EVOLUTION OF CLOUD COMPUTING

Cloud computing has evolved from the most emerged technologies like grid computing, virtualization, utility computing in distributed computation environment with web based platforms. The concept of Cloud Computing came into existence in the year 1950 with implementation of mainframe computers, accessible via thin/static clients. The cloud computing has evolved from the concepts of grid, utility and SaaS. The development towards cloud computing started in the late 1980s with the concept of grid computing. Grid computing also named as On Demand Computing centers around moving a workload to the area of the required computing assets, which are for the most part remote and are promptly accessible for utilize. A grid is a group of servers where huge task could be separated into smaller tasks which will be keep running in parallel frameworks. Starting here of view, a grid could really be seen as only one virtual server and oblige applications to fit in with the grid programming interfaces. In the 1990s, the idea of virtualization was extended beyond virtual servers to to higher levels of abstraction. Storage and network resources, and subsequently the virtual application, which has no specific underlying infrastructure were applied in virtual platform. Utility Computing is a concept established by John McCarthy, who predicted already in the late 1960s that "computation may someday be organized as a public utility". In utility computing, clusters are presented as virtual platforms for computing with a metered business model. Characteristics of clusters are that the computers being linked to each other are normally distributed locally, and have the same kind of hardware and operating system. Therefore cluster work stations are connected together and can possibly be used as a super computer. The utility approach also known as payper-use or metered services increasingly common in enterprise computing and is sometimes used for the consumer market for Internet service, file sharing, web site access and other applications. More recently software as an service (SaaS) has raised the level of virtualization to the application, with a plan of action of charging not by the resources devoured but rather by the estimation of the application to supporters. In 2001, IBM began autonomic computing likewise called selfrevision in which computers can naturally rectify themselves without human mediation. For example, consider a network of computers running a set of programs and when there is a hardware failure on one of the computers on the network, the programs running on that computer are transferred to other computers in the network. The following section discusses the great features exist with cloud computing which made an end user to use this computing concept easily.

Overview Of Cloud Computing

Introduction

Cloud Computing provides us means of accessing the applications as utilities over the Internet. It allows us to create, configure, and customize the applications online.

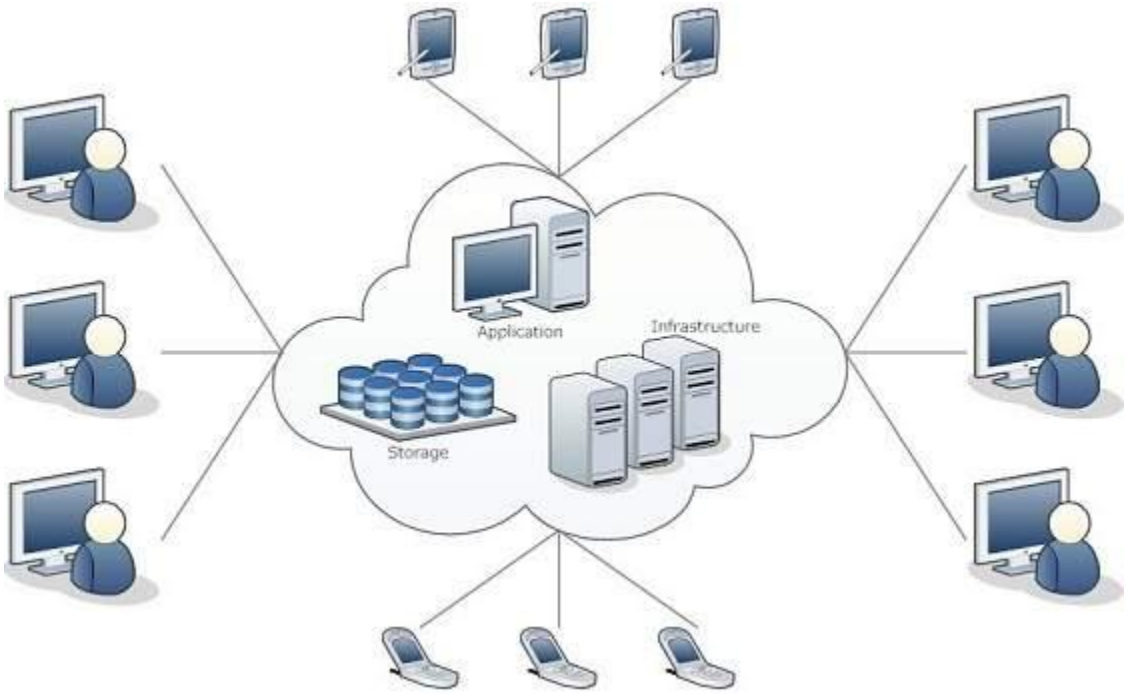
What is Cloud?

The term **Cloud** refers to a **Network** or **Internet.** In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN.

Applications such as e-mail, web conferencing, customer relationship management (CRM) execute on cloud.

What is Cloud Computing?

Cloud Computing refers to **manipulating, configuring,** and **accessing** the hardware and software resources remotely. It offers online data storage, infrastructure, and application.



Cloud computing offers **platform independency,** as the software is not required to be installed locally on the PC. Hence, the Cloud Computing is making our business applications **mobile** and **collaborative.**

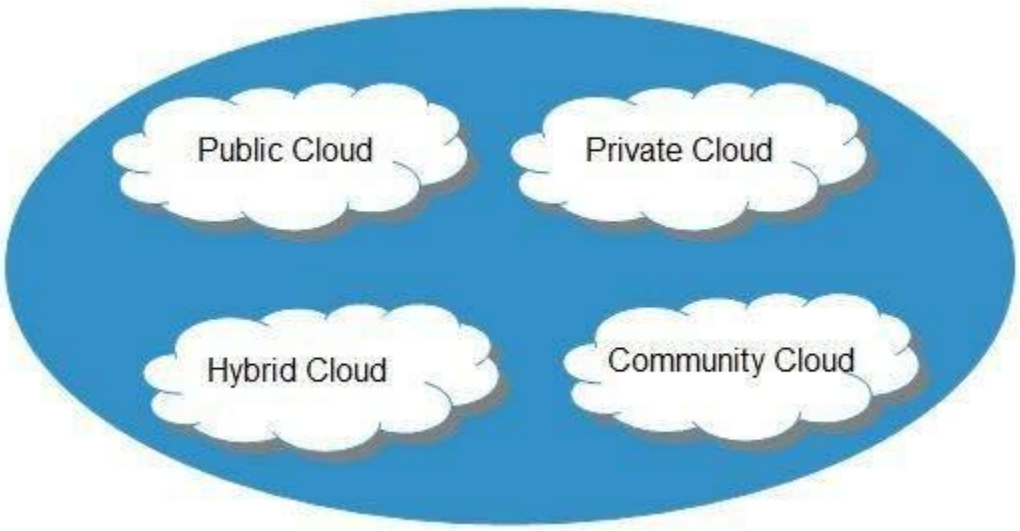
Basic Concepts

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

- Deployment Models
- Service Models

Deployment Models

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid, and Community.



PUBLIC CLOUD

The **public cloud** allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness.

PRIVATE CLOUD

The **private cloud** allows systems and services to be accessible within an organization. It is more secured because of its private nature.

COMMUNITY CLOUD

The **community cloud** allows systems and services to be accessible by a group of organizations.

HYBRID CLOUD

The **hybrid cloud** is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

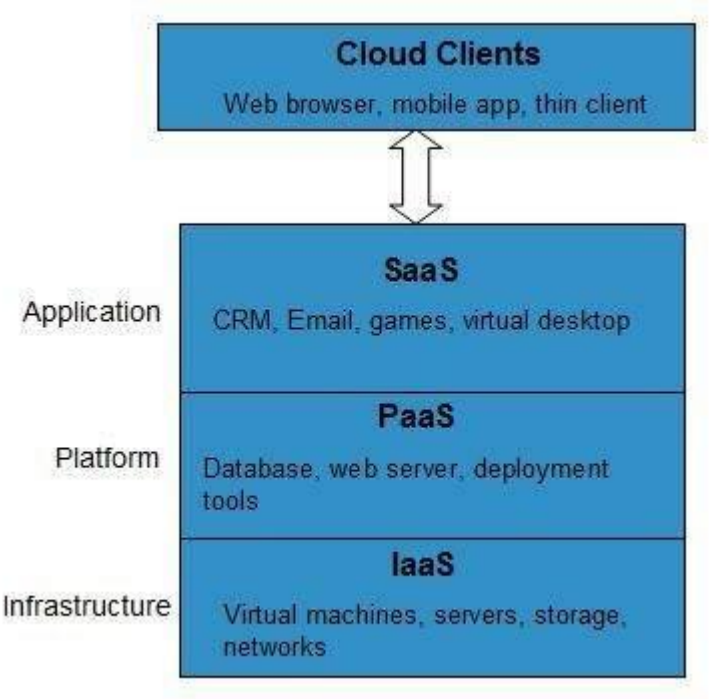
Service Models

Cloud computing is based on service models. These are categorized into three basic service models which are -

- Infrastructure-as–a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Anything-as-a-Service (XaaS) is yet another service model, which includes Network-as-a-Service, Business-as-a-Service, Identity-as-a-Service, Database-as-a-Service or Strategy-as-a-Service.

The **Infrastructure-as-a-Service (IaaS)** is the most basic level of service. Each of the service models inherit the security and management mechanism from the underlying model, as shown in the following diagram:



INFRASTRUCTURE-AS-A-SERVICE (IAAS)

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

PLATFORM-AS-A-SERVICE (PAAS)

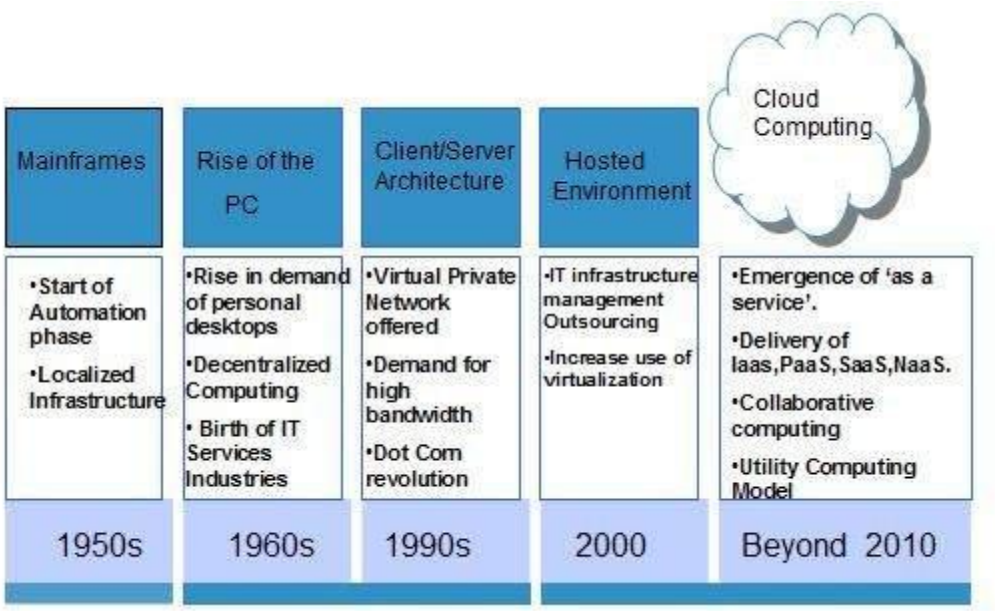
PaaS provides the runtime environment for applications, development and deployment tools, etc.

SOFTWARE-AS-A-SERVICE (SAAS)

SaaS model allows to use software applications as a service to end-users.

