University of Technology
الجامعة التكنولوجية

Computer Science Department
قسم علوم الحاسوب

Computer & Cyber Security Branch
Fourth year – First Course
Subject: - Cloud Computing Security
2024-2025

by

Prof. Dr. Ekhlas Khalaf

اعداد:- ا.د عبير طارق

cs.uotechnology.edu.iq

Cloud Computing Security 1st course

1. Fundamentals of Cloud Computing and Architectural Characteristics

- Understand what is Cloud computing
- Architectural and Technological Influences of Cloud Computing
- Understand the Cloud deployment models a. Public, Private, Community and Hybrid models
- Scope of Control a. Software as a Service (SaaS) b. Platform as a Service (PaaS) c. Infrastructure as a Service (IaaS)

2. INFRASTRUCTURE SECURITY

- Infrastructure Security: The Network Level
- Infrastructure Security: The Host Level
- Infrastructure Security: The Application Level
- Understand the access control requirements for Cloud infrastructure

3. Secure Isolation of Physical & Logical Infrastructure

- Secure Isolation Strategies
- Multitenancy, Virtualization strategies, Virtualization Security ,Platform-to-Virtualization & Virtualization-to-Cloud
- Inter-tenant network segmentation strategies
- Storage isolation strategies

4. Security visualization for cloud computing

- security visualization and data security
- A security visualization standardization model
- Security visualization intelligence framework
- Security visualization intelligence model.

5 . DATA SECURITY AND STORAGE

- Understand the Cloud based Information Life Cycle
- Aspects of Data Security
- Data Security Mitigation 65
- Provider Data and Its Security

6. SECURITY MANAGEMENT IN THE CLOUD

- Security Management Standards
- Security Management in the Cloud
- Availability Management
- SaaS Availability Management
- PaaS Availability Management
- IaaS Availability Management
- Access Control
- Security Vulnerability, Patch, and Configuration Management

7. PRIVACY

- What Is Privacy?
- What Is the Data Life Cycle?
- What Are the Key Privacy Concerns in the Cloud?
- Who Is Responsible for Protecting Privacy?
- Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing

References

1. T. Mather, S.Kumaraswamy, and S. Latif, "Cloud Security and Privacy",1st edition,Copyright © 2009 ,Published by O'Reilly Media, Inc., USA.

2. Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler (Syngress/Elsevier),2011.

3. Vimal Kumar, Sivadon Chaisiri and Ryan Ko," Data Security in Cloud Computing",1st edition, Copyright © The Institution of Engineering and Technology,London,UK,2017.

Cloud Computing

1. Introduction

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations.

Why call it “cloud computing”?

Some say because the computing happens out there "in the clouds"

Examples of cloud services include online file storage, social networking sites, webmail, and online business applications.

Dropbox
box
amazon cloud drive
kindle
NETFLIX
You Tube
iBooks
a
S
in
SkyDrive
ebY
iCloud
tumblr
Y!
Instagram
f

Figure(1) examples of cloud services

- ➢ The cloud computing model allows access to information and computer resources from anywhere that a network connection is available.
- ➢ Cloud computing provides a shared pool of resources, including data storage space,

networks, computer processing power, and specialized corporate and user applications.

We do not need to install the part of the software on the local computer, and we have this is the way, which overcomes the cloud computing platform they are operating completely independent of any does not dependon the type of device or system that is used by the user to gain access to the computerized cloud. Thus, cloud computing makes our mobile applications and effective.

Figure 2, shows six phases of computing paradigms, from terminals/mainframes, to PCs, networking computing, to grid and cloud computing.

In phase 1, many users shared powerful mainframes using terminals.

Inphase 2, stand-alone PCs became powerful enough to meet the majority ofusers' needs.

In phase 3, PCs, laptops, and servers were connected together through local networks to share resources and increase performance.

In phase 4, local networks were connected to other local networks forminga global network such as the Internet to utilize remote applications and resources.

In phase 5, grid computing provides shared compute and storage resourcesdistributed across different administrative domain, Grid Computing is the starting point and basis for Cloud Computing.

In phase 6, cloud computing further provides shared resources on the Internet in a scalable and simple way. The client gets all or part of it according Pay As You Go.

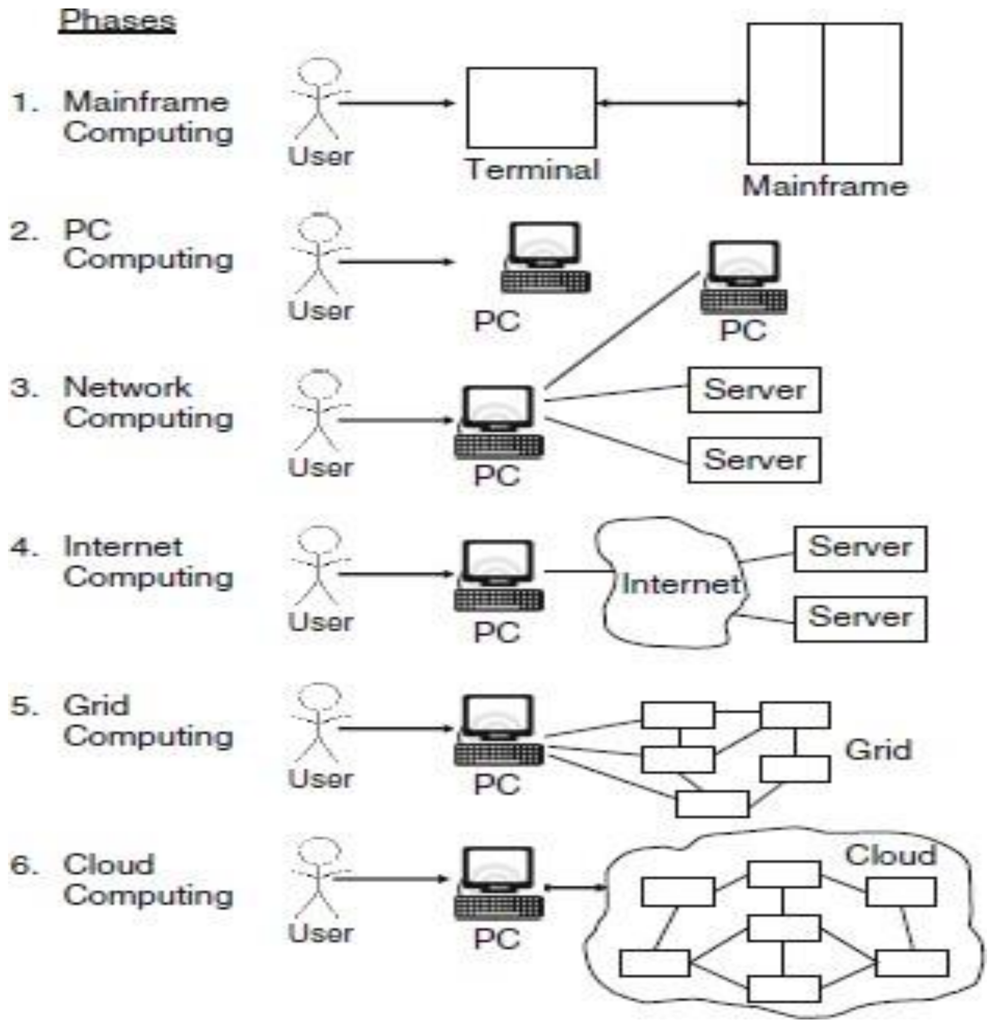


Fig.2 six computing paradigms

Cloud Computing Definition

Our definition of cloud computing is based on five attributes: multitenancy (shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources.

- ✓ ***Multitenancy (shared resources):*** Unlike previous computing models, which assumed dedicated resources (i.e., computing facilities dedicated toa single user or owner), cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level.

- ✓ ***Massive scalability:*** Although organizations might have hundreds or thousands of systems, cloud computing provides the ability to scale to tensof thousands of systems, as well as the ability to massively scale bandwidthand storage space.
- ✓ ***Elasticity:*** Users can rapidly increase and decrease their computing resources as needed, as well as release resources for other uses when theyare no longer required.
- ✓ ***Pay as you go:*** Users pay for only the resources they actually use and for only the time they require them.
- ✓ ***Self-provisioning of resources:*** Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources.

Figure 3 given the overview of cloud computing model.

