4. WHAT DOES IT TAKES TO PROVIDE IAAS?

According to NIST, the Infrastructure-as-a-Service is the capability provided to the consumer is to provision processing, storage networks and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not handle or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications and possibly limited control of selected networking components (e.g., host firewalls) (NIST).

4.1 Infrastructure

Infrastructure-as-a-Service combines the abstracts of hardware and software into a computing system which is used to provide different kind of service to the customer. The usage of these services comes at a cost which the user has to pay. The aim is to provide a virtual environment that is fast, appealing and elastic so that it can be the base for Software-as-a-Service and Platform-as-a-Service. The IaaS is usually seen as a provider of a standardized effective server. The service levels that are provided cover not only an essential environment but also performance. If there are any operational risks, the customer has to take the onus and the responsibility of it. The customer also has to take responsibility for configuration, guest operating system, database and all computing capabilities such a performance, band width and storage. As a provision model, it out sources the equipment and tools that are required as support operations.

The characteristics and components of IaaS are:

- Utility computing services
- Automated administrative tasks
- Dynamic scaling
- Desktop virtualization
- Policy-based services
- Internet connectivity

These all characteristics are explained as given below.
4.1.1 Utility Computing Services
It is when the computing capabilities are packaged for the customer to use for a metered cost. The computation includes storage. It can acquire computer resources at no cost almost instead computational resources are rented. Utility computing can support grid computing. Grid computing has very large computations or sudden peaks in demand.

4.1.2 Automation of Administrative Tasks
When the defined tasks and the system are programmed to respond to the administrative tasks, it is known as automation of administrative tasks. Automatic task control is a simple three steps requirement.

i. Decide which administrative functions occur regularly and can be programmed to respond independently and automatically
ii. Define a set of jobs and alert
iii. Run the SQL Server Agent Service

Automating administration services means a person does not have to repeatedly do the same thing, and a program response can leave the person free for more productive work.

4.1.3 Dynamic Scaling
Scalability is important assistance of cloud computing. Dynamic scaling makes difference as an advanced solution. Most of the IaaS clouds deal with the single management primitives such as adding or deleting VMs.

4.1.4 Desktop Virtualization
Desktop virtualization is otherwise called customer virtualization. It is an engineering used to partitioned the machine environment from the physical machine. It is a kind of customer server where the virtual work area top is put away in a remote or someplace else however not the machine itself.

Virtual Desktop Infrastructure or VDI is the same as the interface. It is a popular method of the interface. This type uses the server computing models. The desk-top virtualization is enabled through hardware and software. VDI hosts the desktop environment in a remote or centralized server. In today’s professional world mobility
and access is very necessary. The aim is to take productivity beyond its traditional means. Today, users want a virtual workspace that is the central hub for accessing computer software devices, allowing greater mobility in a secure and safe environment. The purpose of desktop virtualization is to deliver end user needs through multiple devices anytime anywhere. In a business environment, it helps to reduce costs and minimize risks.

Desktop virtualization gives design and original configuration as well as agilities, which is needed in a highly computerized environment. Desk-top virtualization will be a stable requirement for companies in the transition to cloud computing as it lowers the investment costs, and the services can be rented instead.

Parallel desktop which is known best for its desk-top virtualization around the world is of the opinion that in the years to come, cloud virtualization is the key to success. DABCC also feels that ‘less can be more’ when it comes to desktop virtualization. The new architecture is unlike anything that exists today for desktop virtualization, and the entire industry appears to be optimistic about the long term requirements of desktop virtualization.

The benefit of desktop virtualization is used in conjunction with application virtualization and user profile desktop management (http://www.cisco.com).

### 4.1.5 Disaster-Recovery

Disaster-recovery management is perhaps one of the issues of major area of usage. One can categorize the entire function in five key steps.

- **Get an early start:**
  Whole important data should be stored in an offsite location where it can be accessed immediately during an emergency.

- **Know the business objectives:**
  The specific business requirements for companies must be understood clearly. Storing data in an offsite location and then accessing it during a disaster management process, means that the company functions will be down for at least a day or so before it is functionally again.

  However, companies like Amazon and companies in the finance industry run around the clock twenty-four hours a day, seven days a week and the data is
processed and automatically uploaded to a remote server and then accessed when necessary. This enables these companies to retrieve data immediately without the company functions getting de-operative for a while or a day.

- **Practice:**
  It is important to practice the recovery systems and also have written instructions for employees to understand and use in the event of a disaster or emergency.

- **Share critical knowledge:**
  In desktop virtualization, the need for the independent person to hold all important data just in case the concerned employees are unavailable has been recognized. Every company has now incorporated the independent data holder who can access the emergency data from the remote server.

- **Reliability:**
  During a natural disaster, it is always possible that all communication systems could be down indefinitely or temporarily. In such a case, the cloud is not only essential but also reliable for the continuation of communication during an emergency (www.ciol.com).

### 4.1.6 Policy-Based Services

Cloud computing is a policy-based service which identify the needs of an organization and then work on the cloud computing architecture. With policy-based services of the cloud, it is easy for the people in general to use any device and have communication as well as corporate policy requirements.

To put it simply this is modelling the requirements and incorporating them into the software systems or organizations. It involves various stages:

i. Enterprise architecture
ii. Application architecture
iii. Service oriented architecture and cloud computing

Any methodology that includes a modelling language and can be used in a domain problem or domain solution is what really describes the process of policy-based services. These services provide a comprehensive view of the analysis, architecture and design of all software entities in an organization. These service-oriented software
entities are also known as assets basically assets of policy-based services and collectively, these assets are known as services.