History of Cloud Computing

The concept of **Cloud Computing** came into existence in the year 1950 with implementation of mainframe computers, accessible via **thin/static clients.**Since then, cloud computing has been evolved from static clients to dynamic ones and from software to services. The following diagram explains the evolution of cloud computing:

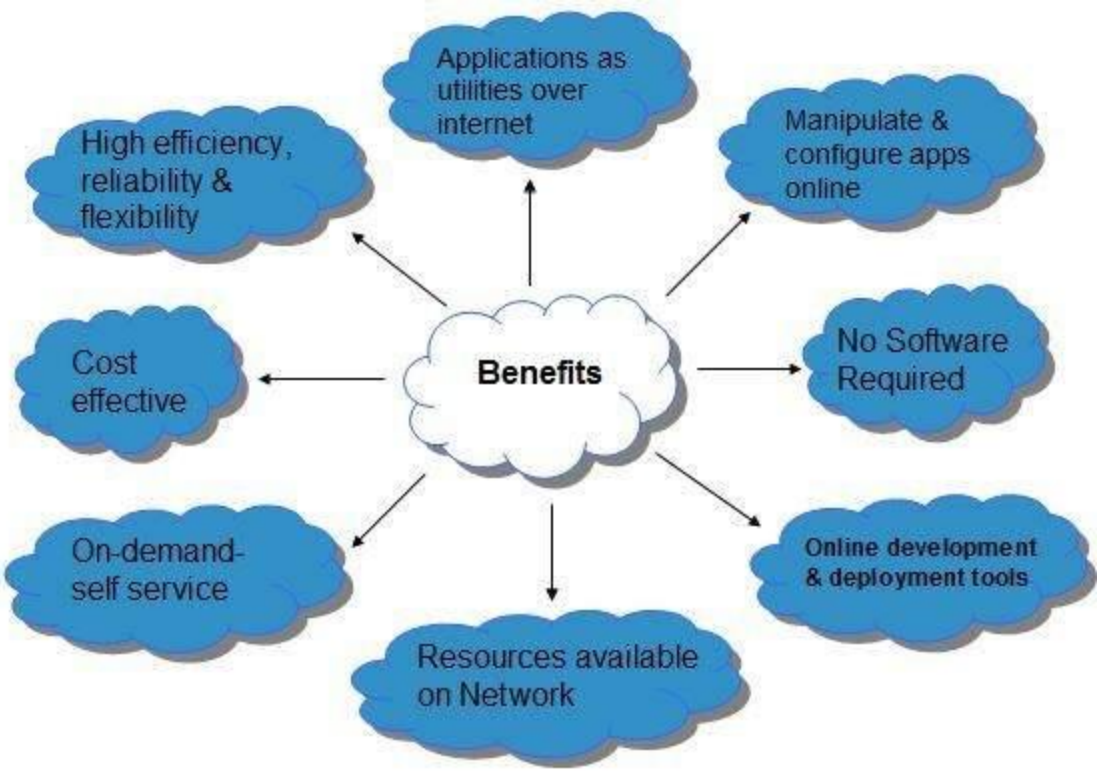


Benefits

Cloud Computing has numerous advantages. Some of them are listed below -

- One can access applications as utilities, over the Internet.
- One can manipulate and configure the applications online at any time.
- It does not require to install a software to access or manipulate cloud application.
- Cloud Computing offers online development and deployment tools, programming runtime environment through **PaaS model.**
- Cloud resources are available over the network in a manner that provide platform independent access to any type of clients.

- Cloud Computing offers **on-demand self-service.** The resources can be used without interaction with cloud service provider.
- Cloud Computing is highly cost effective because it operates at high efficiency with optimum utilization. It just requires an Internet connection
- Cloud Computing offers load balancing that makes it more reliable.



Risks related to Cloud Computing

Although cloud Computing is a promising innovation with various benefits in the world of computing, it comes with risks. Some of them are discussed below:

Security and Privacy

It is the biggest concern about cloud computing. Since data management and infrastructure management in cloud is provided by third-party, it is always a risk to handover the sensitive information to cloud service providers.

Although the cloud computing vendors ensure highly secured password protected accounts, any sign of security breach may result in loss of customers and businesses.

Lock In

It is very difficult for the customers to switch from one **Cloud Service Provider (CSP)** to another. It results in dependency on a particular CSP for service.

Isolation Failure

This risk involves the failure of isolation mechanism that separates storage, memory, and routing between the different tenants.

Management Interface Compromise

In case of public cloud provider, the customer management interfaces are accessible through the Internet.

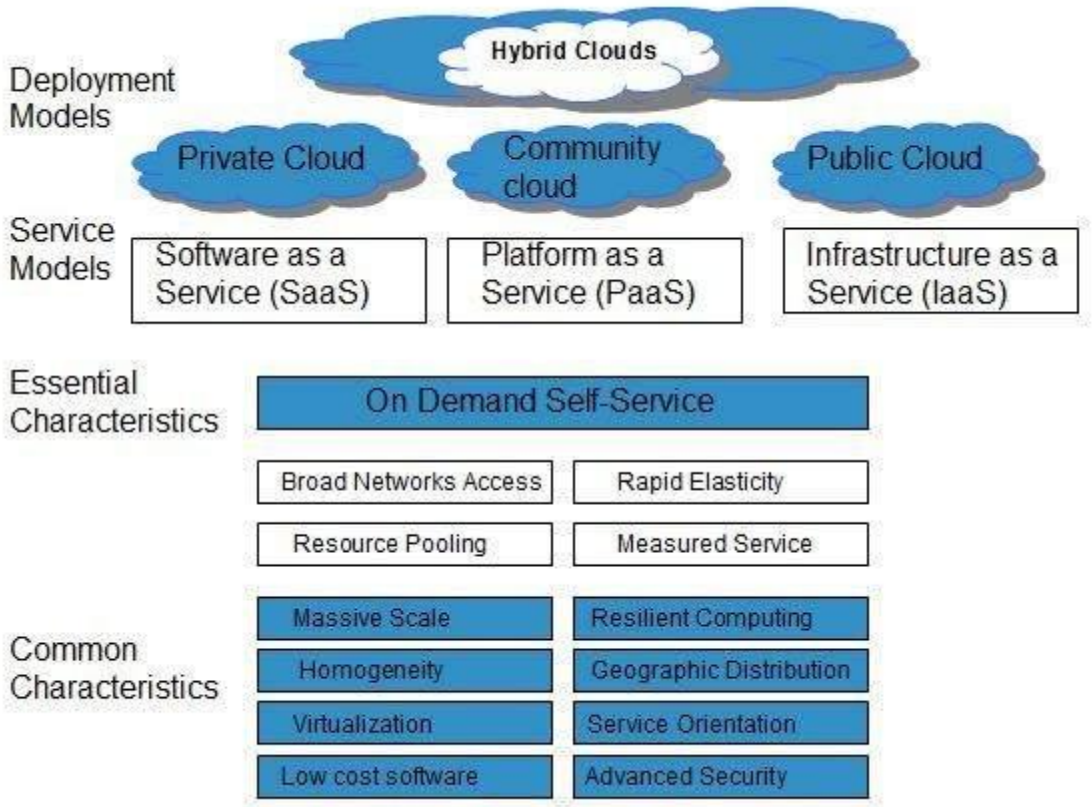
Insecure or Incomplete Data Deletion

It is possible that the data requested for deletion may not get deleted. It happens because either of the following reasons

- Extra copies of data are stored but are not available at the time of deletion
- Disk that stores data of multiple tenants is destroyed.

Characteristics of Cloud Computing

There are four key characteristics of cloud computing. They are shown in the following diagram:



On Demand Self Service

Cloud Computing allows the users to use web services and resources on demand. One can logon to a website at any time and use them.

Broad Network Access

Since cloud computing is completely web based, it can be accessed from anywhere and at any time.

Resource Pooling

Cloud computing allows multiple tenants to share a pool of resources. One can share single physical instance of hardware, database and basic infrastructure.

Rapid Elasticity

It is very easy to scale the resources vertically or horizontally at any time. Scaling of resources means the ability of resources to deal with increasing or decreasing demand.

The resources being used by customers at any given point of time are automatically monitored.

Measured Service

In this service cloud provider controls and monitors all the aspects of cloud service. Resource optimization, billing, and capacity planning etc. depend on it.

Service And Deployment Models

Categories of service model

The service models are categorized into three basic models:

1) Software-as-a-Service (SaaS)
2) Platform-as-a-Service (PaaS)
3) Infrastructure-as-a-Service (IaaS)

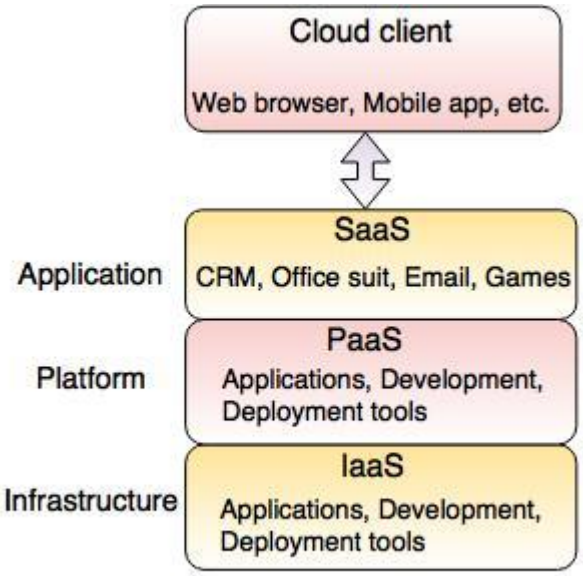


Fig. - Categories of Cloud Computing

1) Software-as-a-Service (SaaS)

- SaaS is known as **'On-Demand Software'.**
- It is a software distribution model. In this model, the applications are hosted by a cloud service provider and publicized to the customers over internet.
- In SaaS, associated data and software are hosted centrally on the cloud server.
- User can access SaaS by using a thin client through a web browser.
- CRM, Office Suite, Email, games, etc. are the software applications which are provided as a service through Internet.
- The companies like Google, Microsoft provide their applications as a service to the end users.

Advantages of SaaS

- SaaS is easy to buy because the pricing of SaaS is based on monthly or annual fee and it allows the organizations to access business functionalities at a small cost, which is less than licensed applications.

- SaaS needed less hardware, because the software is hosted remotely, hence organizations do not need to invest in additional hardware.
- Less maintenance cost is required for SaaS and do not require special software or hardware versions.

Disadvantages of SaaS

- SaaS applications are totally dependent on Internet connection. They are not usable without Internet connection.
- It is difficult to switch amongst the SaaS vendors.

2) Platform-as-a-Service (PaaS)

- PaaS is a programming platform for developers. This platform is generated for the programmers to create, test, run and manage the applications.
- A developer can easily write the application and deploy it directly into PaaS layer.
- PaaS gives the runtime environment for application development and deployment tools.
- Google Apps Engine(GAE), Windows Azure, SalesForce.com are the examples of PaaS.

Advantages of PaaS

- PaaS is easier to develop. Developer can concentrate on the development and innovation without worrying about the infrastructure.
- In PaaS, developer only requires a PC and an Internet connection to start building applications.

Disadvantages of PaaS

- One developer can write the applications as per the platform provided by PaaS vendor hence the moving the application to another PaaS vendor is a problem.

3) Infrastructure-as-a-Service (IaaS)

- IaaS is a way to deliver a cloud computing infrastructure like server, storage, network and operating system.
- The customers can access these resources over cloud computing platform i.e Internet as an on-demand service.
- In IaaS, you buy complete resources rather than purchasing server, software, datacenter space or network equipment.
- IaaS was earlier called as Hardware as a Service(HaaS). It is a Cloud computing platform based model.
- HaaS differs from IaaS in the way that users have the bare hardware on which they can deploy their own infrastructure using most appropriate software.

Advantages of IaaS

- In IaaS, user can dynamically choose a CPU, memory storage configuration according to need.
- Users can easily access the vast computing power available on IaaS Cloud platform.

Disadvantages of IaaS

- IaaS cloud computing platform model is dependent on availability of Internet and virtualization services.
-

Cloud Computing Deployment Models

The Basics of Cloud Computing

Cloud computing — the availability of information resources, such as data repository and computer capacity, on request — provides significant business benefits to companies of different sizes and specifics. However, to make the most use of this computing type, that is, to reduce capital spending, control business-related expenses and improve overall process efficiency, a company should opt for appropriate deployment models in cloud computing.

A cloud deployment model is a "configuration" of certain cloud environment parameters such as the storage size, accessibility and proprietorship. To choose the most suitable one for you, SaM Solutions recommends companies to make a choice based on their computing, networking, storage requirements, TCO expectations and business goals, as well as available resources.

There are four main cloud deployment models that differ significantly and for which most of the companies opt: a public, private, hybrid and a community one. There are also web-based organization systems that are not so widespread, such as virtual private, inter-cloud and others.

Public Cloud

The name speaks for itself, as public clouds are available to the general public and data are created and stored on third-party servers. As server infrastructure belongs to service providers that manage them and administer pool resources, the need for user companies to buy and maintain their own hardware is eliminated. Provider companies offer resources as a service on a free of charge or pay-per-use basis via the Internet connection. Users can scale them when required.

At the same time, relying on a third party in running their infrastructure deprives users of knowing where their information is kept and who has access to it. Often enough, public clouds experience outages and malfunction, as in the case of the Salesforce CRM disruption in 2016 that caused a 10-hour storage collapse.

