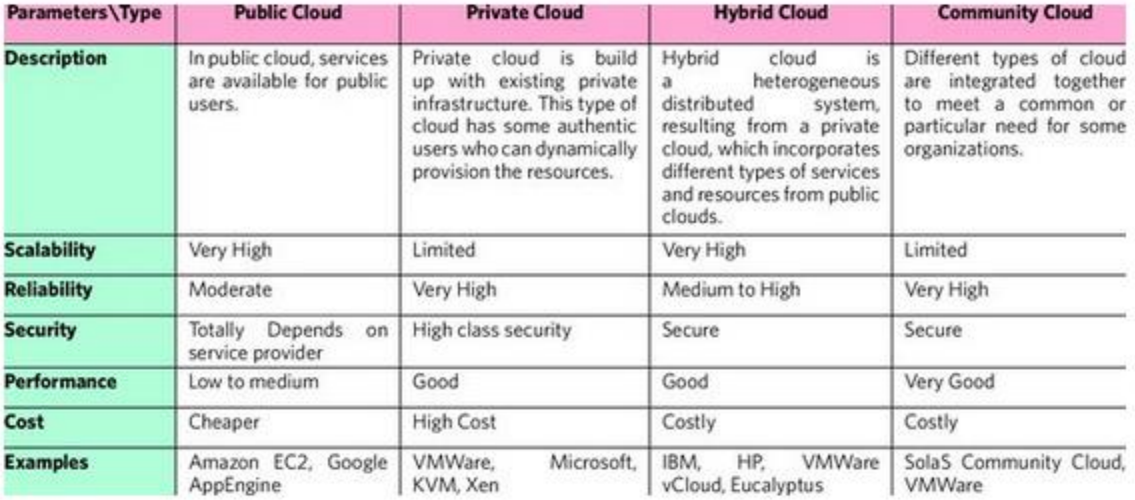
There are the following advantages of Hybrid Cloud -

- Hybrid cloud is suitable for organizations that require more security than the public cloud.
- Hybrid cloud helps you to deliver new products and services more quickly.
- Hybrid cloud provides an excellent way to reduce the risk.
- Hybrid cloud offers flexible resources because of the public cloud and secure resources because of the private cloud.

Disadvantages of Hybrid Cloud

- In Hybrid Cloud, security feature is not as good as the private cloud.
- Managing a hybrid cloud is complex because it is difficult to manage more than one type of deployment model.
- In the hybrid cloud, the reliability of the services depends on cloud service providers.

Difference Between Private Cloud, Public Cloud and Hybrid Cloud:



Parameters\Type	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud
Description	In public cloud, services are available for public users.	Private cloud is build up with existing private infrastructure. This type of cloud has some authentic users who can dynamically provision the resources.	Hybrid cloud is a heterogeneous distributed system, resulting from a private cloud, which incorporates different types of services and resources from public clouds.	Different types of cloud are integrated together to meet a common or particular need for some organizations.
Scalability	Very High	Limited	Very High	Limited
Reliability	Moderate	Very High	Medium to High	Very High
Security	Totally Depends on service provider	High class security	Secure	Secure
Performance	Low to medium	Good	Good	Very Good
Cost	Cheaper	High Cost	Costly	Costly
Examples	Amazon EC2, Google AppEngine	VMWare, Microsoft, KVM, Xen	IBM, HP, VMWare vCloud, Eucalyptus	SolaS Community Cloud, VMWare

IaaS – PaaS – SaaS:

- Cloud computing delivers infrastructure, platform, and software (application) as services, which are made available as subscription-based services in a pay-as-you-go model to consumers.
- The services provided over the cloud can be generally categorized into three different service models: namely IaaS, Platform as a Service (PaaS), and Software as a Service (SaaS). These form the three pillars on top of which cloud computing solutions are delivered to end users. All three models allow users to access services over the Internet, relying entirely on the infrastructures of cloud service providers. These models are offered based on various SLAs between providers and users.
- In a broad sense, the SLA for cloud computing is addressed in terms of service availability, performance, and data protection and security. Figure 4.5 illustrates three cloud models at different service levels of the cloud. SaaS is applied at the application end using special interfaces by users or clients. At the PaaS layer, the cloud platform must perform billing services and handle job queuing, launching, and monitoring services. At the bottom layer of the IaaS services, databases, compute instances, the file system, and storage must be provisioned to satisfy user demands.