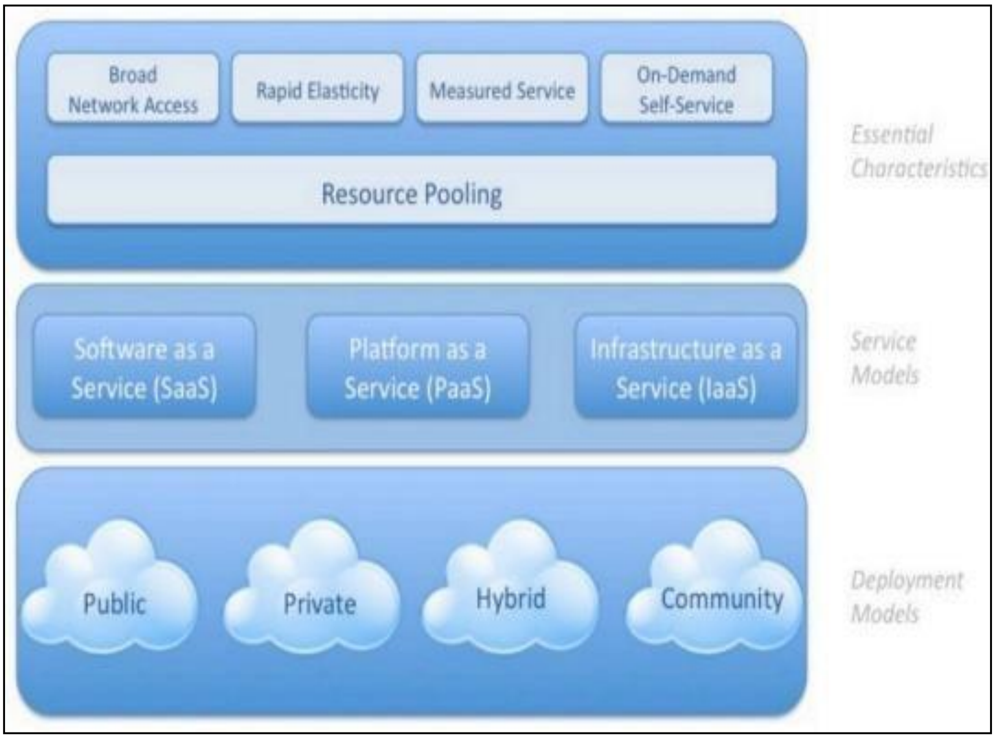


Figure 3 : overview of cloud computing model

Layers of cloud

Cloud computing can be viewed as a collection of services, which can bepresented as a layered cloud computing architecture, as shown in Figure 4. Cloud computing services are divided into five classes, according to theabstraction level of the capability provided and the service model ofproviders, namely: (1) Infrastructure as a Service, (2) Platform as a Service,and (3) Software as a Service (4) Virtualized computers (5) Data-Storage-as-a-Service

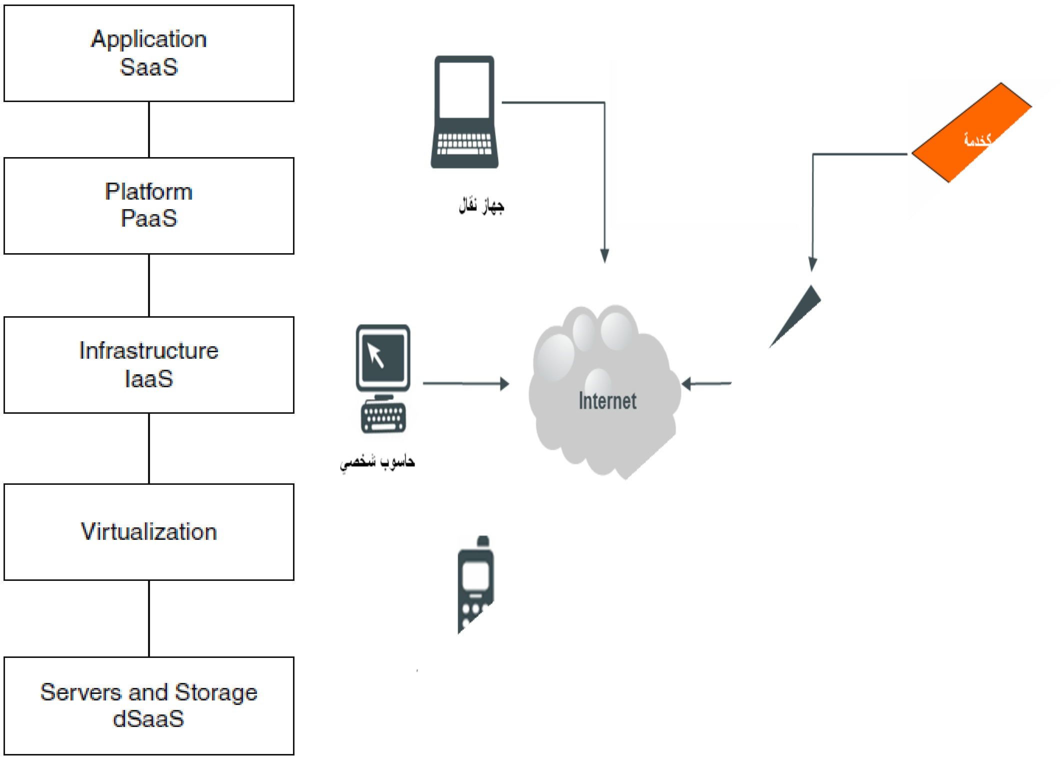


Figure 4 : layers of cloud computing

Types of Cloud Services (Cloud Layers):

Software as a Service (SaaS): Services offered through cloud computing usually include IT services, applications reside on the top of the cloud stack. Services by this layer can be accessed by end users through web portals. Therefore, consumers are increasingly shifting from locally installed computer programs to on-line software services that offer the same functionally. Traditional desktop applications such as wordprocessing and spreadsheet can now be accessed as a service in the web. This model of delivering applications, know as software as a service, alleviates the burden of software maintenance for customers and simplifies development and testing for providers.

Key benefits of a SaaS model include the following:

- SaaS enables the organization to outsource the hosting and managementof applications to a third party (software vendor and service provider) as ameans of reducing the cost of application software licensing, servers, and other infrastructure and personnel required to host the application internally.
- SaaS enables software vendors to control and limit use, prohibits copyingand distribution, and facilitates the control of all derivative versions of theirsoftware. SaaS centralized control often allows the vendor or supplier to establish an ongoing revenue stream with multiple businesses and users without preloading software in each device in an organization.
- Applications delivery using the SaaS model typically uses the one-to- many delivery approach, with the Web as the infrastructure. An end user can access a SaaS application via a web browser; some SaaS vendors

provide their own interface that is designed to support features that are unique to their applications.

- A typical SaaS deployment does not require any hardware and can run over the existing Internet access infrastructure. Sometimes changes to firewall rules and settings may be required to allow the SaaS application torun smoothly.
- Management of a SaaS application is supported by the vendor from theend user perspective, whereby a SaaS application can be configured usingan API, but SaaS applications cannot be completely customized. Examples :Gmail , Photoshop online , Google Docs, Microsoft: officeonline.

<u>Platform-as-a-Service (PaaS):</u> cloud platform offers an environment on which developers create and deploy applications and do not necessarily need to know many processors or how much memory that applications willbe using. In addition, multiple programming models and specialized services (e.g., data access, authentication) are offered as building blocks tonew applications. Paas, offers a scalable environment for developing and hosting web applications, which should be written in specific programming languages such as python or java, also includes operating systems and required services for a particular application.

PaaS platforms also have functional differences from traditional development platforms, including:

Multitenant development tools: Traditional development tools areintended for a single user; a cloud-based studio must support multiple users, each with multiple active projects.

Multitenant deployment architecture: Scalability is often not a concern of the initial development effort and is left instead for the system administrators to handle when the project deploys. In PaaS, scalability of the application and data tiers must be built-in (e.g., load balancing and failover should be basic elements of the developing platform).

Integrated management:Traditional development solutions (usually) are not associated with runtime monitoring, but in PaaS the monitoring ability should be built into the development platform.

Integrated billing:PaaS offerings require mechanisms for billing based onusage that are unique to the SaaS world.

Examples: Google AppEngine, window Azure, salesforce.com – Heroku.

PaaS Examples

amazon web services
salesforce.com Success On Demand.
Azure
Joyent
ca technologies
3tera
info@3tera.com
rackspace

Infrastructure-as-a-service(IaaS) offering virtualized resources (computation, storage, network, and communication) on demand, cloud infrastructure enables on demand provisioning of servers running several choices of operating system and a customized software stack. Infrastructure services are considered to be the bottom layer of cloud computing systems.

Features available for a typical IaaS system include:

- ***Scalability:***The ability to scale infrastructure requirements, such as computing resources, memory, and storage (in near-real-time speeds) based on usage requirements
- ***Pay as you go:*** The ability to purchase the exact amount of infrastructure required at any specific time
- ***Best-of-breed technology and resources:***Access to best-of-breed technology solutions and superior IT talent for a fraction of the cost Examples: op source.

Virtualized computers: - This layer forms the foundation of cloud technology. This enables user request for computing resources by accessing appropriate resources and deploy large numbers of virtual machines (VMs) on hardware (processors, memory, I/O devices).

Virtualization

The advantage of cloud computing is the ability to virtualized and share resources among different applications with the objective for better server utilization. In non-cloud computing three independent platforms exist for three different applications running on its own server. In the cloud, servers can be shared, or virtualized, for operating systems and applications resulting in fewer servers.

The main enabling technology for cloud computing environment is virtualization, virtualization is the heart of cloud computing, virtualization generalizes the physical infrastructure, which is the most rigid component,and makes it available as a soft component that is easy to use and manage, It allows abstraction and isolation of lower-level functionalities and underlying hardware, the concept of virtualization has been applied to all aspects of computing (memory, storage, processors, software, networks, as well as services).

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

Data-Storage-as-a-Service (SaaS) is a business model in which third- party providers rent space on their storage to end users. Provides storage that the consumer is used (bandwidth requirements).

Cloud Computing

Cloud computing Types or Deployment Models

Deployment models, with variation in physical location and distribution, a cloud can be classified as public, private, community, or hybrid.

1. **Public Cloud -**The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer todevelop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated withother deployment options.
   Example: Amazon, Google Apps, Windows Azure
2. **Private Cloud-**The cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may bein-house or with a third party on the premises. Computing architecture is dedicated to the customer and is not shared with other organizations. Example: eBay

Table (1): Public vs. private cloud

attributes	**public**	**private**
Infrastructure Owner	Third party (Cloud provider)	Enterprise
Scalability	Unlimited and On Demand	Limited to the installed Infrastructure
Cost	Lower cost	High cost including: space, cooling, energyand hardware cost
Performance	Unpredictable guaranteed performance	Guaranteed performance
Security	Concerns regarding data privacy	Highly secure

Enterprise computing, we mean the use of computers for data processing in large organizations, also referred to as 'information systems' (IS), or even 'information technology' (IT) in general.