The pros of a public cloud are:

- Unsophisticated setup and use
- Easy access to data
- Flexibility to add and reduce capacity
- Cost-effectiveness
- Continuous operation time
- 24/7 upkeep

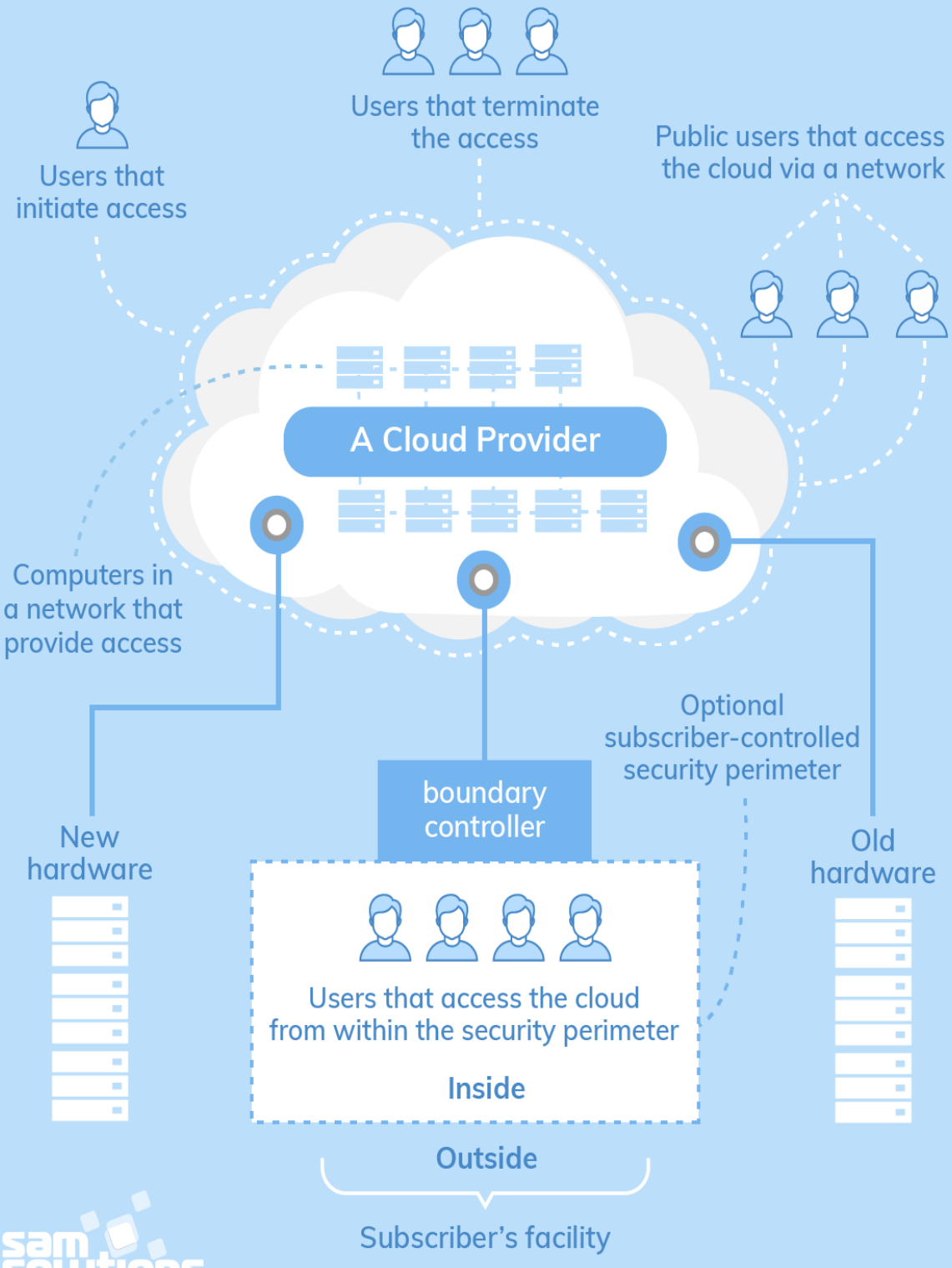
- Scalability
- Eliminated need for software

The cons of a public model:

- Data security and privacy
- Compromised reliability
- The lack of individual approach

The public cloud deployment model is the first choice of businesses that operate within the industries with low privacy concerns. When it comes to popular cloud deployment models, examples are Amazon Elastic Compute, Google AppEngine, IBM's Blue, Microsoft Azure, Salesforce Heroku and others.

Public Cloud



sam solutions

Private Cloud

There is little to no difference between public and private clouds from the technical point of view, as their designs are very similar. However, unlike in the public one, only one specific company owns a private cloud, which is why it is also called internal or corporate. Because these data center architectures reside within the firewall, they provide enhanced security. Even though one organization runs its workloads on a private basis, a third party can also manage it, and the server can be hosted externally or on premises of the user company.

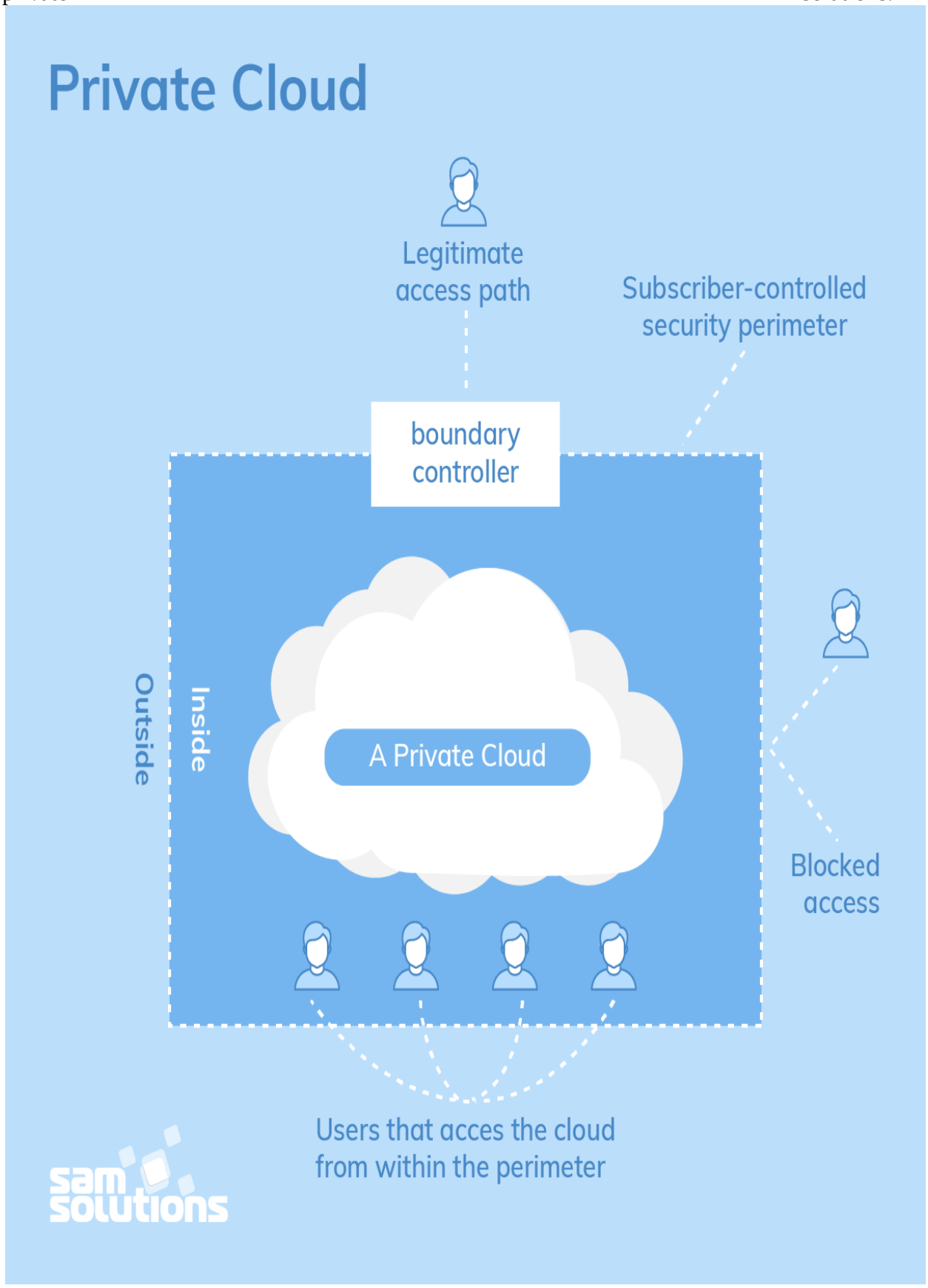
Only a clearly defined scope of persons have access to the information kept in a private repository, preventing the general public from using it. In light of numerous breaches, a growing number of large corporations decided on a closed private type as it is expected to be less risky.

The advantages of a private model:

- Individual development
- Storage and network components are customizable
- High control over the corporate information
- High security, privacy and reliability

The major disadvantage of the private cloud deployment model is its cost intensiveness, as it entails considerable expenses on hardware, software and staff training. That is why this secure flexible computing deployment model is not a choice of small to medium companies. Also, it is especially suitable for companies that seek to safeguard their mission-critical operations or for businesses with changing requirements.

Multiple service providers – including Amazon, IBM, Cisco, Dell and Red Hat – also build private solutions.



Community Cloud

A community cloud deployment model resembles a private one to a large extent; the only difference is the set of users. While a private type implies that only one company owns the server, in the case of a community one, several organizations with similar backgrounds share the infrastructure and related resources.

As the organizations have uniform security, privacy and performance requirements, this multi-tenant data center architecture helps companies achieve their business-specific objectives. That is why a community model is particularly suited for organizations that work on joint projects. In that case, a centralized cloud facilitates project development, management and implementation. Also, the costs are shared across all users.

The strengths of a community computing type include the following:

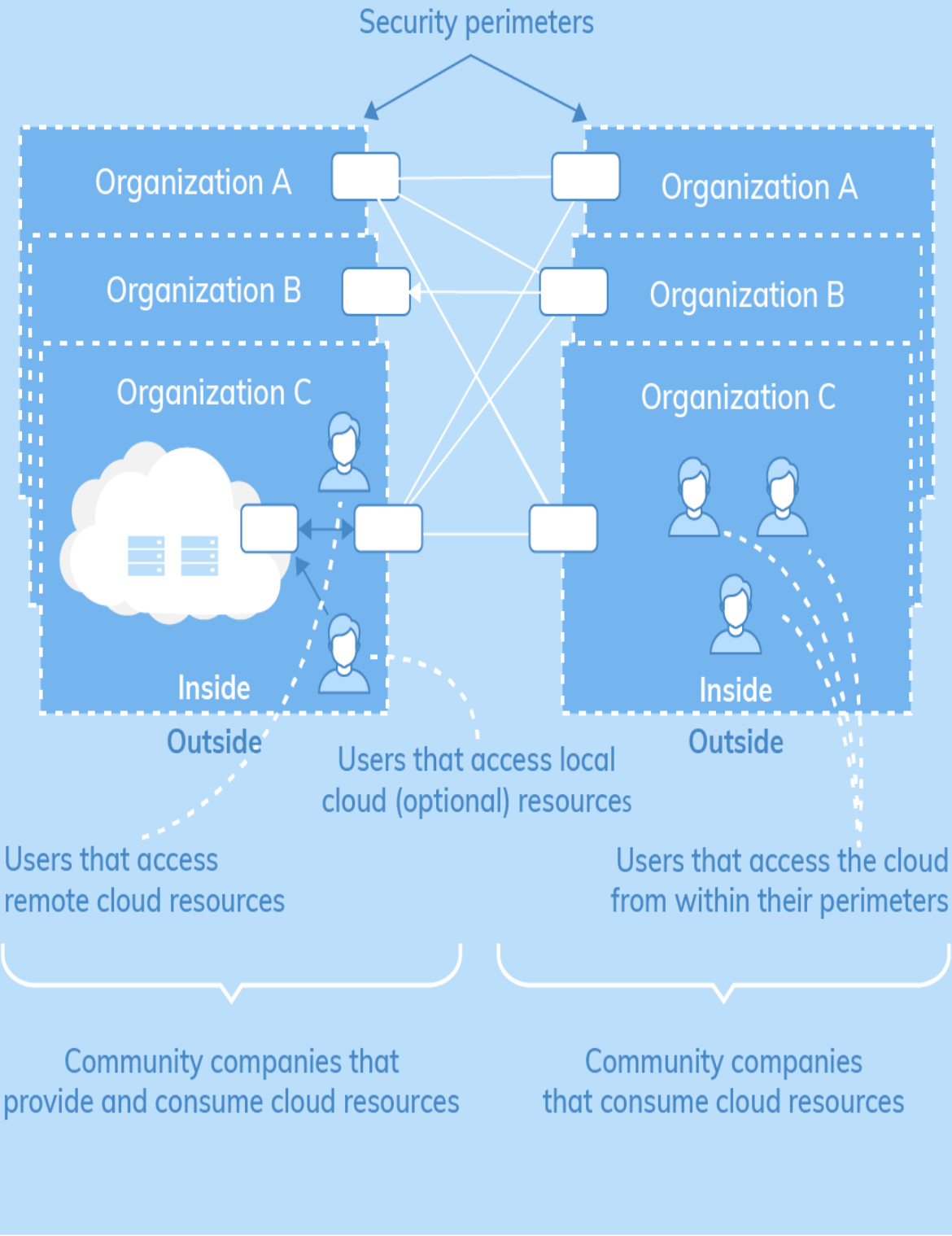
- Cost reduction
- Improved security, privacy and reliability
- Ease of data sharing and collaboration

The shortcomings are:

- Higher cost than that of a public one
- Sharing of fixed storage and bandwidth capacity
- It is not widespread so far

Companies can decide on community solutions that Google, Red Hat, IBM, Microsoft or others provide.