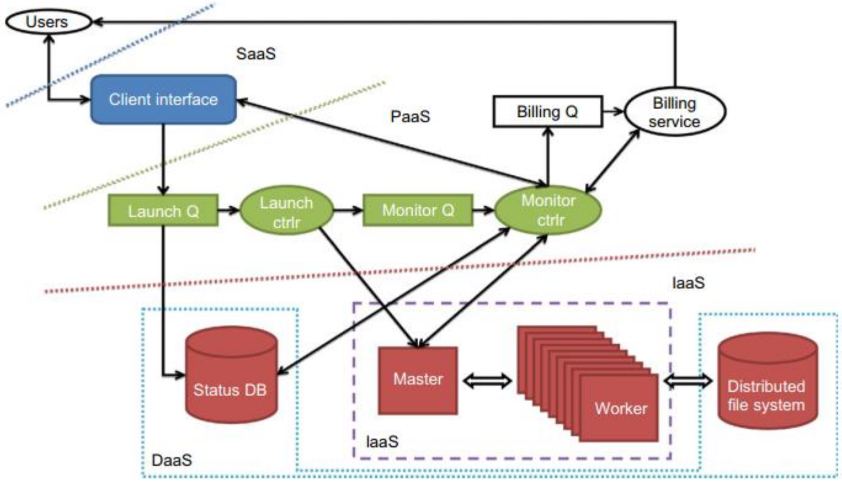


FIGURE 4.5

The IaaS, PaaS, and SaaS cloud service models at different service levels..

Infrastructure as a Service:

- This model allows users to use virtualized IT resources for computing, storage, and networking. In short, the service is performed by rented cloud infrastructure. The user can deploy and run his applications over his chosen OS environment.
- The user does not manage or control the underlying cloud infrastructure, but has control over the OS, storage, deployed applications, and possibly select networking components. This IaaS model encompasses storage as a service, compute instances as a service, and communication as a service.

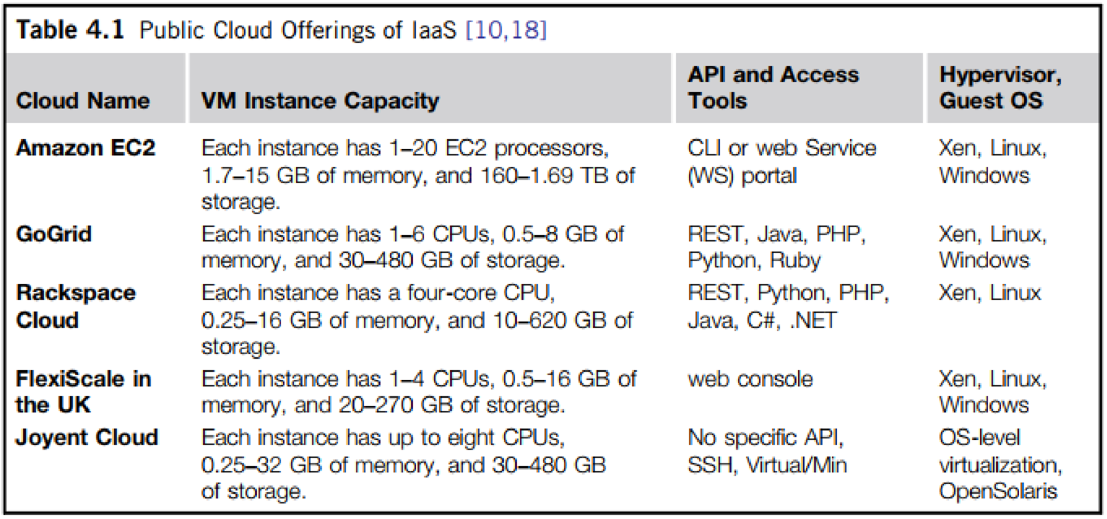


Table 4.1 Public Cloud Offerings of IaaS [10,18]