IBM had earlier announced service oriented modeling and architecture (SOMA), and it was the first publicly claimed SOA methodology in 2004. SOMA refers to use and designing with the SOA method. SOMA covers SOAD through the identification, realization and specification of services [91]. SOMA builds on the latest techniques of domain analysis, functional area grouping. Variability analysis processes modeling, object oriented analysis, design and use case modeling and development that are component based.

The entire range comes under policy-based services. SOMA which is the base of service oriented policies identifies the components and modeling services. Furthermore, it identifies component boundaries, flows as well as compositions and information through complementary methods.

4.1.7 Internet Connectivity

- **Access:**
  To understand the connectivity of the Internet, one must first understand the meaning of Internet access. It is the connection that a person can avail through computer terminals and computers as well as mobile devices and computer networks.

- **Software defined networking (SDN):**
  It allows network administrators to administer the network services through the concept of lower level functionality. Using this, the inventors, vendors and the end users can make networking easier and simpler as well as faster.

- **Open flow:**
  SDN requires a technique for the control plane to interact with the data plane. The mechanism that is used is an open flow. Other mechanisms also fit into the mechanism threshold to help the communication of the control plane and the data plane.

- **Open networking foundation:**
  This was promoted to enhance the image of the SDN and open flow which commonly came to be known as cloud computing.
The advantage of the Internet protocol with the cloud cover is that it enables the networks to scale and extend by connected junctions of forward packages to the next forward hop base with information on a need to know basis. This method is simple, resilient and scalable.

4.2 IaaS Services

Based on the NIST definition of Infrastructure-as-a-Service, it is the hardware made available as a service, and it can be provided in two different ways like Virtual IaaS and Physical IaaS. Infrastructure-as-a-Service is known as virtual when the same hardware is assigned, accessed and used by various instances that think and act as independent systems. Physical IaaS on the other hand, assigns more hardware to extra requirements.

Until recently, physical IaaS has not been so popular because it did not meet up to the essential characteristic of dynamic and automatic resource pooling. The service provider had manually installed the servers and configured according to client requests and there was a time lag of few days between the client request and implementation. Virtual IaaS then again, utilizes virtualization programming and permit single physical server to run different virtual servers on a few machines and give benefit through those various virtual machines which permits checking assets and assigning them naturally. However, increasing the number of virtual machines beyond a certain limit on a physical server will only reduce the performance of the service because the actual load is carried by a single physical server and so elasticity in this case has a limitation. The hypervisors and their management consoles also are extremely expensive because licenses are charged per processor on a server instead of the number of physical servers. The open-source hyper visors is being costly because the management consoles do not come for free, and it is not a practical solution for manually keep an eye on the resources being utilized by the various virtual servers (http://www.fujitsu.com).

On July 4th 2013, Fujitsu Laboratories Limited announced a new technology that is capable of providing on demand physical servers, configured according to client's requirements in flat ten minutes. This technology is called Resource Pool Architecture (RPA). RPA is equipped for pooling different individual fittings assets like CPU, memory, and plate stockpiling and unites them as a component of a construction
modeling inside a physical server. Figure 4.1 below shows a comparison between traditional physical IaaS and the IaaS using RPA.

Figure 4.1 Comparisons between Traditional Physical IaaS and the IaaS Using RPA

In conventional physical IaaS, when physical servers are provided to the customer then there is fixed allocation. Whereas in IaaS using RPA, it is dynamically provided. Also, in conventional physical IaaS, there is fixed allocation of resources to the customer but in IaaS using RPA, physical systems are dynamically configured to customer definition.

4.2.1 Virtual IaaS

Virtual IaaS is made possible by using a hypervisor which can be a software, firmware or hardware that is capable of creating virtual machines (guests) on the physical hardware (host). Hypervisors are again of two types as Type One and Type Two. The figure 4.2 below gives a clear picture of types of hypervisors. The Type One hypervisor is also known as bare metal hypervisor or native hypervisor. This is because the hypervisors installed on the hardware. Then operating system is installed on the hypervisor.
Figure 4.2 Types of Hypervisors

The Type Two hypervisors are also known as hosted hypervisor because in this, the hardware already has an operating system. Furthermore, the hypervisor is installed through the operating system which allows for the installation of other operating systems.

An example for Type One Hypervisor is Microsoft Hyper-V (though it is sometimes misidentified as Type Two). Hyper-V is available as a standalone version and as a part of Windows Server 2008. In both the versions, the hypervisor is installed before the operating system, and the entire virtual environment run directly on the hypervisor. Although servers using Type one hypervisors is faster and need lesser resources when compared to Type Two hyper visors. Type Two hyper visors are more popular because they are not as expensive as Type One hypervisor management consoles and will serve the small-scale requirements well. Type One hypervisors is VMware, Citrix, Xen, Microsoft Hyper-V, Windows Virtual PC, Proxmox VE, Wind River Hypervisor, IBM Power VM, Parallels and Oracle VM Server. Type Two Hypervisors
are Parallels Vitruzzo, Parallel's workstation, VMware V sphere, Virtual Box. Kernel based Virtual Machine (KVM) and OpenVZ.

Hypervisor uses a thin layer of code with software or firmware to achieve fine grained dynamic resource sharing. Hypervisor co-ordinates low level interaction between virtual machine and physical hardware (Gerald, 1974).