Community Cloud



Hybrid Cloud

As it is usually the case with any hybrid phenomenon, a hybrid cloud encompasses the best features of the above-mentioned cloud computing deployment models – a public, private and community ones. It allows companies to mix and match the facets of all three types that best suit their requirements.

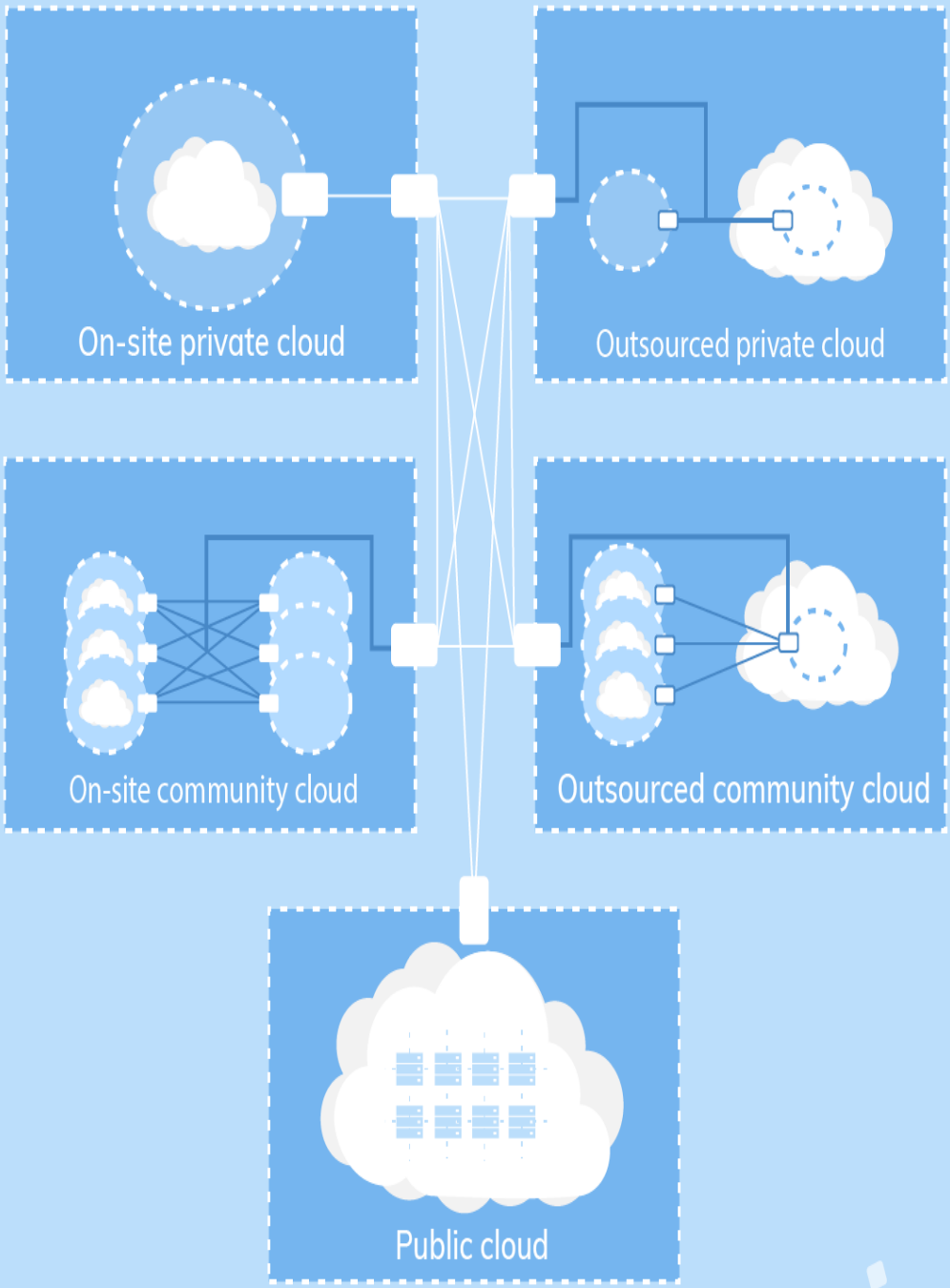
As an example, a company can balance its load by locating mission-critical workloads on a secure private cloud and deploying less sensitive ones to a public one. It not only safeguards and controls strategically important assets but does so in the most cost- and resource-effective way possible for each specific case. Also, this approach facilitates data and application portability.

The benefits of a hybrid model are:

- Improved security and privacy
- Enhanced scalability and flexibility
- Reasonable price

However, the hybrid cloud deployment model only makes sense if companies can split their data into mission-critical and non-sensitive.

Hybrid Cloud



sam solutions

Types of Cloud Deployment Models: The Comparison

To facilitate the choice of the appropriate deployment models of cloud computing by opting for the ones with the most business-critical features, we have created a comparative table that provides an overall view of the specificity of each type.

The comparative analysis of the best cloud deployment models

	Public	**Private**	**Community**	**Hybrid**
Ease of setup and use	Easy	Requires IT proficiency	Requires IT proficiency	Requires IT proficiency
Data security and privacy	Low	High	Comparatively high	High
Data control	Little to none	High	Comparatively high	Comparatively high
Reliability	Vulnerable	High	Comparatively high	High
Scalability and flexibility	High	High	Fixed capacity	High
Cost-effectiveness	The cheapest one	Cost-intensive, the most expensive one	Cost is shared among community members	Cheaper than a private model but more costly than a public one
Demand for in-house hardware	No	Depends	Depends	Depends

A careful consideration of all business and technical requirements, as well as of each model's peculiarity, is a prerequisite for a successful shift to the cloud. However, it is quite a challenging task, which is why SaM Solutions recommends opting for professional cloud deployment services .

Our extensive expertise allows us to choose the most appropriate model that fits the bill for your company, based on your requirements and expectations, to improve your performance and avoid risks and security issues in the future.

Request consultation with a SaM Solutions specialist

Cloud computing is defined with several deployment models, each of which has specific trade-offs for agencies that are migrating services and operations to cloud-based environments. Because of the different characteristics and trade-offs of the various cloud computing deployment models, it is important the agency IT professionals have a clear understanding of their agency's specific needs as well as how the various systems can help them meet these needs. NIST's official definition for cloud computing outlines four cloud

deployment models: private, community, public, and hybrid. Let's take a look at some of the key differences.

Private Cloud

A private cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises

In general, federal agencies and departments opt for private clouds when sensitive or mission-critical information are involved. The private cloud allows for increased security, reliability, performance, and service. Yet, like other types of clouds, it maintains the ability to scale quickly and only pay for what is used when provided by a third party, making it economical as well.

One example of a private cloud deployment model that has been implemented in the federal government relatively recently was implemented by the Los Alamos National Laboratory, which allows researchers to access and utilize servers on demand.

Community Cloud

The Community Cloud is a type of cloud hosting in which the setup is mutually shared between many organizations that belong to a particular community, i.e. banks and trading firms. It is a multi-tenant setup that is shared among several organizations that belong to a specific group which has similar computing apprehensions. The community members generally share similar privacy, performance and security concerns. The main intention of these communities is to achieve their business-related objectives. A community cloud may be internally managed or it can be managed by a third-party provider. It can be hosted externally or internally. The cost is shared by the specific organizations within the community, hence, community cloud has cost saving capacity. A community cloud is appropriate for organizations and businesses that work on joint ventures, tenders or research that needs a centralized cloud computing ability for managing, building and implementing similar projects.

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns

The community cloud deployment model is ideal and optimized for agencies or independent organizations that have shared concerns, and therefore need access to shared and mutual records and other types of stored information.

Examples might include a community dedicated to compliance considerations or a community focused on security requirements policy.

Public Cloud

The general public provisions the cloud infrastructure for open use. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

The public cloud deployment model have the unique advantage of being significantly more secure than accessing information via the Internet and tend to cost less than private clouds because services are more commoditized.

Research by the 1105 Government Information Group found that federal agencies interested in public clouds are most commonly interested in the following four functions:

- Collaboration
- Social Networking
- CRM
- Storage

One example of a public cloud deployment model based solution is the Treasury Department, which has moved its website Treasury.gov to a public cloud using Amazon's EC2 cloud service to host the site and its applications. The site includes social media attributes, including Facebook, YouTube and Twitter which allows for rapid and effective communication with constituents.

Hybrid Cloud

The cloud infrastructure is a composition of two or more distinct cloud deployment models (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Large portions of agencies that have already switched some processes over to cloud based computing solutions have utilized hybrid cloud options. Few enterprises have the ability to switch over all of their IT services at one time, the hybrid option allows for a mix of on base and cloud options which provide an easier transition.

NASA is one example of a federal agency who is utilizing the Hybrid Cloud Computing deployment model. Its Nebula open-source cloud computing project uses a private cloud for research and development as well as a public cloud to shared datasets with external partners and the public.

The hybrid cloud computing deployment model option has also proven to be the choice option for state and local governments as well, with states like Michigan and Colorado having already declared their cloud computing intentions with plans illustrating hybrid cloud deployment models.

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.

Types of SLA

A service level agreement (SLA) is a contract between a business and its customer outlining the details that the two parties have agreed to in a transaction. The types of SLAs that an organization can use depends on many significant aspects. While some are targeted at individual customer groups, others discuss issues relevant to entire companies. This is

because the needs of one user differ from those of another. Below is a list of the types of SLAs used by businesses today, and how each one is utilized for specific situations:

1. **Customer-based SLA**

   This type of agreement is used for individual customers and comprises all relevant services that a client may need, while leveraging only one contract. It contains details regarding the type and quality of service that has been agreed upon. For example, a telecommunication service includes voice calls, messaging and internet services, but that all exists under a single contract.

2. **Service-based SLA**

   This SLA is a contract that includes one identical type of service for all of its customers. Because the service is limited to one unchanging standard, it is more straightforward and convenient for vendors. For example, using a service-based agreement regarding an IT helpdesk would mean that the same service is valid for all end-users that sign the service-based SLA.

3. **Multi-level SLA**

   This agreement is customized according to the needs of the end-user company. It allows the user to integrate several conditions into the same system to create a more suitable service. It addresses contracts at the following levels:

   a. Corporate level:

      This SLA does not require frequent updates since its issues are typically unchanging. It includes a comprehensive discussion of all the relevant aspects of the agreement, and is applicable to all customers in the end-user organization.

   b. Customer level:

      This contract discusses all service issues that are associated with a specific group of customers. However, it does not take into consideration the type of user services.

      An example of this is when an organization requests that the security level in one of its departments is strengthened. In this situation, the entire company is secured by one security agency but requires that one of its customers in the company is more secure for certain reasons.

   c. Service level:

      In this agreement, all aspects that are attributed to a particular service with regard to a customer group are included.

Cloud SLA lifecycle

The Cloud SLA lifecycle is an important part of the provision of Cloud services. There is a tight correlation between the phases of the Cloud service lifecycle (Acquisition, Operation, Termination) and the 7 phases of the Cloud SLA one.