Cloud Name	VM Instance Capacity	API and Access Tools	Hypervisor, Guest OS
Amazon EC2	Each instance has 1–20 EC2 processors, 1.7–15 GB of memory, and 160–1.69 TB of storage.	CLI or web Service (WS) portal	Xen, Linux, Windows
GoGrid	Each instance has 1–6 CPUs, 0.5–8 GB of memory, and 30–480 GB of storage.	REST, Java, PHP, Python, Ruby	Xen, Linux, Windows
Rackspace Cloud	Each instance has a four-core CPU, 0.25–16 GB of memory, and 10–620 GB of storage.	REST, Python, PHP, Java, C#, .NET	Xen, Linux
FlexiScale in the UK	Each instance has 1–4 CPUs, 0.5–16 GB of memory, and 20–270 GB of storage.	web console	Xen, Linux, Windows
Joyent Cloud	Each instance has up to eight CPUs, 0.25–32 GB of memory, and 30–480 GB of storage.	No specific API, SSH, Virtual/Min	OS-level virtualization, OpenSolaris

Platform as a Service (PaaS):

- To be able to develop, deploy, and manage the execution of applications using provisioned resources demands a cloud platform with the proper software environment. Such a platform includes operating system and runtime library support. This has triggered the creation of the PaaS model to enable users to develop and deploy their user applications.

- The platform cloud is an integrated computer system consisting of both hardware and software infrastructure. The user application can be developed on this virtualized cloud platform using some programming languages and software tools supported by the provider (e.g., Java, Python, .NET).
- The user does not manage the underlying cloud infrastructure. The cloud provider supports user application development and testing on a well-defined service platform. This PaaS model enables a collaborated software development platform for users from different parts of the world. This model also encourages third parties to provide software management, integration, and service monitoring solutions.

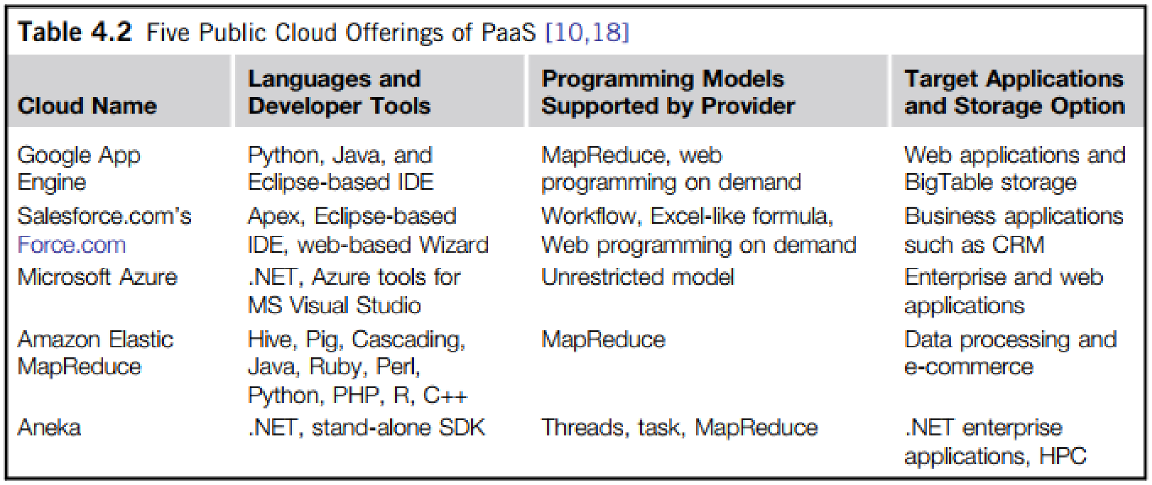


Table 4.2 Five Public Cloud Offerings of PaaS [10,18]