3. Community Cloud

A Community Cloud is a semi private Cloud that is used by a defined group of enterprises with similar backgrounds and requirements can sharetheir infrastructures, thus increasing their scale while sharing the cost**.**

4. Hybrid Cloud

A composition of the two types (private and public) is called a Hybrid Cloud, where a private cloud is able to maintain high services availability by scaling up their system with externally provisioned resources from a public cloud when there are rapid workload actuations orhardware failures**.**

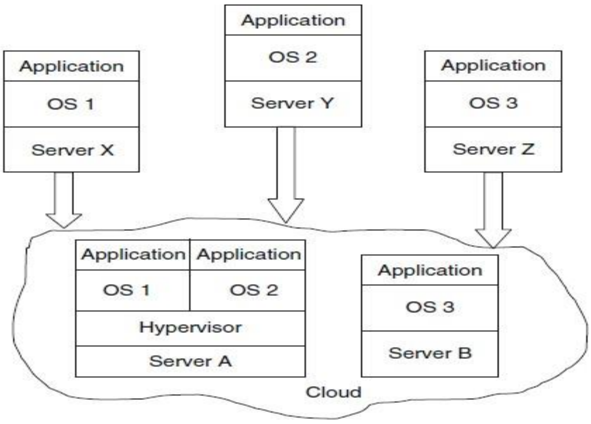
Enabling Technologies

Key technologies that enabled cloud computing are described in thissection; they include virtualization, Web service and service-oriented architecture, service flows and workflows

1- Virtualization

The advantage of cloud computing is the ability to virtualized and share resources among different applications with the objective for better server utilization. **In non-cloud computing three independent platforms exist for three different applications running on its own server.** In the cloud, servers can be shared, or virtualized, for operating systems and applications resulting in fewer servers.

Fig. 1.6 An example of virtualization: in non-cloud computing there is a need for three servers; in the cloud computing, two servers are used (adapted from Jones)



2- **Web Service and Service Oriented Architecture**

Web Services and Service Oriented Architecture (SOA) are not newconcepts; however they represent the base technologies for cloud computing. Cloud services are typically designed as Web services. A Service Oriented Architecture organizes and manages Web services insideclouds. A SOA also includes a set of cloud services, which are available on various distributed platforms.

3- **Service Flow and Workflows**

The concept of service flow and workflow refers to an integrated view of service based activities provided in clouds. Workflows have become one of the important areas of research in the field of database and information systems.

4- **Web 2.0 and Mashup**

Web 2.0 is a new concept that refers to the use of Web technology and Web design to enhance creativity, information sharing, and collaboration amongusers. On the other hand, Mashup is a web application that combines data from more than one source into a single integrated storage tool. Both technologies are very beneficial for cloud computing.

Cloud Computing Benefits

Cloud computing benefits can be categorized into:

- **Cost Reduction**: The consumer does not need to take the stress of updating the software and hardware as they can get the latest and updated resources and services relatively in less time.
- **Power Management**: It is easier to manage virtual server as compared tophysical server.
- **Scalability**: It is the one of the main positive aspects of cloud computing. If there is peak load or high traffic for a site, cloud can handle easily without need of any additional hardware infrastructure or equipments
- **Data Storage**: There are various data centers spread throughout the worldand it makes easy for the businesses to choose the datacenter as per their convenience to get fast and easy access of services with unlimited data storage.
- **Trouble shooting and Backup (Disaster) recovery**: Hardware failure can also be easily traced out and corrected . the assessment of data can be done anytime and is highly beneficial for the IT industry in reducing workloads and whenever data needs to be recovered.
- **Efficiency and reliability**: To find efficiencies many organizations are moving towards cloud and backup is another significant advantage tothe cloud and it maintains backup for all remote sites and branch offices.

Limitations of Cloud Computing

Following are some limitations of cloud computing:-

- ✓ **Data segregation:** As data of many users are stored in same data center and same server or same hard disks it will raise the question from the usersabout the problem of mismatch. How cloud securely isolate users and differentiate the memory and storage of each users as this failure could leadto leakage of information from one customer to another
- ✓ **The Offline cloud :** As cloud computing is fully dependent upon internet connection. If the customer has a problem with internet connection then he/she is unable to access the application or data from internet
- ✓ **Privacy:** Privacy is one of the major issues in cloud. Users are always concerned about their data so to overcome this issue provider should assurethe users in following points. First, Employees are aware of their responsibilities related to the confidentiality, integrity, availability of dataand information systems. Second, The confidential and/or personal client data including system access credentials are protected (e.g. encrypted) from unauthorized interception.
- ✓ **Software Licensing:** Many cloud providers relied heavily on open sourcesoftware because the licensing model for commercial software is not a good match to Utility Computing.
- ✓ **Security: Cloud** computing providers support encryption and identity management but still people do not want to place secrets in to the cloud.

Cloud Computing Features

Cloud computing brings a number of new features compared to othercomputing paradigms. There are briefly described:-

1. **Scalability and on-demand services**

Cloud computing provides resources and services for users on demand.The resources are scalable over several data centers.

2. **User-centric interface**

Cloud interfaces are location independent and can be accesses by well established interfaces such as Web services and Internet browsers

3. **Guaranteed Quality of Service (QoS)**

   Cloud computed can guarantee QoS for users in terms of hardware/CPUperformance, bandwidth, and memory capacity.

4. **Autonomous system**

   The cloud computing systems are autonomous systems managed transparently to users. However, software and data inside clouds can be automatically reconfigured and consolidated to a simple platform depending on user's needs.

5. **Pricing**

   Cloud computing does not require up-from investment. No capital expenditure is required. Users pay for services and capacity as they need them.

Challenges and Risks of cloud computing

The new paradigm of cloud computing provides a number of benefits and advantages over the previous computing paradigms and manyorganizations are adopting it. However, there are still a number of challenges, which are currently addressed by researchers and practitionersin the field they are briefly presented below.

✓ **Performance**

The major issue in performance can be for some intensive transaction- oriented and other data-intensive applications, in which cloud computing may lack adequate performance. Also, users who are at a long distance from cloud providers may experience high latency and delays.

✓ Security and Privacy

Companies are still concerned about security when using cloud computing.Customers are worried about the vulnerability to attacks, when informationand critical IT resources are outside the firewall. The solution for security assumes that cloud computing providers follow standard security practices.

✓ Data Lock-In and Standardization

A major concern of cloud computing users is about having their data locked-in by a certain provider. Users may want to move data and applications out from a provider that does not meet their requirements, there are efforts to create open standards for cloud computing.

✓ Resource Management and Energy-Efficiency

One important challenge faced by providers of cloud computing services is the efficient management of virtualized resource pools. Physical resources such as CPU cores, disk space, and network bandwidth must besliced and shared among virtual machines running potentially heterogeneous workloads.

✓ Bandwidth Costs

With cloud computing, companies can save money on hardware and software; however they could incur higher network bandwidth charges. Bandwidth cost may be low for smaller Internet-based applications, whichare not data intensive, but could significantly grow for data-intensive applications.

Virtualization

One of the most important ideas behind cloud computing is scalability, and the key technology that makes that possible is virtualization. Virtualization,in its broadest sense, is the emulation of one of more workstations/servers withina single physical computer. Put simply, virtualization is the emulation of hardware within a software platform. This allows a single computer to take on the role of multiple computers. This type of virtualization is often referred to asfull virtualization, allowing one physical computer to share its resources across a multitude of environments. This means that a single computer can essentially take the role of multiple computers. However, virtualization is not limited to the simulation of entire machines. There are many different types of virtualization, each for varying purposes.

One of these is in use by almost all modern machines today and is referred to as virtual memory. Although the physical locations of data may be scattered across a computers RAM and Hard Drive, the process of virtual memory makes it appear that the data is stored contiguously and in order. RAID(Redundant Array of Independent Disks) is also a form of virtualization along with disk partitioning, processor virtualization and many other virtualization techniques.

Virtualization allows the simulation of hardware via software. For this tooccur, some type of virtualization software is required on a physical machine. The most well-known virtualization software in use today is VMware. VMwarewill simulate the hardware resources of an x86 based computer, to create a fully functional virtual machine. An operating system and associated applications canthen be installed on this virtual machine, just as would be done on a physical machine. Multiple virtual machines can be installed on a single physical machine, as separate entities. This eliminates any interference between the machines, each operating separately. Although virtualization technology has been around for many years, it is only now beginning to be fully deployed. Oneof the reasons for this is the increase in processing power and advances in hardware technology. As the benefits of virtualization are realised, we can observe the benefits to a wide range of users, from IT professionals, to large businesses and government organizations.

There are four main objectives to virtualization, demonstrating the value offered to organizations:

1. Increased use of hardware resources;
2. Reduced management and resource costs;
3. Improved business flexibility; and
4. Improved security and reduced downtime.

Now we explain each objective with details as following:-

1. Increased use of Hardware Resources

With improvements in technology, typical server hardware resources arenot being used to their full capacity. On average, only 5-15% of hardware resources are being utilized. One of the goals of virtualization is to resolve this problem. By allowing a physical server to run virtualization software, a server's resources are used much more efficiently. This can greatly reduce both management and operating costs. For example, if an organization used 5 different servers for 5 different services, instead of having 5 physical servers, these servers could be run on a single physical server operating as virtual servers.