4.2.1.1 Benefits of virtualization

i. **Server Consolidation:** With the easy availability of low cost servers in the market, enterprises are experiencing a flooding of servers in their data centers. Providing dedicated servers for applications and devoted servers for handling peak loads are generally the reasons for proliferation of servers and extremely low utilization range is between 10-20%. Virtualization technology is capable of enabling logical server consolidation. This allows enterprises to achieve higher utilization and manage their resources better which in turn reduces Total Cost of Ownership (TCO). There are some workloads that cannot go hand in hand with virtualization on their own or when combined with other workloads. Such circumstances call for ‘intelligent virtualization’ which is achieved with Intelligent Workload Management Strategy, because it is capable of a scan of the network followed by a thorough analysis of the different workloads and their purposes and managing accordingly.

ii. **Dynamic provisioning:** The resource requirements of applications running are dynamic in nature. Dynamic provisioning refers to the flexible provisioning of additional resources. Virtualization software can assign distinct priorities to different workloads and depending on the need to be online or not. This ability is called Workload Quality of Service (QoS). Using this kind of service, clusters can be reconfigured so that the servers in a cluster can be switched dynamically and preemptively from one type of workload to another.

iii. **Virtual hosting:** The method of hosting of multiple domain names on the computer system using a single IP address is called virtual hosting. Virtual hosting allows of efficient use of computer resources such as memory and processor cycles. A common application of virtual hosting is Shared Web Hosting service. The price of Shared Web Hosting is very cheaper than a
dedicated server because many customers are hosted on a single piece of hardware.

iv. **Reliability, Availability and Serviceability:** Virtualization allows for decoupling of workload from underlying hardware to be moved around. This property of virtualization makes services more reliable and available. The ability to move or to migrate the live virtual machines around a network of PCs or servers gives room for easy hardware upgrades without any down time. Rolling software upgrades can be performed in this environment. A mix of production and test environment can be achieved by virtually isolating one environment from the other.

v. **Workload management:** Virtualization is what allows for workload management like isolating workloads from the underlying hardware and QoS prioritization and deploying vertical applications on the same hardware. This feature of virtualization is particularly useful when dealing with legacy compatibility. For example, legacy operating systems like NetWare and Windows 2000 can be kept as one workload alongside others without having to worry about driver updates and hardware changes. In terms of management tools and administration tasks performed on a workload, the virtual machine is not any different from a physical machine.

### 4.2.1.2 Virtualization architecture

It is important to understand architecture of various virtualization solutions because correct planning, exact decisions and performing accurate tasks are impossible without an understanding of the virtualization architecture.

- **Traditional architecture or Type two Hypervisor architecture**

  Below figure 4.3 shows Traditional architecture. It uses Type Two hypervisors. It is installed on a host operating system. The virtualization layer includes the hypervisor and the operating system. It is responsible for the intervention to access the underlying hardware and allowing virtual drivers to share access with the hardware.
Figure 4.3 Traditional Architecture or Type Two Hypervisor

It also does the virtualization management. In this architecture, the I/O virtualization and virtualization management happens in the host operating system. Virtualization software like VMware and Virtual PC use this architecture.

- **Xen Architecture**

  Figure 4.4 gives Xen hypervisor (Microsoft). It is also called a Type One ‘Lean’ hypervisor as it does not require an operating system to be installed and run on the hardware; furthermore, it is reliable only for mediation of access to underlying hardware and is not responsible for sharing access to the hardware with virtual drivers.
As device drivers are not loaded into the Xen platform, it is compatible with virtually any hardware platform. Although the hypervisor does not perform I/O operations, it acts as the traffic police and directing traffic for the operating system to perform the I/O. In the Xen hypervisor the I/O virtualization happens in the virtual machine, and the management tools also run there as well. The OS that runs the management tools or console is called (Dom0 or domain 0). In a Xen virtual environment it is recommended that the OS run Dom0 must be as light as possible, like without a graphical interface. This is because the Xen architecture is designed for and is used in production environments [53].

**Hyper-V Architecture**

Figure 4.5 is Microsoft’s Hyper-V virtualization architecture. If we observe it, we can say that it is similar to Xen’s thin Domo architecture. Partitions are the logical units of isolation and supported by the hypervisor. Each operating system executes within a partition.
It is absolutely necessary to have one-parent partition running windows server in a hypervisor instance. It is in the parent partition and so virtualization stack run and has a direct access to the hardware. Every child partition has hosts and the guest operating system is created by the parent partition. Using the hyper call API, the child partition is created by the parent, where it is the application programming interface exposed by Hyper-V.

- **VMWare ESX Architecture**
  Architecture of VMWare ESX hypervisor is shown in below figure 4.6. It falls into the ‘fat’ Type One hypervisor category. This is because in VMWare ESX, the host operating system and the hypervisor are merged together. A fat hypervisor is not only responsible for mediation of access to the underlying hardware but also for sharing the hardware with virtual drivers.
Sharing hardware with virtual drivers is done through hardware. This is achieved by device drivers who are loaded into the hyper visor. The drawback for this system is that the hypervisor’s compatibility with hardware platforms becomes limited. The brighter side is that it is more user friendly in comparison to the lean hyper visors (Vmware) (Microsoft).

- **Kernel Virtual Machine (KVM) Architecture**

The Kernel Virtual Machine (KVM) is a Type One hypervisor because it is loaded into a Linux kernel and converting it into a hyper visor. Due to this, it becomes a ‘fat’ hyper visor. It is shown in figure 4.7 below.
The management console for the hypervisor is a modified version of QEmu (Quick Emulator) which is a free and open source hosted hypervisor. Device emulation and VM management are handled by QEmu running in user space (linux-kongress) (Microsoft).