Cloud Name	Languages and Developer Tools	Programming Models Supported by Provider	Target Applications and Storage Option
Google App Engine	Python, Java, and Eclipse-based IDE	MapReduce, web programming on demand	Web applications and BigTable storage
Salesforce.com's Force.com	Apex, Eclipse-based IDE, web-based Wizard	Workflow, Excel-like formula, Web programming on demand	Business applications such as CRM
Microsoft Azure	.NET, Azure tools for MS Visual Studio	Unrestricted model	Enterprise and web applications
Amazon Elastic MapReduce	Hive, Pig, Cascading, Java, Ruby, Perl, Python, PHP, R, C++	MapReduce	Data processing and e-commerce
Aneka	.NET, stand-alone SDK	Threads, task, MapReduce	.NET enterprise applications, HPC

Software as a Service (SaaS):

- This refers to browser-initiated application software over thousands of cloud customers. Services and tools offered by PaaS are utilized in construction of applications and management of their deployment on resources offered by IaaS providers. The SaaS model provides software applications as a service.
- As a result, on the customer side, there is no upfront investment in servers or software licensing. On the provider side, costs are kept rather low, compared with conventional hosting of user applications. Customer data is stored in the cloud that is either vendor proprietary or publicly hosted to support PaaS and IaaS.
- The best examples of SaaS services include Google Gmail and docs, Microsoft SharePoint, and the CRM software from Salesforce.com. They are all very successful in promoting their own business or are used by thousands of small businesses in their day-to-day operations. Providers such as Google and Microsoft offer integrated IaaS and PaaS services, whereas others such as Amazon and GoGrid offer pure IaaS services and expect third-party PaaS providers such as Manjrasoft to offer application development and deployment services on top of their infrastructure services.
- Three Success Stories on SaaS Applications:
  - To discover new drugs through DNA sequence analysis, Eli Lily Company has used Amazon's AWS platform with provisioned server and storage clusters to conduct high-

performance biological sequence analysis without using an expensive supercomputer. The benefit of this IaaS application is reduced drug deployment time with much lower costs.

- The New York Times has applied Amazon’s EC2 and S3 services to retrieve useful pictorial information quickly from millions of archival articles and newspapers. The New York Times has significantly reduced the time and cost in getting the job done.
- Pitney Bowes, an e-commerce company, offers clients the opportunity to perform B2B transactions using the Microsoft Azure platform, along with .NET and SQL services. These offerings have significantly increased the company’s client base.

Architectural Design Challenges:

Following are six open challenges in cloud architecture development:

1. Service Availability and Data Lock-in Problem:

- The management of a cloud service by a single company is often the source of single points of failure. To achieve HA, one can consider using multiple cloud providers. Even if a company has multiple data centers located in different geographic regions, it may have common software infrastructure and accounting systems. Therefore, using multiple cloud providers may provide more protection from failures. Another availability obstacle is distributed denial of service (DDoS) attacks.
- Software stacks have improved interoperability among different cloud platforms, but the APIs itself are still proprietary. Thus, customers cannot easily extract their data and programs from one site to run on another.

2. Data Privacy and Security Concerns:

- Current cloud offerings are essentially public (rather than private) networks, exposing the system to more attacks. Many obstacles can be overcome immediately with well-understood technologies such as encrypted storage, virtual LANs, and network middleboxes (e.g., firewalls, packet filters).

3. Unpredictable Performance and Bottlenecks:

- Multiple VMs can share CPUs and main memory in cloud computing, but I/O sharing is problematic.
  For example, to run 75 EC2 instances with the STREAM benchmark requires a mean bandwidth of 1,355 MB/second. However, for each of the 75 EC2 instances to write 1 GB files to the local disk requires a mean disk write bandwidth of only 55 MB/second. This demonstrates the problem of I/O interference between VMs.
- Internet applications continue to become more data-intensive. If we assume applications to be “pulled apart” across the boundaries of clouds, this may complicate data placement and transport.