Cloud service lifecycle: Acquisition

A prospective cloud customer can use service offerings published by the cloud service provider to check whether it meets her/his requirements, for example, security, personal data protection, performance etc., and see how one offering compares with another in the market. Why is it important? This phase is crucial for establishing an SLA between the cloud customer and the cloud service provider.

Assessment	Any relationship starts with pre-assessing what one would like, why, when and with whom (for instance one or more CSPs), so does the first Cloud SLA lifecycle phase, Assessment. This includes for instance doing market intelligence, checking specific needs, offerings, CSPs, performance of CSPs and setting up a business case...
Preparation	This second Cloud SLA lifecycle phase, includes for instance, the first contact and conversation with possible CSPs, further assessment, pre-evaluation and fine-tuning goals and assumptions...
Negotiation & Contracting	This phase can include preparing for negotiation and the actual negotiation and deal making with one or more CSPs, including sharing concerns, discuss in-scope and out-of-scope (cloud) services, debating about trade-offs and finding common grounds, reaching agreement, double-checking needs, goals and assumptions, and of course documenting the contractual arrangements, and signing thereof...

Cloud service lifecycle: Operation

This phase determines whether a cloud service meets the committed service level objective (SLO) during the provisioning of the cloud service. This might imply that cloud service providers taking corrective actions to avoid SLA violations. Why is it important? SLAs can be used to monitor the cloud service provider in order to assess the correct fulfilment of the cloud service, or detect potential violations in which case remediation may take place.

Execution & Operation	This phase includes the actual start of setting up the cloud services, populating the respective cloud service with relevant data, on boarding and training users, setting up communication channels and further operational activities while using the respective cloud services...
Updates & Amendments	This phase includes updated or otherwise amended needs, goals and assumptions by the Cloud Service Customer during the term of the ongoing cloud services arrangements, as well as improved or added cloud services by the CSP there under. It also includes optimisation of the respective cloud services by CSP as per (contractual or other) non-compliance, breaches and other incidents during that term...
Escalation	This phase deals with contractual or other) non-compliance, breaches and other incidents during the term of the ongoing cloud services arrangements that have resulted in a dispute that needs escalation, (perhaps even litigation as a last resort), negotiation and resolution, either by parties themselves or by arbitration, court or otherwise...

Cloud service lifecycle: Termination

Why is it important? You should already think about termination in phase 1, as an SLA can be used to arrange the conditions under which the Cloud customer's data (including but not limited to for instance Personal Identifiable Information or PII) will be exported and returned to the cloud customer, and not retained by the cloud service provider (to the extent mandatorily possible).

Termination & Consequences of Termination	This phase deals with the end of the relationship between CSP and CSC, including the end of the legal relationship even though the latter will generally continue for several years after any termination as per mandatory laws and legislation. This last phase for instance includes the assessment of alternatives, settlement and termination arrangements, cloud services transition projects and services, data export, customer and (end)use care and diligence, and adequate data deletion...

SLA Management System

The SLA monitor mechanism is used to specifically observe the runtime performance of cloud services to ensure that they are fulfilling the contractual QoS requirements published in SLAs (Figure 1). The data collected by the SLA monitor is processed by an SLA management system to be aggregated into SLA reporting metrics. This system can proactively repair or failover cloud services when exception conditions occur, such as when the SLA monitor reports a cloud service as "down."

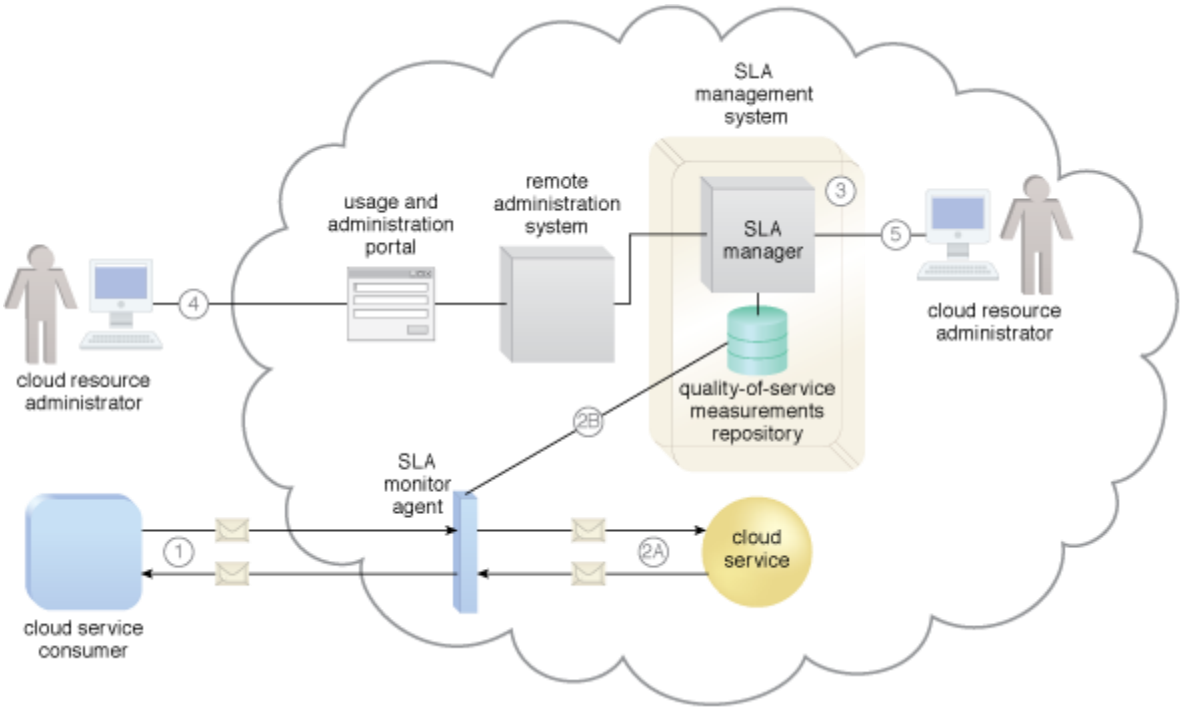


Figure 1 – The SLA monitor polls the cloud service by sending over polling request messages (MREQ1 to MREQN). The monitor receives polling response messages (M to M) that report that the service was "up" at each polling cycle (1a). The SLA monitor stores the "up" time—time period of all polling cycles 1 to N—in the log database (1b). The SLA monitor polls the cloud service that sends polling request messages (M to M). Polling response messages are not received (2a). The response messages continue to time out, so the SLA monitor stores the "down" time—time period of all polling cycles N+1 to N+M—in the log database (2b). The SLA monitor sends a polling request message (M) and receives the polling response message (M) (3a). The SLA monitor stores the "up" time in the log database (3b).

Virtualization in Cloud Computing

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

In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

What is the concept behind the Virtualization?

Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

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

Types of Virtualization:

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

1) Hardware Virtualization:

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

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

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

Usage:

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

2) Operating System Virtualization:

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

Usage:

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

3) Server Virtualization:

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

Usage:

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

4) Storage Virtualization:

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

Storage virtualization is also implemented by using software applications.

Usage:

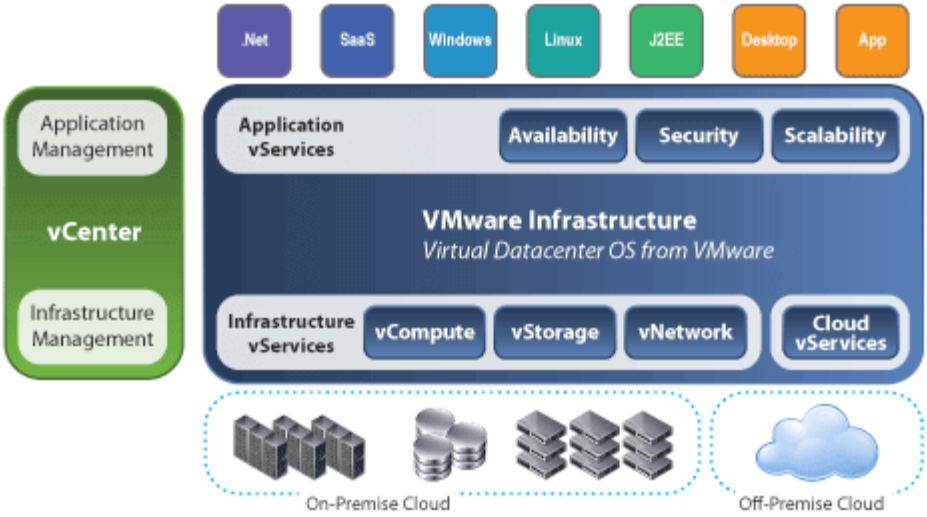
Storage virtualization is mainly done for back-up and recovery purposes.

How does virtualization work in cloud computing?

Virtualization plays a very important role in the cloud computing technology, normally in the cloud computing, users share the data present in the clouds like application etc, but actually with the help of virtualization users shares the Infrastructure.

The **main usage of Virtualization Technology** is to provide the applications with the standard versions to their cloud users, suppose if the next version of that application is released, then cloud provider has to provide the latest version to their cloud users and practically it is possible because it is more expensive.

To overcome this problem we use basically virtualization technology, By using virtualization, all severs and the software application which are required by other cloud providers are maintained by the third party people, and the cloud providers has to pay the money on monthly or annual basis.



Mainly Virtualization means, running multiple operating systems on a single machine but sharing all the hardware resources. And it helps us to provide the pool of IT resources so that we can share these IT resources in order get benefits in the business.

Virtualization is the creation of virtual servers, infrastructures, devices and computing resources. A great example of how it works in your daily life is the separation of your hard drive into different parts. While you may have only one hard drive, your system sees it as two, three or more different and separate segments. Similarly, this technology has been used for a long time. It started as the ability to run multiple operating systems on one hardware set and now it a vital part of testing and cloud-based computing.

Virtualization vs. Cloud Computing

Virtualization changes the hardware-software relations and is one of the foundational elements of cloud computing technology that helps utilize cloud computing capabilities to the full. Unlike virtualization, cloud computing refers to the service that results from that change. It describes the delivery of shared computing resources, SaaS and on-demand services through the Internet. Most of the confusion occurs because virtualization and cloud computing work together to provide different types of services, as is the case with private clouds.

The cloud often includes virtualization products as a part of their service package. The difference is that a true cloud provides the self-service feature, elasticity, automated management, scalability and pay-as-you-go service that is not inherent to the technology.

The Basics

A technology called the Virtual Machine Monitor — also called virtual manager– encapsulates the very basics of virtualization in cloud computing. It is used to separate the physical hardware from its emulated parts. This often includes the CPU's memory, I/O and network traffic. A secondary operating system that is usually interacting with the hardware is now a software emulation of that hardware, and often the guest operating system has no idea

it's on the virtualized hardware. Despite the fact that performance of the virtual system is not equal to the functioning of the "true hardware" operating system, the technology still works because most secondary OSs and applications don't need the full use of the underlying hardware. This allows for greater flexibility, control and isolation by removing the dependency on a given hardware platform.

The layer of software that enables this abstraction is called "hypervisor". A study in the *International Journal of Scientific & Technology Research* defines it as "a software layer that can monitor and virtualize the resources of a host machine conferring to the user requirements." The most common hypervisor is referred to as Type 1. By talking to the hardware directly, it virtualizes the hardware platform that makes it available to be used by virtual machines. There's also a Type 2 hypervisor, which requires an operating system. Most often, you can find it being used in software testing and laboratory research.

Types of Virtualization in Cloud Computing

Here are six methodologies to look at when talking about virtualization techniques in cloud computing:

Network Virtualization

Network virtualization in cloud computing is a method of combining the available resources in a network by splitting up the available bandwidth into different channels, each being separate and distinguished. They can be either assigned to a particular server or device or stay unassigned completely — all in real time. The idea is that the technology disguises the true complexity of the network by separating it into parts that are easy to manage, much like your segmented hard drive makes it easier for you to manage files.

Storage Virtualizing

Using this technique gives the user an ability to pool the hardware storage space from several interconnected storage devices into a simulated single storage device that is managed from one single command console. This storage technique is often used in storage area networks. Storage manipulation in the cloud is mostly used for backup, archiving, and recovering of data by hiding the real and physical complex storage architecture. Administrators can implement it with software applications or by employing hardware and software hybrid appliances.

Server Virtualization

This technique is the masking of server resources. It simulates physical servers by changing their identity, numbers, processors and operating systems. This spares the user from continuously managing complex server resources. It also makes a lot of resources available for sharing and utilizing, while maintaining the capacity to expand them when needed.