- **Container Based Architecture**
  Below figure 4.8 is the architecture of Container based virtualization. It is different from the rest of the structures seen because there are no hypervisors involved. The host operating system provides all the operating system services to each virtual container.
Another name for container based virtualization is parallel virtualization. Container based virtualization does not allow room for any other operating system. Although each container is separate and protected from the other containers, they all consume a single instance of the operating system at the back end. Container based virtualization has the advantage of better performance in comparison to the other architectures but in the matter of flexibility, it lags way behind (Microsoft).

4.2.1.3 Para virtualization / Interoperability

We have seen that in all the distinctive virtual architecture except the container based architecture; various operating systems can be installed as guests on the virtual machines. Although the different operating systems install and operate quite well on the host systems, there are codes or drivers designed to run different systems in enlightened mode. To enable optimum performance of the operating systems, it is important to understand that what it takes to make it happen? We will have a look at the drivers used to enlighten the deployment of Suse Linux enterprise Server (SLES) virtual machines as a guest on Hyper-V host and Windows virtual machines as a guest on Xen host.

- *Hyper-V Linux Integration Components (IC):*
Linux IC is the driver who enables Linux VMs to run in enlightened mode on Hyper-V. Although Linux can run on Hyper-V without the Linux IC, the performance will not be so enhanced. These drivers have been coded in such a path, to the point that it exploits VM Bus, which is information channel between Vsp(virtualization Service Provider), Vsc(virtualization Service Client) and manufactured gadgets gave in Hyper-V to improve the execution of Linux as an issue OS.

The figure 4.9 underneath gives a concise clarification of how gadget drivers are utilized by the working frameworks to connect with the equipment. Every driver has appointed distinctive capacity, and each one capacity compares to diverse equipment. The drivers make gadget items (DO) for each one bit of fittings that it can control. Every gadget article is a representation of the particular equipment to the driver. The Device Objects (DO) is contained in a gadget stack. The stack is made up of DO and utilized for taking care of info/yield (I/O) of every gadget.

The physical structure of the gadget driver can be separated into three modes (Vmware):

i. User mode: This has the API which is the programming application. The working framework uses to begin the I/O Manager, and the Ntdll is the capacity library that uses stubs to begin the working framework.

ii. I/O Manager: The I/O Manager is the sub framework which chooses about what is permitted to every driver to do? The Ntreadfile is a framework used to make and control I/O demands.

iii. Kernel Mode: It is solicitation parcel utilized by I/Os to ask data from the drivers. The I/O Call drivers send IRPS to the right driver who is connected with each one DO.
The figure 4.9 is detail about Characteristics and Functions of the Linux IC Modules, VMBus and VSCs. It is explained as follows:

- In this, communication with parent partition is done through the Linux VMBus.
- VSCs are the Linux drivers for synthetic devices (SCSI, IDE and Ethernet) provided by Hyper-V.
- Each of them translates between Linux I/O requests and Hyper-V VSC commands.
- The devices are registered with Linux Driver Model (LDM)
- The two portions that each VSC contains are:
  a) Driver Interface Mapper (DIM), the portion of the VSC component which interacts with the Linux kernel like a regular Linux driver.
b) VSC Core, the implementation of the core portion of the VSC module which is based on the protocol of the corresponding VSP at Hyper-V host. The VSC core interacts with VSP through the VMBus interface.

i. **SUSE Linux Enterprise Virtual Machine driver pack**

![Figure 4.10 Virtual Machine Driver Pack](image)

The driver model is shown in figure 4.10 which is used by Xen. It has a back end and front end. The back end which can be an emulated device model or para virtual device model, runs in the host OS (Dom0) and provides the multiplexing of the virtual I/O requests across the physical devices. The front end driver is loaded in the guest operating system which sees it as a routine hardware driver that can be used for I/O with hardware devices. For emulated devices, the frontend driver is the same as the typical physical driver for the same device whereas for para virtual devices, it is a special driver designed to talk to the para virtual device at the back end. The front end
driver passes all I/O requests to the back end driver who is running in Dom0. The para virtual device back end has a better performance than emulated device back end. SUSE Linux Enterprise Virtual Machine Driver Pack (VMDP) contains para virtual disk and network front end device drivers for Windows, which allow it to use the higher-performance para virtual devices (shown in grey in the diagram) on the Xen Bus instead of emulated devices (shown in purple in the diagram) on the emulated PCI bus.

These drivers allow hosting of unmodified guests on the top of the combination of SUSE Linux Enterprise Server (SLES 10) SP2 and Xen 3.2 or later, though the recommended host combination is SUSE Linux Enterprise Server 11 (SP1) and Xen3.3 or later (Microsoft).

**4.2.1.4 Virtual networking**

The deliberation of physical assets in virtualization reaches out to the design of systems administration. System cards and switches are additionally virtualizes and the conceivable setups can be very perplexing. The most ordinarily confronted help issues are virtual system setup issues. Understanding the essentials of virtual systems administration is amazingly vital in IaaS on the grounds that virtual systems administration is dependably either in part or completely the obligation of the administration supplier (http://www.networkcomputing.com).

At first, the virtual host (guardian segment or Dom0) before introducing the visitor Virtual machine (tyke or Domu) is joined with the physical system through its physical system card. In this express, all the conventions are sure to the physical system card which gives immediate integration to the server to the physical system.
The above system in figure 4.11 is the virtual network model. In the virtual systems administration show, a virtual machine utilizes a virtual system connector which exhibits itself to the virtual machine's working framework with a MAC address. It can be designed like a physical system connector through the working framework's typical apparatus. This virtual connector can then be joined with a virtual extension or virtual switch.