4. Distributed Storage and Widespread Software Bugs:

- The database is always growing in cloud applications. The opportunity is to create a storage system that will not only meet this growth, but also combine it with the cloud advantage of scaling arbitrarily up and down on demand. This demands the design of efficient distributed SANs.
- Large-scale distributed bugs cannot be reproduced, so the debugging must occur at a scale in the production data centers. No data center will provide such a convenience. One solution may be a reliance on using VMs in cloud computing.

5. Cloud Scalability, Interoperability, and Standardization:

- The pay-as-you-go model applies to storage and network bandwidth; both are counted in terms of the number of bytes used. Computation is different depending on virtualization level. GAE automatically scales in response to load increases and decreases; users are charged by the cycles used. AWS charges by the hour for the number of VM instances used, even if the machine is idle.
- The opportunity here is to scale quickly up and down in response to load variation, in order to save money, but without violating SLAs.

6. Software Licensing and Reputation Sharing:

- Many cloud computing providers originally relied on open source software because the licensing model for commercial software is not ideal for utility computing.
- The primary opportunity is either for open source to remain popular or simply for commercial software companies to change their licensing structure to better fit cloud computing. One can consider using both pay-for-use and bulk-use licensing schemes to widen the business coverage.

Cloud Storage:

Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It’s delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure. This gives you agility, global scale and durability, with “anytime, anywhere” data access.

Cloud storage is purchased from a third party cloud vendor who owns and operates data storage capacity and delivers it over the Internet in a pay-as-you-go model. These cloud storage vendors manage capacity, security and durability to make data accessible to your applications all around the world.

Cloud storage is based on a virtualized storage infrastructure with accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud-based data is stored in logical pools across disparate, commodity storage servers located on premises or in a data center managed by a third-party cloud provider.

Types of cloud storage

There are three main cloud storage options, based on different access models: public, private and hybrid.

Public cloud: These storage services provide a multi-tenant storage environment that is most suited for unstructured data on a subscription basis. Data is stored in the service provider's data centers with storage data spread across multiple regions or continents. Customers generally pay on a per-use basis, similar to the utility payment model. In many cases, there are also transaction charges based on frequency and the volume of data being accessed. This market sector is dominated by the following services:

- Amazon Simple Storage Service (S3);
- Amazon Glacier for deep archival or cold storage;
- Google Cloud Storage;
- Google Cloud Storage Nearline for cold data; and
- Microsoft Azure.

Private cloud: A private cloud storage service is an in-house storage resource deployed as a dedicated environment protected behind a firewall. Internally hosted private cloud storage implementations emulate some of the features of commercial public cloud services, providing easy access and allocation of storage resources for business users, as well as object storage protocols. Private clouds are appropriate for users who need customization and more control over their data or who have stringent data security or regulatory requirements.

Hybrid cloud: This cloud storage option is a mix of private cloud storage and third-party public cloud storage services, with a layer of orchestration management to operationally integrate the two platforms.

The model offers businesses flexibility and more data deployment options. An organization might, for example, store actively used and structured data in an on-premises private cloud and unstructured and archival data in a public cloud. A hybrid environment also makes it easier to handle seasonal or unanticipated spikes in data creation or access by cloud bursting to the external storage service and avoiding having to add in-house storage resources.

How does cloud storage work?

Cloud service providers maintain large data centers in multiple locations around the world. When customers purchase cloud storage from a provider, they turn over most aspects of the data storage to the vendor, including security, capacity, storage servers and computing resources, data availability and delivery over a network. Customer applications can access the stored cloud data through traditional storage protocols or application programming indicators (APIs), or they can also be moved to the cloud.