Data Virtualization

This kind of cloud computing virtualization technique is abstracting the technical details usually used in data management, such as location, performance or format, in favor of broader access and more resiliency that are directly related to business needs.

Desktop Virtualizing

As compared to other types of virtualization in cloud computing, this model enables you to emulate a workstation load, rather than a server. This allows the user to access the desktop remotely. Since the workstation is essentially running in a data center server, access to it can be both more secure and portable.

Application Virtualization

Software virtualization in cloud computing abstracts the application layer, separating it from the operating system. This way the application can run in an encapsulated form without being dependant upon the operating system underneath. In addition to providing a level of isolation, an application created for one OS can run on a completely different operating system.

Conclusion

If a company decides on whether or not to apply the technology in a company's IT landscape, we recommend making an in-depth analysis of its specific needs and capabilities, which is better handled by specialists who can address costs, scalability requirements and security needs and implement continuous development.

But also remember that all of these techniques and services are not omnipotent or all-inclusive solutions. Like any other technology, tool or service a business adopts, things can always change.

In this article, we covered what is virtualization in cloud computing, types of hypervisors, different techniques and how to understand that you really need this system in your IT infrastructure. It can be viewed as part of an overall trend in enterprise IT that includes autonomic and utility computing. Usually, it is done by centralizing the administrative parts while improving scalability and workloads, and many businesses derive a lot of benefits from it.

Benefits of Virtualization in a Cloud Environment

1. Protection from System Failures

Technology is always at the risk of crashing down at the wrong time. Businesses can tolerate a few glitches, but if your developer is working on an important application that needs to be finished immediately, the last thing you could wish for is a system crash.

To counter this risk, virtualization lets you open the same work on another device. Store all your backup data through virtualization on cloud services or virtual networks and get easy access to it from any device. Apart from that, there are usually two servers working side-by-side keeping all your data accessible. If one faces any problem, the other is always available to avoid any interruption.

2. Hassle-free Transfer of Data

You can easily transfer data from a physical storage to a virtual server, and vice versa. Administrators don't have to waste time digging out hard drives to find data. With a dedicated server and storage, it's quite easy to locate the required files and transfer them within no time.

You'll realize virtualizations actual worth when you'll have to transfer data over a long-distance. You also have the choice of getting a virtual disk space. If you don't need much space, you can opt for a thin-provisioned virtual disk.

3. Firewall and Security

Security is a major aspect IT professionals have to focus on. However, with virtual firewalls, access to your data is restricted at much lower costs as compared to traditional methods. Through virtualization, you get protected by a virtual switch that protects all your data and applications from harmful malware, viruses, and other cyber threats.

You are allotted the firewall feature for network virtualization to create segments within the system. Server virtualization storage on cloud services will save you from the risks of having your data get lost or corrupted. Cloud services are also encrypted with high-end protocols that protect your data from other various threats.

So it's a good idea to virtualize all your storage and then create a backup on a server that you can store on cloud services. However, in order to ensure that you do this correctly, it's preferable to first go through a cloud computing online course, to avoid making any errors.

4. Smoother IT Operations

Virtual networks help IT professionals become efficient and agile at work. These networks are easy to operate and process faster, reducing the effort and time required to work on them. Before virtual networks were introduced in the digital world, it would take days and weeks for technical workers to maintain and install devices and software on physical servers.

Apart from the operations, visualization has also benefited IT support teams in solving technical problems in physical systems. As all the data is available on a virtual server, technicians don't have to waste time recovering it from crashed or corrupted devices. Learn all the skills behind virtualization with cloud training online, and become a successful technician.

5. Cost-Effective Strategy

Virtualization is a great way to reduce operational costs. With all the data stored on virtual servers or clouds, there's hardly a need for physical systems or hardware, thus allowing businesses to witness a vast reduction in wastage, electricity bills, and maintenance costs. 70% of senior executives have supported virtualization by calling it efficient and cost saving.

Virtualization also helps companies save a significant amount of space which can be utilized to increase operations of a profitable department. This cost-effective strategy is both a profitability and productivity booster!

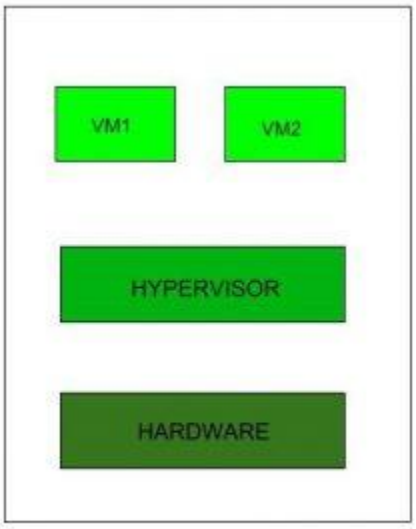
The above mentioned benefits are perfect to convince any IT expert to stop using traditional methods and switch to virtualization. With top-notch security protocols, reduction in costs and better operations you can boost your performance and help grab the next flight towards a prosperous future. The best way to do that and excel in operating virtual servers is to obtain a recognized cloud certification.

Hypervisor

Hypervisor is a form of virtualization software used in Cloud hosting to divide and allocate the resources on various pieces of hardware.The program which provide partitioning, isolation or abstraction is called virtualization hypervisor. Hypervisor is a hardware virtualization technique that allows multiple guest operating systems (OS) to run on a single host system at the same time. A hypervisor is sometimes also called a virtual machine manager(VMM).

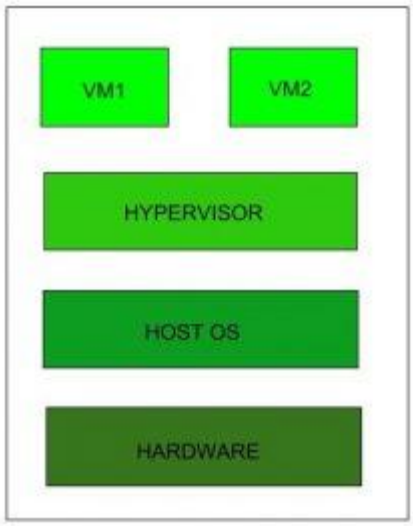
Types of Hypervisor –

TYPE-1 Hypervisor:
Hypervisor runs directly on underlying host system.It is also known as "Native Hypervisor" or "Bare metal hypervisor".It dose not require any base server operating system.It has direct access to hardware resources.Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer and Microsoft Hyper-V hypervisor.



TYPE1 HYPERVISOR

TYPE-2 Hypervisor:
A Host operating system runs on undrlying host system.It is also known as 'Hosted Hypervisor".Basically a software installed on an operating system.Hypervisor asks operating system to make hardware calls.Example of Type 2 hypervisor include VMware Player or Parallels Desktop. Hosted hypervisors are often found on endpoints like PCs.



TYPE 2 HYPERVISOR

Choosing the right hypervisor

Type 1 hypervisors offer much better performance than Type 2 ones because there's no middle layer, making them the logical choice for mission-critical applications and workloads. But that's not to say that hosted hypervisors don't have their place – they're much simpler to set up, so they're a good bet if, say, you need to deploy a test environment quickly.One of the best ways to determine which hypervisor meets your needs is to compare their performance metrics. These include CPU overhead, amount of maximum host and guest memory, and support for virtual processors.The following factors should be examined before choosing a suitable hypervisor:

1. Understand your needs: The company and its applications are the reason for the data center (and your job). Besides your company's needs, you (and your co-workers in IT) also have your own needs.Needs for a virtualization hypervisor are:

a.Flexibility
b.Scalability
c.Usability
d.Availability
e.Reliability
f.Efficiency
g. Reliable support

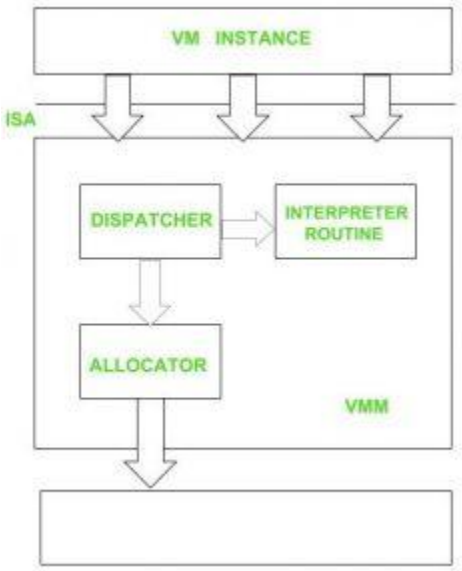
2. The cost of a hypervisor: For many buyers, the toughest part of choosing a hypervisor is striking the right balance between cost and functionality. While a number of entry-level solutions are free, or practically free, the prices at the opposite end of the market can be staggering. Licensing frameworks also vary, so it's important to be aware of exactly what you're getting for your money.

3. Virtual machine performance: Virtual systems should meet or exceed the performance of their physical counterparts, at least in relation to the applications within each server. Everything beyond meeting this benchmark is profit.

4. Ecosystem: It's tempting to overlook the role of a hypervisor's ecosystem – that is, the availability of documentation, support, training, third-party developers and consultancies, and so on – in determining whether or not a solution is cost-effective in the long term.

5. Test for yourself: You can gain basic experience from your existing desktop or laptop. You can run both VMware vSphere and Microsoft Hyper-V in either VMware Workstation or VMware Fusion to create a nice virtual learning and testing environment.

HYPERVISOR REFERENCE MODEL



There are 3 main modues coordinate in order to emiulate the undrelying hardware:

1. Dispatcher
2. Allocator
3. Interpreter

DISPATCHER:
The dispatcher behaves like the entry point of the monitor and reroutes the instructions of the virtual machine instance to one of the other two modules.

ALLOCATOR:
The allocator is responsible for deciding the system resources to be provided to the virtual machine instance.It means whenever virtual machine tries to execute an instruction that results in changing the machine resources associated with the virtual machine, the allocator is invoked by the dispatcher.

INTERPRETER:
The interpreter module consists of interpreter routines.These are executed, whenever virtual machine executes a priviliged instruction.

Infrastructure Security

IaaS application providers treat the applications within the customer virtual instance as a black box and therefore are completely indifferent to the operations and management of a applications of the customer . The entire pack 146 D. Velev and P. Zlateva (customer application and run time application) is run on the customers' server on provider infrastructure and is managed by customers themselves. For this reason it is important to note that the customer must take full responsibility for securing their cloud deployed applications .

• Cloud deployed applications must be designed for the internet threat model.

• They must be designed with standard security countermeasures to guard against the common web vulnerabilities.

• Customers are responsible for keeping their applications up to date - and must therefore ensure they have a patch strategy to ensure their applications are screened from malware and hackers scanning for vulnerabilities to gain unauthorized access to their data within the cloud.
• Customers should not be tempted to use custom implementations of Authentication, Authorization and Accounting as these can become weak if not properly implemented. The foundational infrastructure for a cloud must be inherently secure whether it is a private or public cloud or whether the service is SAAS, PAAS or IAAS.
• Inherent component-level security: The cloud needs to be architected to be secure, built with inherently secure components, deployed and provisioned securely with strong interfaces to other components and supported securely, with vulnerability-assessment and change-management processes that produce management information and service-level assurances that build trust.
• Stronger interface security: The points in the system where interaction takes place (user-to-network, server-to application) require stronger security policies and controls that ensure consistency and accountability.
• Resource lifecycle management: The economics of cloud computing are based on multi-tenancy and the sharing of resources. As the needs of the customers and requirements will change, a service provider must provision and decommission correspondingly those resources - bandwidth, servers, storage and security. This lifecycle process must be managed in order to build trust. The infrastructure security can be viewed, assessed and implemented according its building levels - the network, host and application levels
Infrastructure Security – The Network Level When looking at the network level of infrastructure security, it is important to distinguish between public clouds and private clouds. important to distinguish between public clouds and private clouds. With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider. If public cloud services are chosen, changing security requirements will require changes to the network topology and the manner in which the existing network topology interacts with the cloud provider's network topology should be taken into account .There are four significant risk factors in this use case: Cloud Infrastructure Security 147
• Ensuring the confidentiality and integrity of organization's data-in-transit to and from a public cloud provider; • Ensuring proper access control (authentication, authorization, and auditing) to whatever resources are used at the public cloud provider;
• Ensuring the availability of the Internet-facing resources in a public cloud that are being used by an organization, or have been assigned to an organization by public cloud providers;
• Replacing the established model of network zones and tiers with domains. 4.2 Infrastructure Security – The Host Level When reviewing host security and assessing risks, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models public, private, and hybrid) should be considered [7]. The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services. IaaS customers are primarily responsible for securing the hosts provisioned in the cloud (virtualization software security, customer guest OS or virtual server security). 4.3 Infrastructure Security – The Application Level Application or software security should be a critical element of a security program. Most enterprises with information security programs have yet to institute an application

security program to address this realm. Designing and implementing applications aims at deployment on a cloud platform will require existing application security programs to reevaluate current practices and standards. The application security spectrum ranges from standalone single-user applications to sophisticated multiuser e-commerce applications used by many users. The level is responsible for managing [7], [9], [10]:
• Application-level security threats;
• End user security;
• SaaS application security;
• PaaS application security;
• Customer-deployed application security
• IaaS application security
• Public cloud security limitations It can be summarized that the issues of infrastructure security and cloud computing lie in the area of definition and provision of security specified aspects each party delivers. 5 Conclusion The cloud is a major challenge in how computing resources will be utilized since aim of the cloud computing is to change the economics of the data center, but before sensitive and regulated data move into the public cloud, issues of security 148 D. Velev and P. Zlateva standards and compatibility must be addressed including strong authentication, delegated authorization, key management for encrypted data, data loss protections and regulatory reporting. All are elements of a secure identity, information and infrastructure model and can be applied to private and public clouds as well as to IAAS, PAAS and SAAS services. In the development of public and private clouds the service providers will need to use these guiding principles to adopt and extend security tools and secure products to build and offer end-to-end trustworthy cloud computing and services.