Arranges that are associated with virtual machines are called virtual systems. In a virtual system, virtual machines cooperate with one another and with physical machines. Straightforward extensions and complex directed situations can be arranged in a virtual system that has been designed on the virtualization host machine.

The virtual network in the below figure 4.12 is an example of a simple bridge between a physical network interface on the host and a virtual bridge. In this diagram, the bridge is connected to a virtual network interface. The virtual network is configured
as a bridge in the virtualization host machine and when configuring a virtual network, and a network switch is created in the host.

**Figure 4.12 Virtual Network**

If the host is Xen, the virtual network can be configured with configuration files for a static configuration or with scripts or with liberty for dynamic configuration. On a Hyper-V host, the virtual network can be configured using the Virtual Network Management Tool.

A virtual bridge which is like a network switch, functions at Layer 2, which is the Data Link Layer (DLL) of the OSI model and forwards frames out through ports based on the Media Access Control (MAC) address destination. If there is an IP address, it is configured on the bridge. The physical interfaces in these are switch ports. They are connected to the physical network because of which the physical interfaces do not have IP addresses. As a result, the host sees and uses the bridge as its network interface.

- Virtual Network adapters
Xen and Hyper-V have different methods of providing network adapters for the guest virtual machine. By understanding their methods, we will get a clear picture of the virtual network concept.

- **Hyper-V Network adapters**

Hyper-V allows its guests to use of two different types of network adapters namely the Legacy Network adapter and the Network Adapter.

- **The Legacy Network adapter**

It is an emulated adapter (Intel 21140 PCI) that is available for guests who cannot use integrated services or must have connectivity to the physical network to download and install pre requisites to be able to use integrated services (e.g. Windows XP x86 must install service pack 3)

- **Network adapter**

It is a synthetic device that can be used by non-enlightened guests only after installing integrated services. Enlightened guests are already equipped with the required components to be able to use this network adapter.

When creating a new virtual machine, the default configuration is the network adapter. If a Legacy Network Adapter has to be added, it can be done after the creation of the virtual machine. The legacy adapter can be added from the Hyper-V management interface by modifying the settings using the Add Hardware process.

- **Xen Network adapters**

Xen also provides two different types of virtual network adapters to its guests. One is for the para-virtual guest and the other is for enlightened or fully virtual guests. They are the emulated and para-virtual network adapters.

- **Emulated virtual adapters**

Emulated adapters are available to fully virtual and enlightened machines. Emulated adapter emulates a PCI Network interface card and by default provides three options as Realtek 8139, Intel e100/e1000 and AMD Pc net 32.
✓ **Para Virtual Adapters**

Para Virtual adapters have a higher-performance virtual network interface and are available by default to Para Virtual guests. They are also available to full virtual and enlightened guests but require special drivers.

- **Virtual network types in Hyper-V**

There are three network types in Hyper-V as:

i. **External network:** An external network is bound to a physical adapter in the parent partition in order to allow guest connectivity to a physical network. Only one external network can be bound to a physical adapter. If additional external networks are required, additional physical adapters have to be installed in the Hyper-V server. An External network is required to connect to resources like the Internet or other organizational resources that reside outside the parent partition. When an external connection is configured a brand new network connection is created, which unbinds all the protocols from the physical network card and binds the Microsoft Virtual Network Switch Protocol. This new network connection can be used by the parent partition to regain access to the physical network.

ii. **Internal Network:** The Internal Network provides connectivity between the guest, parent partition and other child partitions on the same Hyper-V server. In Virtual Server 2005R2, internal network was possible only with the installation and configuration of the Microsoft Loopback Adapter. Hyper-V does not need a loop back adapter. Like the External Network, the internal network also adds another network connection on the Networks Connections Interface. This connection can be configured on the same logical network as a virtual machine, providing connectivity between the Child and Parent partitions for exchanging data such as file transfers.

iii. **Private Network:** A private network provides connectivity between guests only. A private virtual network does not have external communication or communication with the parent partition. The private network does not add a network connection to the Networks Connections Interface.

- **Virtual Network Types in Xen**
Xen gives the administrator and the liberty to name the networks which preferred. By default, all virtual networks are named br\textit{n} where ‘\textit{n}’ stands for the number of the network, e.g. br0, br1, br2 and so on. The type of the network does not reflect in its name by default.

✓ **Bridged / Shared Interfaces**

A virtual network where all the virtual machines are connected the physical LAN is called a Bridged Network. In a simple bridged network the interfaces in the vHost are shared. By default, the name of a bridged network is br\textit{X} (where \textit{X} is the number of the shared interface). VMs appear to be on the same LAN as the VM server and are visible to the world outside. All traffic leaving the VM server and any VMs connected to the bridge travels across the bridge before going out on the wire.

✓ **I-bridged Network on Bonded Interface**

Here the bridge is attached to a bonded interface in the vHost. The difference between a bridged network on a bonded interface and a normal bridged network is that the bridged network on the bonded interface can take advantage of NIC failover and/or aggregation.

✓ **Shared Interfaces**

By default, the name of a shared interface in the vHost is eth\textit{X} (where \textit{X} is the number of the shared interface). Virtual Networks with shared interfaces have the same features and behavior as normal bridged networks. Here the physical interface is renamed as peth\textit{X} and the bridge is named eth\textit{X}. This is useful if applications expect an interface to named eth\textit{X}.

✓ **Bridges with VLANs**

Bridged virtual networks can also be attached to VLANs. Bridges can also be attached to VLANs that have been created on bonded network interfaces.