How cloud storage works varies depending on the type of storage used. The three main types are block storage, file storage and object storage:

- **Block storage** divides large volumes of data into smaller units called *blocks*. Each block is associated with a unique identifier and placed on one of the system's storage drives. Block storage is fast, efficient and provides the low latency required by applications such as databases and high-performance workloads.

- **File storage** organizes data in a hierarchical system of files and folders; it is commonly used with personal computer storage drives and network-attached storage (NAS). Data in a file storage system is stored in files, and the files are stored in folders. Directories and subdirectories are used to organize the folders and locate files and data. A file storage-based cloud can make data access and retrieval easier, with this hierarchical format being familiar to users and required by some applications.
- **Object storage** stores data as objects, which consist of three components: data stored in a file, metadata associated with the data file and a unique identifier. Using the RESTful API, an object storage protocol stores a file and its associated metadata as a single object and assigns it an identification (ID) number. To retrieve content, the user presents the ID to the system and the content is assembled with all its metadata, authentication and security. Object-based storage systems allow metadata to be customized, which can streamline data access and analysis. With object storage, data can be stored in its native format with massive scalability.

Storage as a service (STaaS):

STaaS is a managed service in which the provider supplies the customer with access to a data storage platform. The service can be delivered on premises from infrastructure that is dedicated to a single customer, or it can be delivered from the public cloud as a shared service that's purchased by subscription and is billed according to one or more usage metrics.

STaaS can be used for data transfers and redundant storage, as well as to restore any corrupted or lost data. Instead of storing data on-premises, organizations that use STaaS will typically utilize a public cloud for storage and backup needs. Public cloud storage may also use different storage methods for STaaS. These storage methods include backup and restore, disaster recovery, block storage, SSD storage, object storage and bulk data transfer. Backup and restore refers to the backing up of data to the cloud, which provides protection in case of data loss. Disaster recovery may refer to protecting and replicating data from virtual machines (VMs).

Advantages of STaaS

Key advantages to STaaS in the enterprise include the following:

- **Storage costs.** Personnel, hardware and physical storage space expenses are reduced.
- **Disaster recovery.** Having multiple copies of data stored in different locations can better enable disaster recovery measures.
- **Scalability.** With most public cloud services, users only pay for the resources that they use.
- **Syncing.** Files can be automatically synced across multiple devices.
- **Security.** Security can be both an advantage and a disadvantage, as security methods may change per vendor. Data tends to be encrypted during transmission and while at rest.

Disadvantages of STaaS

Common disadvantages of STaaS include the following:

- **Security.** Users may end up transferring business-sensitive or mission-critical data to the cloud, which makes it important to choose a service provider that's reliable.
- **Potential storage costs.** If bandwidth limitations are exceeded, these could be expensive.
- **Potential downtimes.** Vendors may go through periods of downtime where the service is not available, which can be trouble for mission-critical data.
- **Limited customization.** Since the cloud infrastructure is owned and managed by the service provider, it is less customizable.
- **Potential for vendor lock-in.** It may be difficult to migrate from one service to another.

Popular storage-as-a-service vendors

Examples of STaaS vendors include Dell EMC, Hewlett Packard Enterprise (HPE), NetApp and IBM. Dell EMC provides Isilon NAS storage, EMC Unity hybrid-flash storage and other storage options. HPE has an equally large, if not larger, presence in storage systems compared to Dell EMC.

Advantages of using cloud storage

1. **Cost reduction:** The largest benefit of cloud storage is cost saving. It lets you save considerable capital costs because no actual hardware expenditures are required.
2. **Security:** There are several reasons why cloud storage is more reliable than in-house computing, including certain high-profile cloud data breaches.
3. **Reliability:** One of the main benefits of cloud storage for businesses is reliability. You will still get updated about the updates immediately.
4. **Data centralization:** There are also projects that are housed in a specific location that can be viewed anywhere and at any time.
5. **Ease of accessibility:** An Internet cloud infrastructure maximizes enterprise productivity and efficiency by ensuring your application is always accessible.
6. **Mobility:** Both facilities can be easily obtained by staff operating on the premises or at distant locations. What they need is a link to the Internet.
7. **Unlimited storage capacity:** The cloud has computing space that is nearly infinite. You can easily increase the storage space at any time with very nominal monthly charges.