2. Reduced Management and Resource Costs

Due to the sheer number of physical servers/workstations in use today, most organizations have to deal with issues such as space, power and cooling. Not only is this bad for the environment but, due to the increase in power demands, the construction of more buildings etc is also very costly for businesses. Using a virtualized infrastructure, businesses can save large amounts of money because they require far fewer physical machines.

3. Improved Business Flexibility

Whenever a business needs to expand its number of workstations or servers, it is often a lengthy and costly process. An organization first has to makeroom for the physical location of the machines. The new machines then have tobe ordered in, setup, etc. This is a time consuming process and wastes abusiness's resources both directly and indirectly.Virtual machines can be easily setup. There are no additional hardware costs, no need for extra physical space and no need to wait around. Virtual machine management software also makes it easier for administrators to setup virtual machines and control access to particular resources, etc.

4. **Improved Security and Reduced Downtime**

When a physical machine fails, usually all of its software content becomesin accessible. All the content of that machine becomes unavailable and there is often some downtime to go along with this, until the problem is fixed. Virtual machines are separate entities from one another. Therefore if one of them fails or has a virus, they are completely isolated from all the other software on that physical machine, including other virtual machines. This greatly increases security, because problems can be contained. Another great advantage of virtualmachines is that they are not hardware dependent. What this means is that if a server fails due to a hardware fault, the virtual machines stored on that particularserver can be migrated to another server. Functionality can then resume as though nothing has happened, even though the original server may no longer beworking.

What is Virtualization in Cloud Computing?

Virtualization in Cloud Computing is making a virtual platform of serveroperating system and storage devices. This will help the user by providingmultiple machines at the same time it also allows sharing a single physical instance of resource or an application to multiple users. Cloud Virtualizations also manage the workload by transforming traditional computing and make it more scalable, economical and efficient. Virtualizations in Cloud Computing rapidly integrating the fundamental way of computing. One of the important features of virtualization is that it allows sharing of applications to multiple customers and companies.

Types of Virtualization

Server Virtualization

In server virtualization in Cloud Computing, the software directly installs on the server system and use for a single physical server can divide into many servers on the demand basis and balance the load. It can be also stated that the server virtualization is masking of the server resources which consists of number and identity. With the help of software, the server administrator divides one physical server into multiple servers.

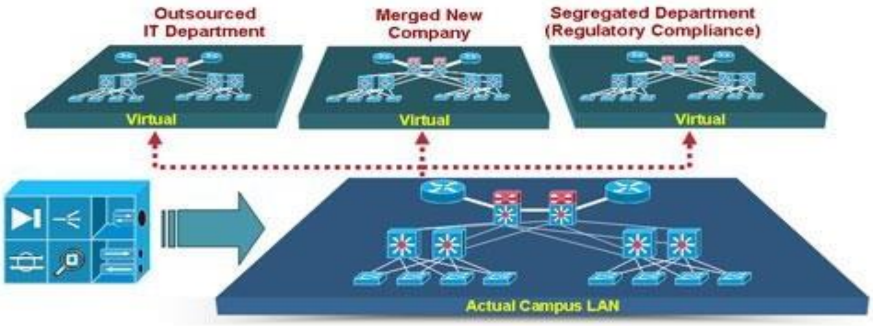
1. Hardware Virtualization

Hardware virtualization in Cloud Computing, used in server platform as it is flexibleto use Virtual Machine rather than physical machines. In hardware virtualizations, virtual machine software installs in the hardware system and then it is known as hardware virtualization. It consists of a hypervisor which use to control and monitorthe process, memory, and other hardware resources. After the completion of hardware virtualization process, the user can install the different operating system init and with this platform different application can use.

2. Network Virtualization

Network Virtualization is nothing but virtually pooling & managing all the available network resources such as IP’s, Switches, Routers, NIC’s, VLAN tags etc. via meansof tools such as routing tables in real time and each channel is independently secured and distinct from one another. For e.g. Virtual Private Network (VPN) allows us to create a virtual network over the internet without the use of actual wires or physicalhardware. Network virtualization can be categorized into two categories viz

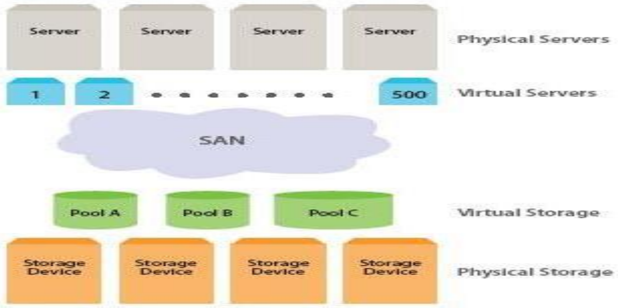
- **Internal** – Provides a network to a single system.
- **External** – Combines network array or parts of networks into a virtual unit.



3. Storage Virtualization

In storage virtualization in Cloud Computing, a grouping is done of physical storagewhich is from multiple network storage devices this is done so it looks like a single storage device. It can implement with the help of software applications and storage virtualization is done for the backup and recovery process. It is a sharing of the physical storage from multiple storage devices.

- **Block** – It replaces controllers and takes over at the disk level & works before the file system exists.
- **File** – The server that uses the storage must have the software installed on it in orderto enable file-level usage.

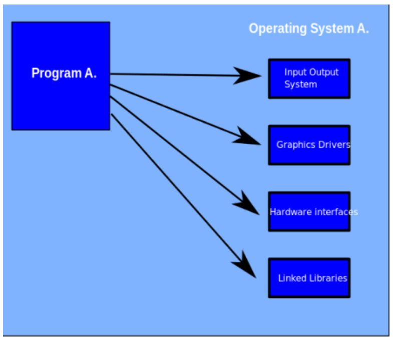


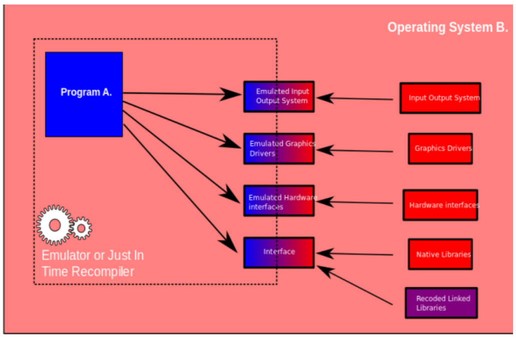
4. Application Server Virtualization

Application Server Virtualization also referred as ‘Advanced Load Balancing’ it enables IT departments to balance workloads of an application in an agile way. It spreads applications across servers and servers across applications. It also enables tomanage the servers as a single instance. ASV gives a better network securitycompliance as only one server is visible to the public while the rest are hidden behinda reverse proxy network security appliance.

5. Application virtualization

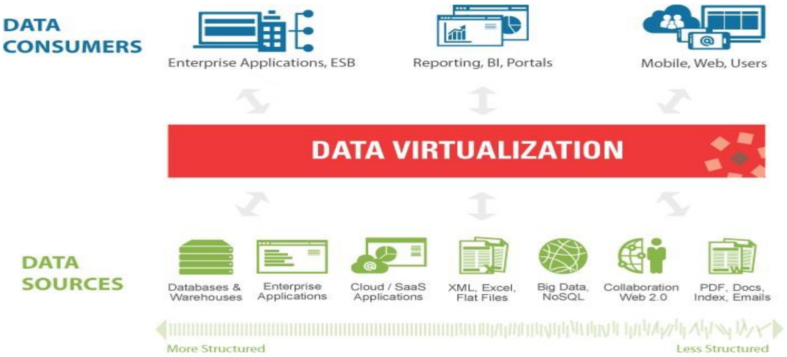
Application virtualization is the process by which a computer program iscompletely segregated from the underlying operating system. Whenever executed itbehaves as if it is directly interfacing with the original OS. Though it is nottraditionally installed on the system hardware and can be isolated or sandboxed as per convenience.





6. Data Virtualization

Data virtualization enables to decrease the data errors and workloads. It also enables to simply manipulate data, where is it physically located and how is it formatted.



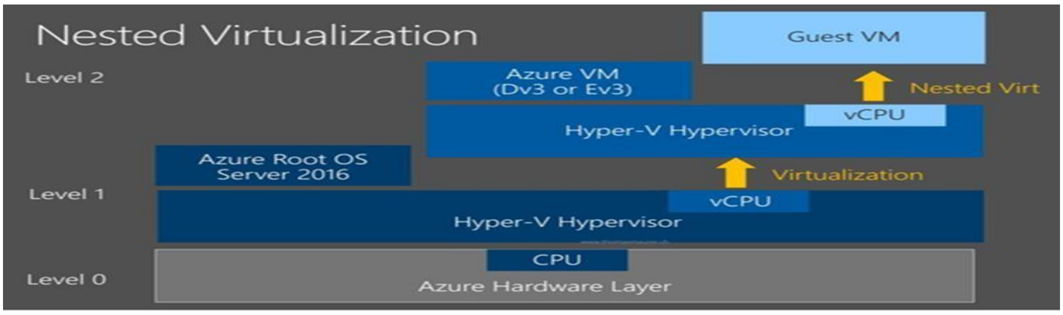
7. Desktop Virtualization

The Phrase ‘Work from Anywhere’ is practically possible because of Desktop Virtualization it provides work convenience and security. It enables us to remotely access the data from anywhere and anytime through any device. It provides a lot of flexibility and feasibility for employees and the data is safe and secure as it is storedat a centralized location.

Virtual Desktop Cloud
Thin Clients and Desktop PCs
Tablets and Smartphones
Laptops

8. Nested Virtualization

Nested Virtualization technology enables us to run one or more hypervisor withina virtual machine for e.g. we can create a virtual machine using hardware virtualization and deploy application virtualization within that virtual machine.