✓ **Host-only networks**

When virtual machines can only see each other and the VMServer in a virtual network, it is called a host-only network. In a host-only network a bridge is treated
as a network interface in the vHost, but it is not connected to a physical LAN. VMs connected to the host-only network can communicate with each other and the vHost but not with the outside world, and the VMS are not visible to the outside world.

✔ Route/NAT

Virtual machines can only see each other and the VMServer in this network. A routed or NAT Network works like a host-only network, but IP forwarding and optionally masked has been enabled in the kernel and IP tables. The VMs connected to the NAT Network can communicate with each other, the vHost and the outside world through NAT routing in Dom0.

4.2.1.5 Virtual storage

When multiple network storage devices are pooled into what appears to be a single storage device which is managed from a central console is called a Virtual Storage. Physical disks are passed onto virtual machines in many ways. We will look at how Xen and Hyper-V pass on physical disks to VMs.

Xen has two methods of passing disks to its virtual machines.

- **Xen Virtual Disks (xvd):**
  Storage devices other than tape drives are passed into the guest as Xen Virtual disks. Xen Virtual Disks do not support removable media. So if an optical drive is passed to a guest as an xvd, it cannot be ejected. However, Xen Virtual Disks are hot pluggable and can be removed and added while the guest is running. In Linux, these disks appear as a new type of block device and not as IDE or SCSI. In Windows, they appear as IDE disks and as SCSI disks if the Virtual Machine Driver Pack drivers are installed. Disk image files can be passed to a guest only as a xen virtual disk (xvd). The disk image xvd will have the same features and limitations on the guest OS as the physical device xvd. The disk image formats supported by Xen as xen virtual disks (xvd) are raw disk images, QEmu Copy-on-write (qcow2) disk images and VMware disk images (vmdk).

- **SCSI:**
Xen pass's storage devices as an SCSI device to a virtual machine using a feature called Para Virtual SCSI (PVSCSI). PVSCSI is currently supported only by Linux guests on the Xen host. A PVSCSI driver has yet to be written for a Windows guest. With PVSCSI any device registered as SCSI on Dom0 can be passed on to a guest as an SCSI device. All the features of the SCSI device will be available to the guest. A virtual SCSI host bus adapter is loaded in the guest, and the physical SCsIs are attached to it when they are being passed through the guest. PVSCSIs are also hot pluggable and can be attached and removed from a guest while it is still running. Devices that can be passed through as PVSCSI devices are CD/DVD drives, ROM drives, Entire disks (IDE, SATA, SCSI, USB, and FireWire), SAN LUNs and tape drives.

However, it is recommended that disks be passed through to the guests as Xen Virtual Disks rather than PVSCSI devices. This feature is typically used to pass tape drives through to the guests.

Hyper visors are an important part of cloud computing, and it is the hyper visors that make virtualization possible. Virtualization allows for backup and restoration without downtime and accelerates scalability.

### 4.2.2 Physical IaaS

The Physical Infrastructure-as-a-Service now available in the market, fall into the manual server allocation category. This means that every request to increase or decrease resources assigned to a client is manually implemented, which means it will take a few days before the changes take place. However, Fujitsu Laboratories has come up with a platform that is a prototype which will make the implementation of physical IaaS as simple and easy as Virtual IaaS. Fujitsu Laboratories has run a test of the new technology successfully with 48 servers and 512 hard disk drives and solid state drives. They could configure physical servers, including operating system installations within a ten-minute time frame. When hardware is becoming cheaper and smaller by the day, new technologies like the Fujitsu platform can reduce the cost of setting up IaaS by replacing the extremely expensive hyper visors that dominate the scene today (http://www.fujitsu.com).
4.3 Location
As Infrastructure-as-a-Service is made accessible for a system like the Internet, the administration supplier has the freedom to set up shop in any piece of the world that is helpful. The comfort can be in numerous structures like nearness to power source, lower base expenses like rent and area cost, harmonious climatic conditions that will diminish the expense for aerating and cooling and to wrap things up government approaches that advance the business. Area of the administration supplier is to a great degree critical to both the administration supplier and the customer as the laws of the area representing the physical area of the IaaS are appropriate to both administration supplier and customer.

4.4 Security and Legal Issues
- Despite the fact that distributed computing has numerous profits; any office with machine capacity may be likewise exceptionally helpless. The adequacy and the soundness furnished with customary routines for securing a framework are not relevant to this new framework and accordingly, the likelihood of following it lawfully or unlawfully stances to be an issue. On the other hand, the measures pertinent in an imparted large number security centralized server can be relevant to cloud security additionally.
- Control over the private cloud gear is more secure than when the supplies are offsite or in the control of another person. Physical control in the terms of reviewing the information connections, access port and visual review of other information connections ought not to be traded off. Inner and outer associations, in any case, are uncomfortable still about the outside administration of the security based administrations. There is each possibility of the information connections and the right to gain entrance ports being traded off and everybody will say that nobody did it!

The security issues have been ordered as indicated by the worry as: SeNISTive data access
- Data segregation
- Privacy
- Bug exploitation
- Recovery
• Accountability
• Malicious intruders
• Management console security
• Account control
• Multi tenancy issues

The good news is that for every category, there is a solution that is viable and usable and secure. It could be the use of cryptography or the use of public-key infrastructure, or the use of multiple cloud providers, or standardization of API’s, improving virtual machine support and legal support. The threat of data compromise is the largest of all the threats that seem to make most people diffident. There have been losses so far and some remain uncovered yet but the stakeholders need to invest heavily in securing the risk assessment of not only the infrastructure but also the theft of data, which could prove costly and render the cloud effectively incompatible with the risks that exist. The security aspect needs consideration and effective solutions that will help in the sustainability of the security system and it’s applications.