Data Security And Privacy Issues

Cloud computing has been envisioned as the next generation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user's requirements .

Data security has consistently been a major issue in IT. Data security becomes particularly serious in the cloud computing environment, because data are scattered in different machines and storage devices including servers, PCs, and various mobile devices such as wireless sensor networks and smart phones. Data security in the cloud computing is more complicated than data security in the traditional information systems.

To make the cloud computing be adopted by users and enterprise, the security concerns of users should be rectified first to make cloud environment trustworthy. The trustworthy environment is the basic prerequisite to win confidence of users to adopt such a technology. Cloud computing environment provides two basic types of

functions: *computing* and *data storage.* In the cloud computing environment, consumers of cloud services do not need anything and they can get access to their data and finish their computing tasks just through the Internet connectivity. During the access to the data and computing, the clients do not even know where the data are stored and which machines execute the computing tasks.

Coming to data storage, data protection and security are the primary factors for gaining user's trust and making the cloud technology successfully used. A number of data protections and data security techniques have been proposed in the research field of cloud computing. However, data protection related techniques need to be further enhanced.

Services of cloud computing are provided across the entire computing spectrum. Nowadays, organizations and companies are moving and extending their business by adopting the cloud computing to lower their cost. This can contribute to free more man-powers to focus on creating strategic differentiation and business division of labor is clearer.

The cloud is growing continuously because it could provide high performance computational services at cheaper rates. Famous IT companies such as Microsoft (http://azure.microsoft.com/), Amazon (http://aws.amazon.com/), Google (https://cloud.google.com/), and Rakespace (http://www.rackspace.com/) have provided cloud service on the Internet.

The concept of cloud has a number of implementations based on the services from service providers. For example, Google Apps Engine, Microsoft Azure, and Amazon Stack are popular implementations of cloud computing provided by cloud service providers, that is, Google, Microsoft, and Amazon companies. Besides, the ACME enterprise implemented VMware based v-Cloud for permitting multiple organizations to share computing resources.

According to the difference of access scope, cloud can be divided into three types: *public cloud*, *private cloud*, and *hybrid cloud.* Public cloud is as the property of service provider and can be used in public, private cloud refers to being the property of a company, and hybrid cloud is the blends of public and private cloud. Most of the existing cloud services are provided by large cloud service companies such as Google, Amazon, and IBM. A private cloud is a cloud in which only the authorized users can access the services from the provider. In the public cloud anybody can use the cloud services whereas the hybrid cloud contains the concept of both public and private clouds.

Cloud computing can save an organization's time and money, but trusting the system is more important because the real asset of any organization is the data which they share in the cloud to use the needed services by putting it either directly in the relational database or eventually in a relational database through an application.

Cloud computing brings a number of attributes that require special attention when it comes to trusting the system. The trust of the entire system depends on the data protection and prevention techniques used in it. Numerous different tools and techniques have been tested and introduced by the researchers for data protection and prevention to gain and remove the hurdle of trust but there are still gaps which need attention and are required to be lined up by making these techniques much better and effective.

The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information .

The major issues in the cloud computing include resource security, resource management, and resource monitoring. Currently, there are no standard rules and regulations to deploy applications in the cloud, and there is a lack of standardization control in the cloud. Numerous novel techniques had been designed and implemented in cloud; however, these techniques fall short of ensuring total security due to the dynamics of the cloud environment.

The inherent issues of data security, governance, and management with respect to control in the cloud computing are discussed in . Sun et al. highlighted the key security, privacy, and trust issues in the existing environment of cloud computing and help users to recognize the tangible and intangible threats related to its use. According to the authors, there are three major potential threats in cloud computing, namely, *security*, *privacy*, and *trust*. Security plays a critical role in the current era of long dreamed vision of computing as a utility. It can be divided into four subcategories: *safety mechanisms*, *cloud server monitoring or tracing*, *data confidentiality*, and *avoiding malicious insiders' illegal operations and service hijacking.*

A data security framework for cloud computing networks is proposed . The authors mainly discussed the security issues related to cloud data storage. There are also some patents about the data storage security techniques . A security and privacy framework for RFID in cloud computing was proposed for RFID technology integrated to the cloud computing , which will combine the cloud computing with the Internet of Things.

In short, the foremost issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. The security challenges in the cloud include threats, data loss, service disruption, outside malicious attacks, and multitenancy issues . Data security issues are primarily at SPI (SaaS, PaaS, and IaaS) level and the major challenge in cloud computing is data sharing.

Now we will review different security techniques and challenges for data storage security and privacy protection in the cloud computing environment. As Figure 1 shows, a comparative research analysis of the existing research work regarding the techniques used in the cloud computing through data security aspects including data integrity, confidentiality, and availability. Data privacy issues and technologies in the cloud are also studied, because data privacy is traditionally accompanied with data security. Comparative studies on data security and privacy could help to enhance the user's trust by securing data in the cloud computing environment.

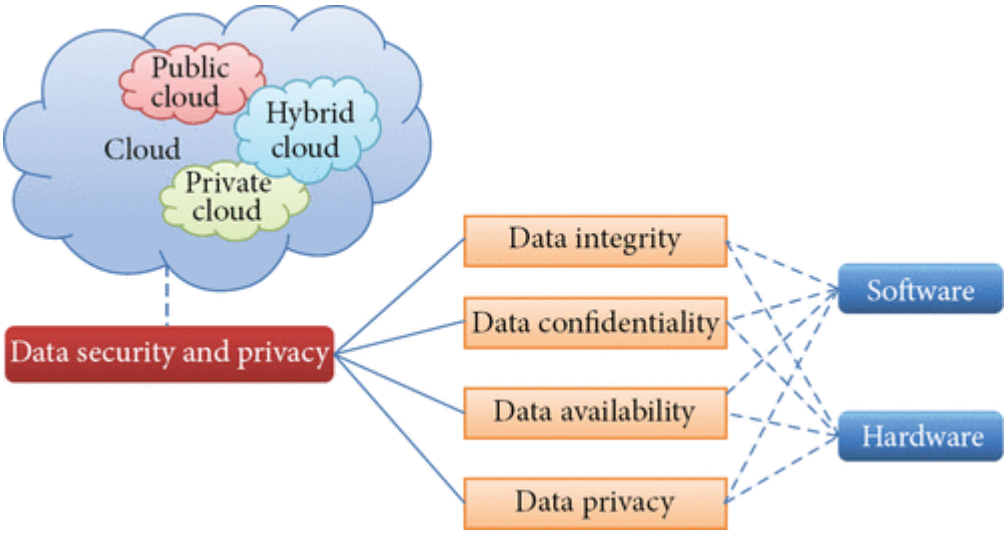


Figure 1 Organization of data security and privacy in cloud computing.

2. Data Integrity

Data integrity is one of the most critical elements in any information system. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen.

Data integrity is easily achieved in a standalone system with a single database. Data integrity in the standalone system is maintained via database constraints and transactions, which is usually finished by a database management system (DBMS). Transactions should

follow ACID (atomicity, consistency, isolation, and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity.

Authorization is used to control the access of data. It is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.

Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users. Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS. Besides data storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.

Owing to the large quantity of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data. By avoiding the unauthorized access, organizations can achieve greater confidence in data integrity. The monitoring mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity. Cloud computing providers are trusted to maintain data integrity and accuracy. However, it is necessary to build the third party supervision mechanism besides users and cloud service providers.

Verifying the integrity of data in the cloud remotely is the perquisite to deploy applications. Bowers et al. proposed a theoretical framework “Proofs of Retrievability” to realize the remote data integrity checking by combining error correction code and spot-checking [17]. The HAIL system uses POR mechanism to check the storage of data in different clouds, and it can ensure the redundancy of different copies and realize the availability and integrity checking .

3. Data Confidentiality

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness .

Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key

management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization.

3.1. Homomorphic Encryption

Encryption is usually used to ensure the confidentiality of data. Homomorphic encryption is a kind of encryption system . It ensures that the cipher text algebraic operation results are consistent with the clear operation after encryption results; besides, the whole process does not need to decrypt the data. The implementation of this technique could well solve the confidentiality of data and data operations in the cloud.

Gentry firstly proposed the fully homomorphic encryption method [22], which can do any operation that can be performed in clear text without decrypting. It is an important breakthrough in the homomorphic encryption technology. However, the encryption system involves very complicated calculation, and the cost of computing and storage is very high. This leads to the fact that the fully homomorphic encryption is still far from real applications.

For more flexibility and enhanced security, a hybrid technique that combines multiple encryption algorithms such as RSA, 3DES, and random number generator has been proposed . RSA is useful for establishing secure communication connection through digital signature based authentication while 3DES is particularly useful for encryption of block data. Besides, several encryption algorithms for ensuring the security of user data in the cloud computing are discussed .

3.2. Encrypted Search and Database

Because the homomorphic encryption algorithm is inefficient, researchers turn to study the applications of limited homomorphic encryption algorithm in the cloud environment. Encrypted search is a common operation.

Manivannan and Sujarani have proposed a lightweight mechanism for database encryption known as transposition, substitution, folding, and shifting (TSFS) algorithm. However, as the numbers of keys are increased, the amount of computations and processing also increases.

In-Memory Database encryption technique is proposed for the privacy and security of sensitive data in untrusted cloud environment . A synchronizer exists between the owner and the client for seeking access to the data. Client would require a key from the synchronizer to decrypt the encrypted shared data it receives from the owner. The synchronizer is utilized to store the correlated shared data and the keys separately. A

shortcoming of this technique is that the delays occur due to the additional communication with the central synchronizer. However, this limitation can be mitigated by adopting group encryption and through minimizing communication between nodes and synchronizer.

Huang and Tso proposed an asymmetric encryption mechanism for databases in the cloud. In the proposed mechanism, the commutative encryption is applied on data more than once and the order of public/private key used for encryption/decryption does not matter. Reencryption mechanism is also used in the proposed scheme which shows that the cipher-text data is encrypted once again for duality. Such schemes are very useful in the cloud applications where privacy is a key concern.

A privacy-preserving multikeyword ranked search approach over encrypted cloud data was proposed , which can search the encrypted cloud data and rank the search results without leakage of the user's privacy.

3.3. Distributive Storage

Distributive storage of data is also a promising approach in the cloud environment. Security issues related to data privacy in the cloud computing including integrity of data, intrusion, and availability of service in the cloud. To ensure the data integrity, one option could be to store data in multiple clouds or cloud databases. The data to be protected from internal or external unauthorized access are divided into chunks and Shamir's secret algorithm is used to generate a polynomial function against each chunk. Ram and Sreenivaasan have proposed a technique known as security as a service for securing cloud data. The proposed technique can achieve maximum security by dividing the user's data into pieces. These data chunks are then encrypted and stored in separated databases which follow the concept of data distribution over cloud. Because each segment of data is encrypted and separately distributed in databases over cloud, this provides enhanced security against different types of attacks.

Arfeen et al. describe the distribution of resources for cloud computing based on the tailored active measurement. The tailored measurement technique is based on the network design and the specific routes for the incoming and outgoing traffic and gradually changing the resources according to the user needs. Tailored measurement depends on the computing resources and storage resources. Because of the variable nature of networks, the allocation of resources at a particular time based on the tailored active method does not remain optimal. The resources may increase or decrease, so the system has to optimize changes in the user requirement either offline or on-line and the resource connectivity.