9. Memory Virtualization

Memory Virtualization is the process of aggregating & pooling the complete Random-Access Memory (RAM) resources from the network grid or cluster into a single memory pool. It provides a greater memory capacity and the disk drive also serves as an extension of the main memory.

Aspects of Data Security

With regard to data-in-transit, the primary risk is in not using a vetted encryption algorithm. Although this is obvious to information security professionals, it is not common for others to understand this requirement when using a public cloud, regardless of whether it is IaaS, PaaS, or SaaS. It is also important to ensure that a protocol provides confidentiality as well as integrity (e.g., FTP over SSL [FTPS], Hypertext Transfer Protocol Secure [HTTPS], and Secure Copy Program [SCP]) - particularly if the protocol is used for transferring data across the Internet. Although using encryption to protect data-at-rest might seem obvious, thereality is not that simple. If you are using an IaaS cloud service (public or private) for simple storage (e.g., Amazon's Simple Storage Service or S3), encrypting data-at-rest is possible— and is strongly suggested. However, encrypting data-at-rest that a PaaS or SaaS cloud-based application is using (e.g., Google Apps, Salesforce.com) as a compensating control is not always feasible. Data-at-rest used by a cloud-based application is generally not encrypted, because encryption would prevent indexing or searching of that data.

Data Security Mitigation

If prospective customers of cloud computing services expect that data security will serve as compensating controls for possibly weakened infrastructure security, since part of a customer's infrastructure security moves beyond its control and a provider's infrastructure security may (for many enterprises) or may not (for small to medium-size businesses, or SMBs) be less robust than expectations, you will be disappointed. Although data-in-transit canand should be encrypted, any use of that data in the cloud, beyond simple storage, requires thatit be decrypted. Therefore, it is almost certain that in the cloud, data will be unencrypted. Andif you are using a PaaS-based application or SaaS, customer-unencrypted data will also almost certainly be hosted in a multitenancy environment (in public clouds). Add to that exposure thedifficulties in determining the data's lineage, data provenance—where necessary—and even many providers' failure to adequately address such a basic security concern as data remanence,and the risks of data security for customers are significantly increased

Provider Data and Its Security

In addition to the security of your own customer data, customers should also be concerned about what data the provider collects and how the CSP protects that data. Specifically with regard to your customer data, what metadata does the provider have about your data, how is it secured, and what access do you, the customer, have to that metadata? As your volume of datawith a particular provider increases, so does the value of that metadata. Additionally, your provider collects and must protect a huge amount of security-related data. For example, at thenetwork level, your provider should be collecting, monitoring, and protecting firewall, intrusion prevention system (IPS), security incident and event management (SIEM), and routerflow data. At the host level your provider should be collecting system log files, and at the application level SaaS providers should be collecting application log data, including authentication and authorization information.

1. **Storage**

For data stored in the cloud (i.e., storage-as-a-service), we are referring to IaaS and notdata associated with an application running in the cloud on PaaS or SaaS. The same three information security concerns are associated with this data stored in the cloud (e.g., Amazon'sS3) as with data stored elsewhere: confidentiality, integrity, and availability.

2. **Confidentiality**

When it comes to the confidentiality of data stored in a public cloud, you have a potential concern. what access control exists to protect the data? Access control consists of both authentication and authorization. CSPs generally use weak authentication mechanisms (e.g., username + password), and the authorization ("access") controls available to users tendto be quite coarse and not very granular. For large organizations, this coarse authorization presents significant security concerns unto itself. Often, the only authorization levels cloud vendors provide are administrator authorization (i.e., the owner of the account itself) and userauthorization (i.e., all other authorized users)—with no levels in between (e.g., business unit administrators, who are authorized to approve access for their own business unit personnel). Protection of data stored in the cloud involves the use of encryption. If a CSP does encrypt a customer's data, the next consideration concerns what encryption algorithm it uses. Not all encryption algorithms are created equal. Cryptographically, many algorithms provide insufficient security. Only algorithms that have been publicly vetted by a formal standards body (e.g., NIST) or at least informally by the cryptographic community should be used. Any algorithm that is proprietary should absolutely be avoided. Note that we are talking about symmetric encryption algorithms here. Symmetric encryption (see Figure 1) involves the use of a single secret key for both the encryption and decryption of data. Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumesof data. It would be highly unusual to use an asymmetric algorithm for this encryption use case. (See Figure 2). Although the example in Figure 1 is related to email, the same concept isused in data storage encryption.

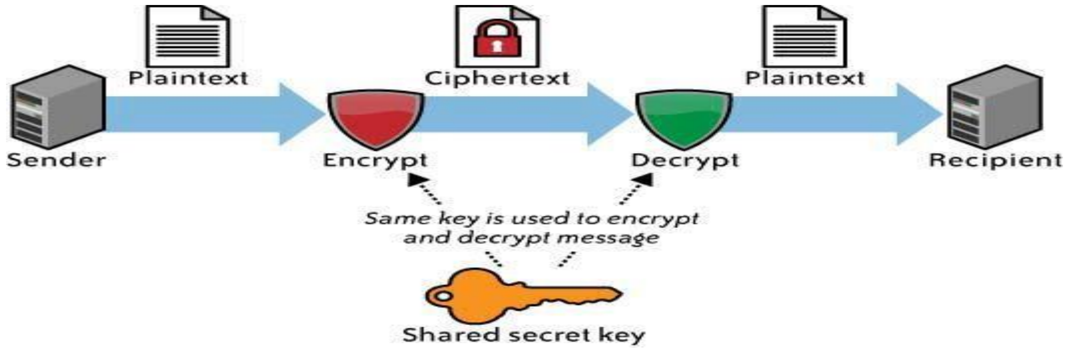


Figure 1 Symmetric encryption

Although the example in Figure 2 is related to email, the same concept is *not* used in data storage encryption

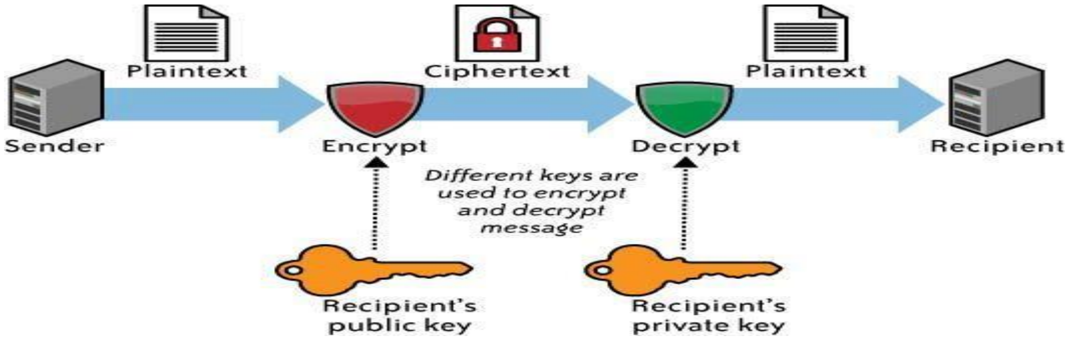


Figure 2 Asymmetric encryption

The next consideration for you is what key length is used. With symmetric encryption,the longer the key length (i.e., the greater number of bits in the key), the stronger the encryption. Although long key lengths provide more protection, they are also more computationally intensive, and may strain the capabilities of computer processors.

3. Integrity

for confidentiality purposes, and yet you might not have a way to verify the integrity of that data. Encryption alone is sufficient for confidentiality, but integrity also requires the use of message authentication codes (MACs). The simplest way to use MACs on encrypted data is to use a block symmetric algorithm (as opposed to a streaming symmetric algorithm) in cipher block chaining (CBC) mode, and to include a one-way hash function. This is not for the cryptographically uninitiated—and it is one reason why effective key management is difficult.

Another aspect of data integrity is important, especially with bulk storage using IaaS. Once a customer has several gigabytes (or more) of its data up in the cloud for storage,how does the customer check on the integrity of the data stored there? There are IaaS transfer costs associated with moving data into and back down from the cloud, as well as network utilization (bandwidth) considerations for the customer's own network. What a customer really wants to do is to validate the integrity of its data while that dataremains in the cloud—without having to download and re upload that data.

4. Availability

Assuming that a customer's data has maintained its confidentiality and integrity, youmust also be concerned about the availability of your data. There are currently three major threats in this regard—none of which are new to computing, but all of which takeon increased importance in cloud computing because of increased risk. The first threatto availability is network-based attacks. The second threat to availability is the CSP's own availability.

Security Management Standards

Based on the authors' assessment, the standards that are relevant to securitymanagement practices in the cloud are ITIL and ISO/IEC 27001 and 27002.

ITIL

The Information Technology Infrastructure Library (ITIL) is a set of best practices and guidelines that define an integrated, process-based approach for managing informationtechnology services. ITIL can be applied across almost every type of IT environment including cloud operating environment. ITIL seeks to ensure that effective information security measures are taken at strategic, tactical, and operational levels. Information security is considered an iterative process that must be controlled, planned, implemented, evaluated, and maintained. ITIL breaks information security down into:

Policies: The overall objectives an organization is attempting to achieve

Processes: What has to happen to achieve the objectives ***Procedures:*** Who does what and when to achieve the objectives***Work instructions:*** Instructions for taking specific actions

ISO 27001/27002

ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). It is also a certification standard and uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS. However, since ISO/IEC 27002 is merely a code of practice/guideline rather than a certification standard, organizations are free to select and implement controls as they see fit. The ITIL, ISO/IEC 20000, and ISO/IEC 27001/27002 frameworks help IT organizations internalize and respond to basic questions such as:

- How do I ensure that the current security levels are appropriate for your needs?
- How do I apply a security baseline throughout your operation?