With any new technology, there come the issues of trademark, infringement, security concerns and sharing of data resources.

One legal problem that has come up with cloud computing is who owns the data that is stored in the cloud. If the cloud company is the possessor of the data that it has possession rights but if the cloud company is only a custodian then a different set of legal principles may apply.

Another problem is the legal ownership of the data. Many companies have remained silent about it in their agreements because this grey area is not defined as beneficial for both the parties like service provider and service purchaser.

• The other problem is if the cloud provided closes down, for any reason, then what is the status of the data and what is the legal standing of the data?
• What happens when there is a data theft? Who will be held accountable, the service purchaser or the cloud provider or a third party?

These are some of the security and legal concerns that are left open to interpretation on a case by case basis. The topographical boundaries that the cloud path traverses
make it necessary for the legal issues to be defined clearly and not left to interpretation. The danger of being left to interpretation would be the suggestion of the U.S. Government telling their citizens to place all their property and asset's data and the cloud and effectively lose it’s ownership because of the legal issues not being made clear, and the US would access all that data to suit it’s purpose and infringe on the fundamental rights of privacy of the American citizens.

This is one of the examples that have led most countries to determine the solutions and have definite answers to these variables and then bring the cloud computing into effect.

The security issues faced by IaaS are different from the issues faced by PaaS or SaaS. However, the security issues of the three services cannot be divided into watertight compartments and there are areas where the issues overlap the distinct tiers of cloud computing. Security in IaaS has to be implemented on six different levels starting from the physical hardware level to the Service Level Agreement (SLA), and the tightness of the security will depend on the sensitivity of the data that is being stored, used or transferred. Data has to be protected in all its three states of its existence. Damage or loss of data can happen from the client’s or service provider’s side. It is the Service Level Agreement (SLA) that defines the extent of responsibility from the provider’s side and the boundaries of the responsibility. SLAs are negotiable and will vary from client to client. However, the areas of concern remain the same irrespective of whose shoulder the responsibility lies on. For example, a client may choose to be responsible for the backup of data in order to reduce charges that need to be paid to the service provider (Patel P. A., 2009) (Service Level Agreement Definition and Contents). We will have a brief look at the six areas of concern.

- **Hardware:** Data on the hardware and services provided can be compromised by:
  
  i. *Physical damage of the drives:*

  Physical damage can be caused by various reasons which can be intentional or unintentional. Natural calamities, accidents and faulty drives can be classified as unintentional damage or loss and theft can be classified as intentional damage. Some of the measures against
these problems are insurance, highly secured areas for the drives and installing monitoring devices.

ii. **Unauthorized access to the data:** Data can be accessed physically or through the network. As long as the access is authorized, the data is secure. Unauthorized access to data on the physical drives can be prevented to a certain extent by encryption of data, security policies, and architecture implemented on the network.

- **Virtualization Layer:** At this level, security can be breached from the host and the virtual machines. The different kinds of the problem raised at this level cannot only affect data but also the services provided by IaaS. Security breach at this level can be protected, to a certain extent, by keeping an eye on events through event logs, monitoring processes, setting up different levels of permissions, encryption and implementing firewalls.

- **Network and Internet Connectivity:** If networks and the Internet connectivity are not implemented properly, access to sensitive areas for miscreants will be quite easy. Some of the measures that can be taken are again traffic encryption, network monitoring, implementing intrusion detection and prevention systems (IDPS) and last but not least segmentations of the logical network and implementing firewalls.

- **Cloud Software:** As ownership and responsibility of software and hardware are in different hands in IaaS, decoupling of applications from middleware is generally done by using the Metadata framework. Threats through the metadata framework can be checked by verifying metadata signature and encryption of metadata.

- **Utility Computing:** Discrepancies can happen when there are multiple levels of providers of the same service. An example of multiple levels of providers is Amazon’s DevPay5, which allows the second-level provider to meter the usage of AWS and meter the user according to the prices determined by the user in the SLA. In such cases management becomes, more complex and monitoring is required from both level providers to prevent unauthorized access to services that may go undetected from both sides and may affect the efficiency of the system. Steps to avoid this are cloud metering and billing software.
• **Service Level Agreements**: Service Level Agreements are the backbone of Cloud Security. Allowing for audit ability and monitoring and clearly defining responsibility and boundaries of both service provider and client can go a long way to provide ample security for IaaS or any of the services.

4.5 Billing

Measured service being an essential characteristic of cloud computing, it is only natural for IaaS to bill according to the resources used by the client. Distinct Service providers have different measures of billing. There is no uniform practice in billing methods and level of transparency among the service providers. At the moment, there is no formal organization to ensure standard practices for service providers (http://iaesjournal.com).

However, there are many software providers with billing software specifically designed for IaaS.

4.5.1 Factors To Be Considered When Billing In IaaS

- **Customer**: A customer can be an individual, an enterprise, a government agency, an organization, an enterprise project, or a department. The ‘customer’ description will have to be defined and redefined over time as the ‘customer’ is a volatile entity. For example, departments can get merged. Individual may become part of an organization and so on. Usage data will have to be measured per customer.

- **CPU usage**: Charges for CPU usage are based on power consumed, number of CPU cores used and the capacity and quality of the CPUs. Power consumption charges will vary according to time zones, and the peak and off-peak charges will be applicable.

- **Server Type**: Quality of the server who may be low-cost or high end in which the CPU is deployed have significantly different costs, which have to be reflected in the customer price.