3.4. Hybrid Technique

A hybrid technique is proposed for data confidentiality and integrity , which uses both key sharing and authentication techniques. The connectivity between the user and the cloud service provider can be made more secure by utilizing powerful key sharing and authentication processes. RSA public key algorithm can be used for secure distribution of the keys between the user and cloud service providers.

A three-layered data security technique is proposed : the first layer is used for authenticity of the cloud user either by one factor or by two factor authentications; the second layer encrypts the user's data for ensuring protection and privacy; and the third layer does fast recovery of data through a speedy decryption process.

An event-based isolation of critical data in the cloud approach is proposed , TrustDraw, a transparent security extension for the cloud which combines virtual machine introspection (VMI) and trusted computing (TC).

3.5. Data Concealment

Data concealment could also be used to keep the data confidentiality in the cloud. Delettre et al. introduced a concealment concept for databases security. Data concealment approaches merge real data with the visual fake data to falsify the real data's volume. However, authorized users can easily differentiate and separate the fake data from the real data. Data concealment techniques increase the overall volume of real data but provide enhanced security for the private data. The objective of data concealment is to make the real data safe and secure from malicious users and attackers.

Watermarking method can serve as a key for the real data. Only the authorized users have key of watermarking, so the authentication of users is the key to ensure the true data to be accessible for right users.

3.6. Deletion Confirmation

Deletion confirmation means that data could not be recovered when users delete their data after the deletion confirmation. The problem is very serious, because more than one copy exists in the cloud for the security and convenience of data recovery. When users delete their data with confirmation, all the copies of data should be deleted at the same time. However, there are some data recovery technologies that could recover the data deleted by users from the hard disks. So the cloud storage providers should ensure that the deleted data of users could not be recovered and used by other unauthenticated users.

To avoid the data be recovered and unauthenticatedly used, a possible approach is to encrypt the data before uploading to the cloud storage space. FADE system is based on

technologies such as Ephemerizer. In the system, data are encrypted before they are uploaded to the cloud storage. When users decide to delete their data, the system just to apply the specific strategy to all the storage space could be covered with new data for replacing the deletion operation.

4. Data Availability

Data availability means the following: when accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.

The issue of storing data over the transboarder servers is a serious concern of clients because the cloud vendors are governed by the local laws and, therefore, the cloud clients should be cognizant of those laws. Moreover, the cloud service provider should ensure the data security, particularly data confidentiality and integrity. The cloud provider should share all such concerns with the client and build trust relationship in this connection. The cloud vendor should provide guarantees of data safety and explain jurisdiction of local laws to the clients. The main focus of the paper is on those data issues and challenges which are associated with data storage location and its relocation, cost, availability, and security.

Locating data can help users to increase their trust on the cloud. Cloud storage provides the transparent storage service for users, which can decrease the complexity of cloud, but it also decreases the control ability on data storage of users. Benson et al. studied the proofs of geographic replication and succeeded in locating the data stored in Amazon cloud .

4.1. Reliable Storage Agreement

The most common abnormal behavior of untrusted storage is that the cloud service providers may discard part of the user's update data, which is hard to be checked by only depending on the simple data encryption. Additionally, a good storage agreement needs to support concurrent modification by multiple users.

Mahajan et al. proposed Depot which can guarantee Fork-Join-Causal-Consistency and eventual consistency . It can effectively resist attacks such as discarding and it can support the implementation of other safety protections in the trusted cloud storage environment (such as Amazon S3).

Feldman et al. proposed SPORC , which can implement the safe and reliable real-time interaction and collaboration for multiple users with the help of the trusted cloud environment, and untrusted cloud servers can only access the encrypted data.

However, operation types supported by reliable storage protocol support are limited, and most of the calculations can only occur in the client.

4.2. Reliability of Hard-Drive

Hard-drive is currently the main storage media in the cloud environment. Reliability of hard disks formulates the foundation of cloud storage. Pinheiro et al. studied the error rate of hard-drives based on the historical data of hard-drive . They found that the error rate of hard-drives is not closely relevant to the temperature and the frequency to be used, while the error rate of hard-drives has the strong clustering characteristics. Current SMART mechanism could not predict the error rate of hard disks. Tsai et al. studied the correlation between the soft error and hard error of hard disks, and they also found that the soft error could not predict the hard errors of hard-drives precisely , only about 1/3 probability that hard errors follow the soft errors.

5. Data Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively . Privacy has the following elements.

(i) When: a subject may be more concerned about the current or future information being revealed than information from the past.

(ii) How: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.

(iii) Extent: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

In commerce, consumer's context and privacy need to be protected and used appropriately. In organizations, privacy entails the application of laws, mechanisms, standards, and processes by which personally identifiable information is managed .

In the cloud, the privacy means when users visit the sensitive data, the cloud services can prevent potential adversary from inferring the user's behavior by the user's visit model (not direct data leakage). Researchers have focused on Oblivious RAM (ORAM) technology. ORAM technology visits several copies of data to hide the real visiting aims of users.

ORAM has been widely used in software protection and has been used in protecting the privacy in the cloud as a promising technology. The privacy issues differ according to different cloud scenarios and can be divided into four subcategories as follows:

(i) how to enable users to have control over their data when the data are stored and processed in cloud and avoid theft, nefarious use, and unauthorized resale,

(ii) how to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is an usual choice, and avoid data loss, leakage, and unauthorized modification or fabrication,

(iii) which party is responsible for ensuring legal requirements for personal information,

(iv) to what extent cloud subcontractors are involved in processing which can be properly identified, checked, and ascertained.

5.1. Service Abuse

Service abuse means that attackers can abuse the cloud service and acquire extra data or destroy the interests of other users.

User data may be abused by other users. Deduplication technology has been widely used in the cloud storage, which means that the same data often were stored once but shared by multiple different users. This will reduce the storage space and cut down the cost of cloud service providers, but attackers can access the data by knowing the hash code of the stored files. Then, it is possible to leak the sensitive data in the cloud. So proof of ownership approach has been proposed to check the authentication of cloud users .

Attackers may lead to the cost increase of cloud service. Fraudulent resource consumption is a kind of attack on the payment for cloud service. Attackers can consume the specific data to increase the cost for cloud service payment

5.2. Averting Attacks

The cloud computing facilitates huge amount of shared resources on the Internet. Cloud systems should be capable of averting Denial of Service (DoS) attacks.

Shen et al. analyzed requirement of security services in cloud computing .The authors suggest integrating cloud services for trusted computing platform (TCP) and trusted platform support services (TSS). The trusted model should bear characteristics of confidentiality, dynamically building trust domains and dynamic of the services. Cloud infrastructures require that user transfers their data into cloud merely based on trust.

Neisse et al. analyzed indifferent attacks scenarios on Xen cloud platform to evaluate cloud services based on trust. Security of data and trust in cloud computing is the key point for its broader adoption .

5.3. Identity Management

Cloud computing provides a podium to use wide range of Internet-based services . But besides its advantages, it also increases the security threat when a trusted third party is involved. By involving a trusted third party, there is a chance of heterogeneity of users which affects security in the cloud. A possible solution to this problem could be to use a trusted third party independent approach for Identity Management to use identity data on untrusted hosts.

Squicciarini et al. focused on problems of data leakage and loss of privacy in cloud computing . Different levels of protections can be used to prevent data leakage and privacy loss in the cloud. Cloud computing provides new business services that are based on demand. Cloud networks have been built through dynamic virtualization of hardware, software, and datasets. Cloud security infrastructure and the trust reputation management play a vital role to upgrade the cloud services . The Internet access security, server access security, program access security, and database security are the main security issues in the cloud.

Legal Issues Surrounding Cloud Computing

The legal issues that frequently arise in the cloud are wide-ranging. However, attempting a broad generalisation, mainly four types of issues arise therein:

1. Privacy of data and data security
2. Issues relating to contractual relation between the cloud service provider and the customer
3. Complex jurisdictional issues, or issues relating to the location of the data and the set of laws applicable
4. Commercial as well as business considerations

At the outset, it may very well be clarified that though cloud computing enables the customer access to computing, networking, storage resources just like traditional outsourcing services and Application Service Providers (ASPs), it has a legal nature quite different from these two owing to its distinctive features like ‘on-demand access’, and ‘unit-based pricing’ (pay-per-use).

Privacy and data security issues:

Seemingly, the main privacy/data security issue relating to the cloud is ‘data breach’. Data breach may be in the generic sense defined as the loss of unencrypted electronically stored

personal information . A data breach can cause loss to both the provider as well as the customer in numerous ways; with identity theft and chances of debit/credit card fraud to the customer, and financial harm, loss of customer, loss of reputation, potential lawsuits et cetera for the provider.

The American law requires data breach notification to be issued of affected persons in such case of a data breach. Almost all the states in the United States now require notification of affected persons upon the occurrence of a data breach.

Talking about the Indian scenario, most of the providers are seen to attempt at lessening their risk liability in case of a data breach scenario. However, as more sensitive information is entering the cloud every passing day, businesses and corporations have started negotiating the contracts so as to insert terms that expand the contractual obligations of the providers.

Problem arises when the data is subject to more than one jurisdictions, and the jurisdictions have different laws regarding data privacy. For example, the European Union Data Privacy Directive clearly states that 'Data cannot leave the EU unless it goes to a country that ensures an "adequate level of protection".' Now, although such statement makes the EU provisions easily enforceable, but it restricts the data movement thereby reducing the data efficiency.

Contracting Issues:

Clearly, licensing agreements are fundamentally different from Service agreements. Cloud essentially, in all its permutations (IaaS, PaaS, SaaS), is a service, and therefore is governed by a Service agreement instead of a Licensing agreement.

However, the main issue regarding the Cloud Service agreements is 'contract of adhesion'. Owing to the limited expansion of Cloud Services in India, most of the time the 'Click-wrap agreement' model is used, causing the contract to be one of the contract of adhesion. It leaves no or little scope for negotiation on the part of the user/customer.

With the expansion of the Cloud computing, gradually the negotiation power of the large corporation will cause the Cloud Contracts to be standard and negotiated ones. However, at an individual level, this is still a far destination.

Legal provisions clearly cannot force the cloud providers to have a negotiating session with each and every customer. However, legal provisions may be made to ensure that the liability and risk responsibility clauses follow a standard pattern which compensates the user for the lack of negotiation during the formation of the contract.

Jurisdictional Issues:

Jurisdiction is the authority of a court to judge acts committed in a certain territory. Jurisdiction in case of legal issues relating to the Cloud services becomes difficult and critical because of the features of Cloud like 'Virtualization', and 'Multi-tenancy'.

While virtualization ensures the requirement of less hardware and consumption of less power thereby ensuring computing efficiency, it also on the other hand makes it difficult for the cloud user or the cloud provider to know what information is housed on various machines at any given time.

Multi-tenancy refers to the ability of a cloud provider to deliver services to many individuals or organisations from a single shared software. The risk with this is that it makes it highly possible that the data of one user may be accessed in an unauthorised manner by another user since the data of various users are only virtually separated and not physically. Also, it makes it difficult to back up and restore data.

The cloud enables a great deal of flexibility in data location, which ensures maximum efficiency in data usage and accessibility. However, it creates a number of legal issues as well. It makes it quite possible a scenario that the same data may be stored in multiple locations at a given time. Now, if the multiple locations are subject to different jurisdiction and different legal system, there arises a possibility that there may be conflicting legal provisions regarding data in the two aforementioned different locations. This gives rise to most of the jurisdictional issues in Cloud computing.

Also, laws relating to confidentiality and Government access to data are different across different nations. While the Indian laws manage to strike a balance between national security and individual privacy, most of the nations do not prefer a balance and have adopted a biased view on this. Problem of conflict of laws arises herein, in such cases.

Commercial and Business Considerations:

Other commercial and business considerations like the urge to minimize risk, maintain data integrity, accessibility and availability of data as well as Service level Agreements have also significantly shaped the present as well as future of Cloud Computing in India. It also creates a number of foreseeable as well as unforeseeable issues that needs to be addressed by dedicated legislations therefor.

It is an accepted truth that Law always lags behind technical innovations, and the complexities of the Cloud innovations and related Cloud Services like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) will force the law and legislations to catch up in order for an effective legal system that provides legal remedies to prevent and redress the resultant harms.

Raising awareness, ensuring universal access to information, and resource mobilizing are complimentary solutions that'll never go wrong for the Indian scenario in order to add to the effectiveness of an effective legal system.