Security Management in the Cloud

After analyzing the management process disciplines across the ITIL and ISO frameworks, the authors identified the following relevant processes as the recommended security management focus areas for securing services in the cloud:

- Availability management (ITIL)
- Access control (ISO/IEC 27002, ITIL)
- Vulnerability management (ISO/IEC 27002)
- Patch management (ITIL)
- Configuration management (ITIL)
- Incident response (ISO/IEC 27002)
- System use and access monitoring (ISO/IEC 27002)

TABLE 1. Relevant security management functions for SPI cloud delivery models in the contextof deployment models (private, public)

Cloud deployment/SPI	Public clouds	Private clouds
Software-as-a-service (SaaS)	Access control (partial) Monitoring system use andaccess (partial) Incident response	The following functions typically managed by your IT department or managed services: Availability management Access control Vulnerability management Patch management Configuration management Incident response Monitoring system use andaccess

Platform-as-a-service(PaaS)	The following are limited to customer applications deployed in PaaS (CSP is responsible for the PaaS platform): Availability management Access control Vulnerability management Patch management Configuration management Incident response Monitoring system use and access	

Infrastructure-as-a-service (IaaS)	Availability management (virtual instances) Access control (user and limited network) Vulnerability management (operating system and applications) Patch management (operatingsystem and applications) Configuration management (operating system and applications) Incident response Monitoring system use and access(operating system andapplications)	

Availability Management

Cloud services are not immune to outages, and the severity and scope of impact to the customer can vary based on the outage situation. Similar to any internal IT-supported application, business impact due to a service outage will depend on the criticality of the cloud application and its relationship to internal business processes. In the case of business-critical applications where businesses rely on the continuous availability of service, even a few minutes of service outage can have a serious impact on your organization's productivity, revenue, customer satisfaction, and service-level compliance

Factors Impacting Availability

The cloud service resiliency and availability depend on a few factors, including the CSP's data center architecture (load balancers, networks, systems), application architecture, hosting location redundancy, diversity of Internet service providers (ISPs), and data storagearchitecture. Following is a list of the major factors:

- SaaS and PaaS application architecture and redundancy.
- Cloud service data center architecture, and network and systems architecture, including geographically diverse and fault-tolerance architecture.
- Reliability and redundancy of Internet connectivity used by the customer and the CSP.
- Customer's ability to respond quickly and fall back on internal applications and other processes, including manual procedures.
- Customer's visibility of the fault. In some downtime events, if the impact affects a small subset of users, it may be difficult to get a full picture of the impact and can make it harder to troubleshoot the situation.
- Reliability of hardware and software components used in delivering the cloud service.
- Efficacy of the security and network infrastructure to withstand a distributed denial of service (DDoS) attack on the cloud service.
- Efficacy of security controls and processes that reduce human error and protect infrastructure from malicious internal and external threats, e.g., privileged users abusing privileges.

SaaS Availability Management

By virtue of the service delivery and business model, SaaS service providers are responsible for business continuity, application, and infrastructure security management processes. This means the tasks your IT organization once handled will now be handled by the CSP. Some mature organizations that are aligned with industry standards, such as ITIL, will be faced with new challenges of governance of SaaS services as they try to map internal.

service-level categories to a CSP. For example, if a marketing application is considered critical and has a high service-level requirement, how can the IT or business unit meet the internal marketing department's availability expectation based on the SaaS provider's SLA?In some cases, SaaS vendors may not offer SLAs and may simply address service terms viaterms and conditions.

PaaS Availability Management

In a typical PaaS service, customers (developers) build and deploy PaaS applicationson top of the CSP-supplied PaaS platform. The PaaS platform is typically built on a CSP owned and managed network, servers, operating systems, storage infrastructure, and application components (web services). Given that the customer PaaS applications are assembled with CSP-supplied application components and, in some cases, third-party web services components (mash-up applications), availability management of the PaaS application can be complicated-for example, a social network application on the Google App Engine that depends on a Facebook application for a contact management service. In that mashed-up software deployment architecture the onus of availability management is shared between the customer and the CSP. The customer is responsible for managing the availability of the customer developed application and third-party services, and the PaaS CSP is responsible for the PaaS platform and any other services supplied by the CSP. For example, Force.com is responsible for the management of the App Exchange platform, and customers are responsible for managing the applications developed and deployed on that platform.

IaaS Availability Management

Availability considerations for the IaaS delivery model should include both a computing and storage (persistent and ephemeral) infrastructure in the cloud. IaaS providersmay also offer other services such as account management, a message queue service, an identity and authentication service, a database service, a billing service, and monitoring services. Hence, availability management should take into consideration all the services that you depend on for your IT and business needs. Customers are responsible for all aspects ofavailability management since they are responsible for provisioning and managing the life cycle of virtual servers. Managing your IaaS virtual infrastructure in the cloud depends on five factors:

- Availability of a CSP network, host, storage, and support application infrastructure.
- Availability of your virtual servers and the attached storage (persistent and ephemeral)

compute services (e.g., Amazon Web Services' S3† and Amazon Elastic Block Store).

- ➢ Availability of virtual storage that your users and virtual server depend on for storage service. This includes both synchronous and asynchronous storage access use cases.
- ➢ Availability of your network connectivity to the Internet or virtual network connectivityto IaaS services.
- ➢ Availability of network services, including a DNS, routing services, and authentication services required to connect to the IaaS service.

Access Control

Access control management is a broad function that encompasses accessrequirements for your users and system administrators (privileged users) who access network, system, and application resources. The access control management functions should address the following:

- ✓ Who should have access to what resource? (Assignment of entitlements to users)
- ✓ Why should the user have access to the resource? (Assignment of entitlements based onthe user's job functions and responsibilities)
- ✓ How should you access the resource? (What authentication method and strength are required prior to granting access to the resource)
- ✓ Who has access to what resource? (Auditing and reporting to verify entitlementassignments)

Access Control in the Cloud

In the cloud, network access control manifests as cloud firewall policies enforcing host-based access control at the ingress and egress points of entry to the cloud and logical grouping of instances within the cloud. This is usually achieved using policies (rules) using standard Transmission Control Protocol/Internet Protocol (TCP/IP) parameters, including source IP, source port, destination IP, and destination port. In contrast to network-based access control, user access control should be strongly emphasized in the cloud, since it can strongly bind a user's identity to the resources in the cloud and will help with fine granular access control, user accounting, support for compliance, and data protection. User access management controls, including strong authentication, single sign-on (SSO), privilege management, and logging and monitoring of cloud resources, play a significant role in protecting the confidentiality and integrity of your information

in the cloud. The followingare the six control statements:

- Control access to information.
- Manage user access rights.
- Encourage good access practices.
- Control access to network services.
- Control access to operating systems.
- Control access to applications and systems.

Access Control: SaaS

In the SaaS delivery model, the CSP is responsible for managing all aspects of the network, server, and application infrastructure. In that model, since the application is delivered as a service to end users, usually via a web browser, network-based controls are becoming less relevant and are augmented or superseded by user access controls, e.g., authentication using a one-time password. Hence, customers should focus on user access controls (authentication, federation, privilege management, deprovisioning, etc.) to protect the information hosted by SaaS. Some SaaS services, such as Salesforce.com, augment network access control (e.g., source IP address/network-based control) to user access control in which case customers have the option to enforce access based on network and user policy parameters.

Access Control: PaaS

In the PaaS delivery model, the CSP is responsible for managing access control to the network, servers, and application platform infrastructure. However, the customer is responsible for access control to the applications deployed on a PaaS platform. Access control to applications manifests as end user access management, which includes provisioning and authentication of users.

Access Control: IaaS

IaaS customers are entirely responsible for managing all aspects of access control totheir resources in the cloud. Access to the virtual servers, virtual network, virtual storage, and applications hosted on an IaaS platform will have to be designed and managed by the customer. In an IaaS delivery model, access control management falls into one of the following two categories:

CSP infrastructure access control: Access control management to the host, network, and management applications that are owned and managed by the CSP.

Customer virtual infrastructure access control: Access control management to your virtual server (virtual machines or VMs), virtual storage, virtual networks, and applications hostedon virtual servers.

Security Vulnerability, Patch, and Configuration Management

The ability for malware (or a cracker) to remotely exploit vulnerabilities of infrastructure components, network services, and applications remains a major threat to cloud services. It is an even greater risk for a public PaaS and IaaS delivery model where vulnerability, patch, and configuration management responsibilities remain with the customer. Customers should remember that in cloud computing environments, the lowest or highest common denominator of security is shared by all tenants in a multitenant virtualenvironment. Hence, the onus is with the customers to understand the scope of their securitymanagement responsibilities. Customers should demand that CSPs become more transparent about their cloud security operations to help customers understand and plan complementary security management functions. The following sections discuss these VPC issues in the SPI delivery model context, and outline the VPC responsibilities for CSPs andtheir customers.

Security Vulnerability Management

Vulnerability management is an essential threat management element to help protecthosts, network devices, and applications from attacks against known vulnerabilities. Matureorganizations have instituted a vulnerability management process that involves routine scanning of systems connected to their network, assessing the risks of vulnerabilities to the organization, and a remediation process (usually feeding into a patch management program)to address the risks.