- **System Administration**: The cost of the operating system on the server will also add to or reduce the charges for the customer. (E.g. Windows and Linux)

- **Storage**: The different storage capacities and the distinct storage types made available by the service provider and chosen by the customer will also reflect in the price and the customer has to pay per use.
• **Disaster recovery:** In the event of a disaster, the extent of recovery required by the customer will decide the additional charges on this front as a backup will have to be kept or created at a different location so that the service will continue smoothly even in the event of a disaster.

• **Other Charges:** Expenses for maintaining security and networking capacity of the IaaS are usually built in to the infrastructure pricing. This means the transparency in these areas is quite low and more opaque.

• **Service Level Agreement:** Service Level Agreement (SLA) defines the boundaries of responsibility between customer, service provider and the level of service to be expected by the customer from the service provider. If extremely high levels of services are expected, the additional costs for maintaining the standards will reflect in the charges per customer.

We can see that all the eight factors that influence the price of service provided will mutually influence each other too. Furthermore, how each aspect is measured and calculated will affect the price to be paid by the customer. Different comparisons between Amazon’s EC2, Microsoft Azure’s, other virtual IaaS provider's pricing and services provided will give a better insight into Virtual IaaS. A few facts have to be kept in mind when reading the details.

The processor core and memory assigned are all virtual instances of a common hardware. So the performance will not be the same as actually having the same amount of physical hardware assigned.

The table 4.1 given below gives a brief comparison of the features and services provided by Amazon EC2 and Microsoft Azure.
Table 4.1 Comparison of the Features and Services Provided by Amazon EC2 and Microsoft Azure

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Features</th>
<th>Amazon RDS</th>
<th>SQL Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Supported Database / databases</td>
<td>My SQL, SQL Server, Oracle</td>
<td>SQL</td>
</tr>
<tr>
<td>2</td>
<td>Provisioned IOPS Storage</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>Database Sizes</td>
<td>100GB to 1TB</td>
<td>1GB to 150GB</td>
</tr>
<tr>
<td>4</td>
<td>Backup / Restore</td>
<td>Turned on by default and backup is available within the retention period of 35 days.</td>
<td>Taking backup is done manually by the user by making a copy of the database or exporting the files from the files using BACPAC.</td>
</tr>
<tr>
<td>5</td>
<td>Pricing</td>
<td>Charges are based on the deployment model chosen by the customer.</td>
<td>Charges are based on storage space used.</td>
</tr>
<tr>
<td>6</td>
<td>Disaster recovery</td>
<td>Automatic</td>
<td>Manual</td>
</tr>
<tr>
<td>7</td>
<td>Additional Supporting tools</td>
<td>Not available</td>
<td>Silver light Database is available with which customer can easily and simply, create, delete and add data and also create stored procedures.</td>
</tr>
<tr>
<td>8</td>
<td>Database features supported</td>
<td>All features of MySQL supported</td>
<td>Only Subsets of features provided by SQL Server supported.</td>
</tr>
<tr>
<td>9</td>
<td>Renaming of database instances</td>
<td>Supported</td>
<td>Can be done with queries.</td>
</tr>
<tr>
<td>10</td>
<td>Automatic Software patching</td>
<td>Deployed instances are automatically updated with latest patches.</td>
<td>Software patching done automatically</td>
</tr>
<tr>
<td>11</td>
<td>Database snapshots</td>
<td>Supported automatic</td>
<td>Supported manual</td>
</tr>
<tr>
<td>12</td>
<td>Automatic host replacement</td>
<td>Compute instance gets replaced automatically in case of hardware failure.</td>
<td>Manual</td>
</tr>
</tbody>
</table>
The table 4.2 given below gives a price comparison based on memory, storage, availability, and compensations provided between six prominent Virtual IaaS providers.

Table 4.2 Price Comparisons Based On Memory, Storage, Availability and Compensations Provided Between Six Prominent Virtual IaaS Providers

<table>
<thead>
<tr>
<th>Factors</th>
<th>Amazon AWS</th>
<th>Microsoft Azure</th>
<th>Google Compute Engine</th>
<th>Rack Space</th>
<th>IBM Smart Cloud</th>
<th>HP Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPUs</td>
<td>1-8</td>
<td>1-8</td>
<td>1-8</td>
<td>1-8</td>
<td>1-16</td>
<td>1-8</td>
</tr>
<tr>
<td>Memory</td>
<td>613 MB - 68.4 GB</td>
<td>1.7GB - 14GB</td>
<td>73.7GB - 52GB</td>
<td>512 MB-30 GB</td>
<td>2 GB-16 GB</td>
<td>1 GB - 32 GB</td>
</tr>
<tr>
<td>Cost/hr</td>
<td>Free - $4.60</td>
<td>$0.06 - $2.04</td>
<td>$0.145 - $1.375</td>
<td>$0.022 - $1.20 (Linux)</td>
<td>Given in cost estimator</td>
<td>$0.035 - $1.01 (Linux)</td>
</tr>
<tr>
<td>Storage Costs</td>
<td>$ 0.095 GB/mo (S3)</td>
<td>$0.095</td>
<td>$0.10 GB/mo</td>
<td>$0.15GB/mo</td>
<td>Given in cost estimator</td>
<td>$0.1 GB/mo</td>
</tr>
</tbody>
</table>

The above table 4.2, it gives evident that profit lies in the method of portioning the chargeable units of the hardware offered as service. The units and portion size varies from provider to provider. The processor and memory mentioned is virtual. It means that their actual performance is not reflected in the pricing.