Disadvantages of cloud storage

1. **Vulnerability to attacks:** Security vulnerability is another downside of dealing with cloud computing providers. Any confidential information about the business can be exchanged with a third-party cloud computing service provider. Hackers could exploit this knowledge.
2. **Downtime:** That's because your cloud provider may face power failure, poor access to the internet, maintenance of services, etc.
3. **Vendor Agreement:** A organization may face some severe challenges due to the discrepancies between provider solutions as it wants to switch from one cloud platform to another.
4. **Limited control:** Cloud clients can be faced with minimal influence over their implementations. On remote servers that are entirely operated and managed by service providers, cloud services run.
5. **Platform dependencies:** Another of the drawbacks of cloud storage is tacit dependence, also known as provider lock-in'. Deep-rooted discrepancies between provider platforms will often make it difficult to switch from one cloud platform to another.

6. **Lack of support:** Cloud Storage providers struggle to provide clients with sufficient assistance. In addition, they tend to focus on FAQs or online assistance from their customers, which can be a boring task for non-technical individuals.
7. **Technical issues:** Cloud infrastructure is often vulnerable to instability and other technological problems. Even in terms of retaining high maintenance standards, the best cloud service provider companies can face this kind of challenge.

Cloud storage provider:

1. A cloud storage provider, also known as a managed service provider (MSP), is a company that offers organizations and individuals the ability to place and retain data in an off-site storage system. Customers can lease cloud storage capacity per month or on demand.
2. A cloud storage provider hosts a customer's data in its own data center, providing fee-based computing, networking and storage infrastructure. Both individual and corporate customers can get unlimited storage capacity on a provider's servers at a low per-gigabyte price.
3. Rather than store data on local storage devices, such as a hard disk drive, flash storage or tape, customers choose a cloud storage provider to host data on a system in a remote data center. Users can then access those files using an internet connection.
4. The delivery of IT services via the internet is broadly defined as cloud computing or utility computing. This business model first hit mainstream enterprises with the rise of application service providers.
5. A cloud storage provider also sells non-storage services for a fee. Enterprises purchase compute, software, storage and related IT components as discrete cloud services with a pay-as-you-go license. For example, customers can opt to lease infrastructure as a service; platform as a service; or security, software and storage as a service.

AWS Simple Storage Service (AWS S3)

AWS offers a wide range of storage services that can be provisioned depending on your project requirements and use case.

S3, is the object storage service provided by AWS. It is probably the most commonly used, go-to storage service for AWS users given the features like extremely high availability, security, and simple connection to other AWS Services. AWS S3 can be used by people with all kinds of use cases like mobile/web applications, big data, machine learning and many more.

Features of AWS S3:

- **Durability:** AWS claims Amazon S3 to have a 99.999999999% of durability (11 9’s). This means the possibility of losing your data stored on S3 is one in a billion.
- **Availability:** AWS ensures that the up-time of AWS S3 is 99.99% for standard access.
  - Note that availability is related to being able to access data and durability is related to losing data altogether.
- **Server-Side-Encryption (SSE):** AWS S3 supports three types of SSE models:
  - **SSE-S3:** AWS S3 manages encryption keys.
  - **SSE-C:** The customer manages encryption keys.

    - **SSE-KMS:** The AWS Key Management Service (KMS) manages the encryption keys.
- **File Size support:** AWS S3 can hold files of size ranging from 0 bytes to 5 terabytes. A 5TB limit on file size should not be a blocker for most of the applications in the world.
- **Infinite storage space:** Theoretically AWS S3 is supposed to have infinite storage space. This makes S3 infinitely scalable for all kinds of use cases.
- **Pay as you use:** The users are charged according to the S3 storage they hold.
- **AWS-S3** is region-specific.