Security Patch Management

Similar to vulnerability management, security patch management is a vital threat management element in protecting hosts, network devices, and applications from unauthorized users exploiting a known vulnerability. Patch management processes follow achange management framework and feeds directly from the actions directed by your vulnerability management program. Security patch management mitigates risk to your organization by way of insider and outsider threats. Hence, SaaS providers should be routinely assessing new vulnerabilities and patching the firmware and software on all systems that are involved in delivering the SaaS service to customers. The scope of patch management responsibility for customers will have a low-to-high relevance in the order ofSaaS, PaaS, and IaaS services that is, customers are relieved from patch management dutiesin a SaaS environment, whereas they are responsible for managing patches for the whole stack of software (operating system, applications, and database) installed and operated on the IaaS platform. Customers are also responsible for patching their applications deployed on the PaaS platform.

Security Configuration Management

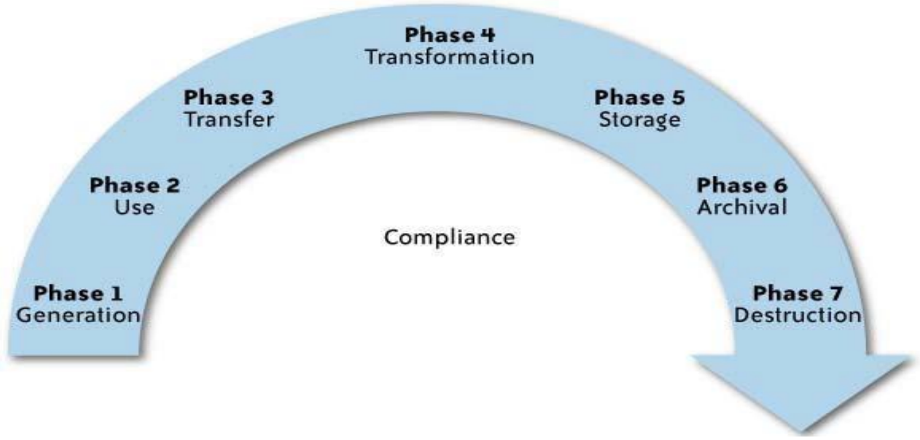
Security configuration management is another significant threat management practice to protect hosts and network devices from unauthorized users exploiting any configuration weakness. Security configuration management is closely related to the vulnerability management program and is a subset of overall IT configuration management.Protecting the configuration of the network, host, and application entails monitoring and access control to critical system and database configuration files, including OS configuration, firewall policies, network zone configuration, locally and remotely attachedstorage, and an access control management database.

What Is Privacy?

The concept of privacy varies widely among countries, cultures, and jurisdictions. Privacy rights or obligations are related to the collection, use, disclosure, storage, anddestruction of personal data (or personally identifiable information—PII). The privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization’s practice around personal information. Likewise, there is no universal consensus about what constitutes personal data.

What Is the Data Life Cycle?

Personal information should be managed as part of the data used by the organization. It should be managed from the time the information is conceived through to its finaldisposition. Protection of personal information should consider the impact of the cloud on each of the following phases as detailed in Figure 2.



The components within each of these phases are:

1. **Generation of the information**

✓ Ownership: Who in the organization owns PII, and how is the ownership maintained if the organization uses cloud computing?

✓ Classification: How and when is PII classified? Are there limitations on the use of cloud computing for specific data classes?

✓ Governance: Is there a governance structure to ensure that PII is managed and protected through its life cycle, even when it is stored or processed in a cloud computing environment?

2. Use

- ✓ Internal versus external: Is PII used only within the collecting organization, or is it used outside the organization (e.g., in a public cloud)?
- ✓ Third party: Is the information shared with third parties (e.g., subcontractors or CSPs)?
- ✓ Appropriateness: Is the use of the information consistent with the purpose for which it wascollected? Is the use within the cloud appropriate based on the commitments the organizationmade to the data subjects?
- ✓ Discovery/subpoena: Is the information managed in the cloud in a way that will enable the organization to comply with legal requirements in case of legal proceedings?

3. Transfer

- *Public versus private networks*: When information is transferred to a cloud is the organization using public networks, and is it protected appropriately? (PII should always be protected to address the risk level and legal requirements.)
- *Encryption requirements*: Is the PII encrypted? Some laws require that PII will be encrypted when transmitted via a public network (and this will be the case when the organization is using a public cloud).
- *Access control*: Are there appropriate access controls over PII when it is in the cloud?

4. Transformation

- *Derivation*: Are the original protection and use limitations maintained when data is transformed or further processed in the cloud?
- *Aggregation*: Is data in the cloud aggregated so that it is no longer related to an identifiable individual (and hence is no longer considered PII)?
- *Integrity*: Is the integrity of PII maintained when it is in the cloud?

5. Storage

- *Access control*: Are there appropriate controls over access to PII when stored in the cloudso that only individuals with a need to know will be able to access it?
- Structured versus unstructured: How is the data stored to enable the organization to access and manage the data in the future?
- Integrity/availability/confidentiality: How are data integrity, availability, and

confidentiality maintained in the cloud?

- Encryption: Several laws and regulations require that certain types of PII should be stored only when encrypted. Is this requirement supported by the CSP?

6. Archival

- *Legal and compliance*: PII may have specific requirements that dictate how long it should be stored and archived. Are these requirements supported by the CSP?
- *Off-site considerations*: Does the CSP provide the ability for long-term off-site storage thatsupports archival requirements?
- *Media concerns*: Is the information stored on media that will be accessible in the future? Isthe information stored on portable media that may be more susceptible to loss? Who controlsthe media and what is the organization’s ability to recover such media from the CSP if needed?
- *Retention*: For how long will the data be retained by the CSP? Is the retention period consistent with the organization’s retention period?

7. Destruction

- **Secur***e*: Does the CSP destroy PII obtained by customers in a secure manner to avoidpotential breach of the information?
- ***Complete*****:** Is the information completely destroyed? Does the destruction completely erasethe data, or can it be recovered?

What Are the Key Privacy Concerns in the Cloud?

Privacy advocates have raised many concerns about cloud computing. These concernstypically mix security and privacy. **Here are some additional considerations to be aware of:**

1. Access

Data subjects have a right to know what personal information is held and, in some cases, canmake a request to stop processing it. In the cloud, the main concern is the organization's ability to provide the individual with access to all personal information, and to comply with stated requests.

2. Compliance

What are the privacy compliance requirements in the cloud? What are the applicable laws, regulations, standards, and contractual commitments that govern this information, and who is responsible for maintaining the compliance? How are existing privacy compliance requirements impacted by the move to the cloud?

3. *Storage*

Where is the data in the cloud stored? Was it transferred to another data center in another country? Is it commingled with information from other organizations that use the same CSP?Privacy laws in various countries place limitations on the ability of organizations to transfer some types of personal information to other countries.

4. Retention

How long is personal information (that is transferred to the cloud) retained? Which retentionpolicy governs the data? Does the organization own the data, or the CSP? Who enforces the retention policy in the cloud, and how are exceptions to this policy (such as litigation holds) managed?

5. Destruction

How does the cloud provider destroy PII at the end of the retention period? How do organizations ensure that their PII is destroyed by the CSP at the right point and is not available to other cloud users? How do they know that the CSP didn't retain additional copies? Cloud storage providers usually replicate the data across multiple systems and sites— increased availability is one of the benefits they provide. This benefit turns into a challenge when the organization tries to destroy the data.

6. **Audit and monitoring**

How can organizations monitor their CSP and provide assurance to relevant stakeholders thatprivacy requirements are met when their PII is in the cloud?

7. **Privacy breaches**

How do you know that a breach has occurred, how do you ensure that the CSP notifies you when a breach occurs, and who is responsible for managing the breach notification process (and costs associated with the process)?

Who Is Responsible for Protecting Privacy?

There are conflicting opinions regarding who is responsible for security and privacy. Some publications assign it to providers; but although it may be possible to transfer liability via contractual agreements, it is never possible to transfer accountability. Ultimately, in the eyes of the public and the law, the onus for data security and privacy falls on the organizationthat collected the information in the first place—the user organization. This is true even if theuser organization has no technical capability to ensure that the contractual requirements withthe CSP are met. History and experience have proven that data breaches have a cascading effect. When an organization loses control of users' personal information, the users are responsible (directly or indirectly) for subsequent damages resulting from the loss. Identity theft is only one of the possible effects; others may include invasion of privacy or unwelcomesolicitation. When an affected individual is dealing with the fallout, he will likely blame the one who made the decision to use the service, as opposed to the provider of the service.

Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing

The following topics describe analysis of the potential impact of cloud computing on the key OECD and other common privacy principles.

1. Collection Limitation Principle

This principle specifies that collection of personal data should be limited to the minimum amount of data required for the purpose for which it is collected. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. In the privacy arena, lack of specifics on data collection with providers creates misunderstandings down the road. Many organizations want to do what theyperceive to be “the right thing”; however, their perception may be different from the law. Asa result, there may be different expectations regarding what privacy means between the organization and the CSP, and no agreed best practices. It is essential that service-level agreements (SLAs) are initially defined before any information is provided or shared, becauseit is very hard to negotiate them later.

2. Use Limitation Principle

This principle specifies that personal data should not be disclosed, made available, orotherwise used for purposes other than those with the consent of the data subject, or by the authority of law. Cloud computing places a diverse collection of user and business information in a single location. As data flows through the cloud, strong data governance is needed to ensure that the original purpose of collection and limitation on use is attached to the data. This is critical when organizations create a centralized database, because future applications can easily combine the data via expanded views that are utilized for new purposes never approved by data subjects.

3. Security Principle

Security is one of the key requirements to enable privacy. This principle specifies that personal data should be protected by reasonable security safeguards against such risks as lossor unauthorized access, destruction, use, modification, or disclosure of data.

4. Retention and Destruction Principle

This principle specifies that personal data should not be retained for longer than needed to perform the task for which it was collected, or as required by laws or regulations. Data shouldbe destroyed in a secure way at the end of the retention period. How long data should be retained and when it should be destroyed is still a challenge for most companies. Data growthhas led to definitions of policies and procedures for data retention and destruction.

5. Transfer Principle

This principle specifies that data should not be transferred to countries that don't provide thesame level of privacy protection as the organization that collected the information. In a cloud computing environment, infrastructure is shared between organizations; therefore, there are threats associated with the fact that the data is stored and processed remotely, and there is increased sharing of platforms between users, which increases the need to protect privacy of data stored in the cloud

6. Accountability Principle

This principle states that an organization is responsible for personal information under its control and should designate an individual or individuals who are accountable for the organization's compliance with the remaining principles. Accountability within cloud computing can be achieved by attaching policies to data and mechanisms to ensure that these policies are adhered to by the parties that use, store, or share that data, irrespective of the jurisdiction in which the information is processed.

7. Multi-Tenancy

Multi-tenancy is an architecture in which a single instance of a software applicationserves multiple customers. Each customer is called a tenant. Tenants may be giventhe ability to customize some parts of the application, such as the color of the userinterface (UI) or business rules, but they cannot customize the application's code. In a multi-tenant architecture, multiple instances of an application operate in ashared environment. This architecture is able to work because each tenant isintegrated physically, but logically separated; meaning that a single instance of the software will run on one server and then serve multiple tenants. In this way, asoftware application in a multi-tenant architecture can share a dedicated instance ofconfigurations, data, user management and other properties.

Multi-tenancy applications can share the same users, displays, rules although userscan customize these to an extent and database schemas, which tenants can also customize.

Importance of multi-tenancy

Multi-tenancy has seen a lot of could adoption and is used most with cloud computing. Multi-tenant architectures are found in both public cloud and private cloud environments, allowing each tenant's data to be separated from each other. For example, in a multi-tenant public cloud, the same servers willbe used in a hosted environment to host multiple users. Each user is given a separateand ideally secure space within those servers to store data. Multi-tenancy is also important for the scalability of public and private clouds, and has helped make multi-tenancy a standard. The multi-tenant architecture can also aid in providing abetter ROI for organizations, as well as quickening the pace of maintenance and updates for tenants.

Types of multi-tenant architecture

There are three main multi-tenancy model types, all with varying levels of complexity and costs. A single, shared database schema is a multi-tenancy model with a multi-tenant database. This is the simplest form out of the three and is a relatively low cost for tenants because of the use of shared resources. This form uses a single application and database instance to host tenants and store data. Usinga single, shared database schema allows for easier scaling; however, operational costs can be higher.

Another multi-tenant architecture includes the use of a single database with multiple schemas. This tenant system uses a single application instance with individual databases for each tenant. In addition, this architecture has a higher costwith more overhead with each database. It is a valuable architecture when data fromdifferent tenants need to be treated differently such as if they had to go through different geographic regulations.

The third type of multi-tenant architecture hosts data in multiple databases. This model is relatively complex in terms of management and maintenance, but tenantscan be separated by a chosen criteria

Advantages and disadvantages of multi-tenancy

Some advantages include:

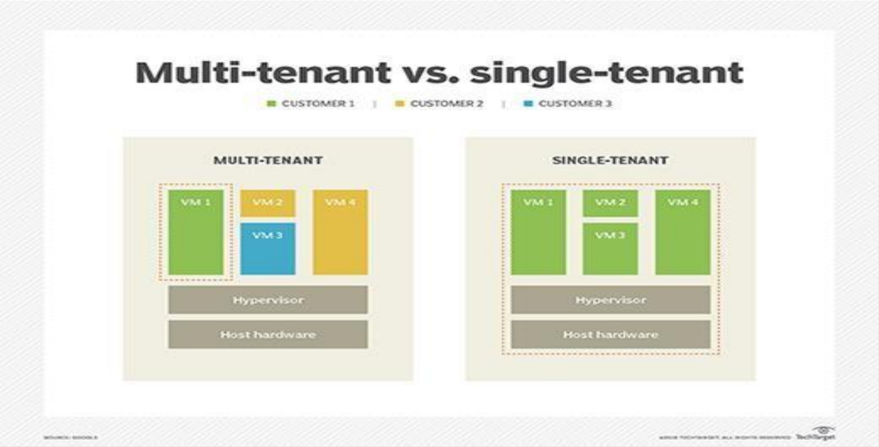
- ✓It is less expensive when compared to other tenant hosting architectures.
- ✓An offering of pay-for-what-you-need pricing models.
- ✓Tenants don't have to worry about updates, since they are pushed out by the host provider.
- ✓Tenants don't have to worry about the hardware their data is being hosted on.
- ✓Providers only have to monitor and administrate a single system.
- ✓The architecture is easily scalable.

Some disadvantages, however, that come with multi-tenancy include:

- Multi-tenant apps tend to be less flexible than apps in other tenant architectures,such as single-tenancy.
- Multi-tenancy is, in general, more complex than single-tenancy.
- Multi-tenant apps need stricter authentication and access controls for security.
- Tenants have to worry about noisy neighbors, meaning someone else on thesame CPU that consumes a lot of cycles, which may slow response time.
- Downtime may also be an issue depending on the provider.

Multi-tenant vs. single-tenant

Multi-tenancy can be contrasted with single-tenancy, an architecture in which each customer has their own software instance and may be given access to source code. In single-tenant architectures, a tenant will have a singular instance of a SaaS application dedicated to them, unlike multi-tenancy where there are shared services. Because each tenant is in a separate environment, they are not bound in the same way that users of shared infrastructure would be; meaning single-tenant architectures are much more customizable.



A comparison of multi-tenancy and single-tenancy architectures per customer.

Secure Separation / Isolation Strategies

Traditionally, IT administrators deployed dedicated infrastructure for their tenants. Deploying multiple tenants in a shared, common infrastructure optimizes resourceutilization at lower cost, but requires designs that address secure tenant separation to insure end-to-end path isolation and meet tenant security requirements. The following design considerations provide secure tenant separation and path isolation:

Network Separation

In order to address the need to support multi-tenancy while providing the same degree of tenant isolation as a dedicated infrastructure, the VMDC referencearchitecture uses path isolation techniques to logically divide a shared infrastructure into multiple (per-tenant) virtual networks. These rely on both data path and devicevirtualization, implemented in end-to-end fashion across the multiple hierarchical layers of the infrastructure and include:

➢ **Network Layer 3 (L3) Separation (core/aggregation layers)—**VRF-lite implemented at core and aggregation layers provides per tenant isolation at L3, with separate dedicated per-tenant routing and forwarding tables insuring that no inter- tenant (server to server) traffic within the data center will be allowed, unless explicitly configured. A side benefit of separated routing and forwarding instancesis the support for overlapping IP addresses; a required feature in the public cloud case or in merger or other situations involving IP addressing transitions in the private Enterprise case.

- **Network Layer 2 (L2) Separation (access, virtual access)—VLAN IDs** and the802.1q tag provide isolation and identification of tenant traffic across the L2 domain, and more generally, across shared links throughout the infrastructure.
- **Network Services Separation (services core, compute)—**On physicalappliance or service module form factors, dedicated contexts or zones provide the means for virtualized security, load balancing, NAT, and SSL offload services andthe application of unique per-tenant policies at the VLAN level of granularity.

Compute Separation

Traditionally, security policies were implemented at the physical server level. However, server virtualization and mobility introduce new security challenges andconcerns; in effect, in order to meet these challenges, policy must be implementedat the virtual machine level and be capable of following virtual machines as they move from host to host. Separation of per-tenant traffic in the compute layer of theinfrastructure leverages the following technologies:

- **VNICs**: In the highly virtualized data center, separation of traffic is accomplishedvia use of multiple vNICs, rather than physical NICs.
- **VLANs**: VLANs provide logical isolation across the L2 domain, including the Nexus 1000V virtual access switching domain within the compute tier of the infrastructure.

Storage Separation

In the VMDC reference architecture, separation of virtual machine data stores within the storage domain of the shared infrastructure is accomplished in the following ways:

- **Cluster File System Management**: the cluster file system management creates aunique Virtual Machine Disk per VM, insuring that multiple VMs cannot access the same VMDK sub-directory within the Virtual Machine File System (VMFS) volume and thus isolating one tenant's VMDK from another.
  - **LUN Masking**— Logical Unit Number (LUN) masking creates an authorizationprocess that restricts storage LUN access to specific hosts on the shared SAN.
  - **V Filers**: vFilers provide logical separation of NFS data stores. These may be correlated with IP addresses and used in combination with Application Tier Separation VLANs and ACL-based security policy enforcement to limit NFS datastore access to specific tenants or groups of tenants across the shared infrastructure.

Application Tier Separation

Many applications follow a three-tiered functional model, consisting of web, application, and database tiers. Servers in the web tier provide the public facing, "front-end" presentation services for the application, while servers in the application and database tiers function as the middleware and back-end processing components. Due to this functional split, servers in the web tier are typically considered to be likely targets of malicious attacks, with the level of vulnerability increasing in proportion to the scope of the user community. Applications that accessible over the public Internet represent a major security concern. Several methods exist for separation of application tiers:

1. **Network-Centric Method:** This method involves the use of VLANs within the L2 domain to logically separate each tier of servers.

   Server-Centric Method: This method relies on the use of separate VM vNICs