Unit - 05

Information storage on cloud

Unit 05/Lecture - 01

Cloud computing – [Rgpv /dec 2014(2), Rgpv/dec 2013(10), Rgpv/dec 2012(10)]

Cloud computing is a term used to refer to a model of network computing where a program or application runs on a connected server or servers rather than on a local computing device such as a pc, tablet or smartphone. Like the traditional client-server model or older mainframe computing,[1] a user connects with a server to perform a task. The difference with cloud computing is that the computing process may run on one or many connected computers at the same time, utilizing the concept of virtualization. With virtualization, one or more physical servers can be configured and partitioned into multiple independent "virtual" servers, all functioning independently and appearing to the user to be a single physical device. Such virtual servers are in essence disassociated from their physical server, and with this added flexibility, they can be moved around and scaled up or down on the fly without affecting the end user. The computing resources have become "granular", which provides end user and operator benefits including on-demand self-service, broad access across multiple devices, resource pooling, rapid elasticity and service metering capability.

In more detail, cloud computing refers to a computing hardware machine or group of computing hardware machines commonly referred as a server or servers connected through a communication network such as the internet, an intranet, a local area network (lan) or wide area network (wan). Any individual user who has permission to access the server can use the server's processing power to run an application, store data, or perform any other computing task. Therefore, instead of using a personal computer every time to run a native application, the individual can now run the application from anywhere in the world, as the server provides the processing power to the application and the server is also connected to a network via the internet or other connection platforms to be accessed from anywhere. all this has become possible due to increased computer processing power available to humankind with decreased cost .

In common usage the term "the cloud" has become a shorthand way to refer to cloud computing infrastructure. the term came from the cloud symbol that network engineers used on network diagrams to represent the unknown (to them) segments of a network. marketers have further popularized the phrase "in the cloud" to refer to software, platforms and infrastructure that are sold "as a service", i.e. Remotely through the internet. Typically, the seller has actual energy-consuming servers which host products and services from a remote location, so end-users don't have to; they can simply log on to the network without installing anything. The major models of cloud computing service are known as software as a service, platform as a service, and infrastructure as a service. These cloud services may be offered in a public, private or hybrid network. google, amazon, ibm, oracle cloud, rackspace, salesforce, zoho and microsoft are some well-known cloud vendors.

Cherecteristics – [Rgpv/dec 2012(10)]

Cloud computing exhibits the following key characteristics:

- **Agility** improves with users' ability to re-provision technological infrastructure resources.
- **Application programming interface** (API) accessibility to software that enables machines to interact with cloud software in the same way that a traditional user interface (e.g., a computer desktop) facilitates interaction between humans and computers. Cloud computing systems typically use Representational State Transfer (REST)-based APIs.
- **Cost**: cloud providers claim that computing costs reduce. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a

utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state-of-the-art repository[46] contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

- **Device and location independence** enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.
- **Maintenance** of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

- **Multitenancy** enables sharing of resources and costs across a large pool of users thus allowing for:
    - **centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
    - **peak-load capacity** increases (users need not engineer for highest possible load-levels)
    - **utilisation and efficiency** improvements for systems that are often only 10–20% utilised.
- **Performance** is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Productivity** may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.

- **Reliability** improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
- **Scalability and elasticity** via dynamic ("on-demand") provisioning of resources on a fine-

grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, os and cloud providers, without users having to engineer for peak loads.

- **Security** can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.
- **Virtualization** technology allows sharing of servers and storage devices and increased utilization. Applications can be easily migrated from one physical server to another

S.no	Rgpv question	Year	Marks
Q.1	What is cloud computing?Enlist and explain essential characteristics of cloud computing.	Dec 2014 Dec 2013 Dec 2011	2 10 10
Q.2	What are the essential features of cloud computing?	Dec 2012	10

Unit 05/Lecture - 02

Architecture of cloud computing – [Rgpv/dec 2013(7), Rgpv/dec 2012(10)]

Cloud computing is a term used to refer to a model of network computing where a program or application runs on a connected server or servers rather than on a local computing device such as a PC, tablet or smartphone. Like the traditional client-server model or older mainframe computing,[1] a user connects with a server to perform a task. The difference with cloud computing is that the computing process may run on one or many connected computers at the same time, utilizing the concept of virtualization. With virtualization, one or more physical servers can be configured and partitioned into multiple independent "virtual" servers, all functioning independently and appearing to the user to be a single physical device. Such virtual servers are in essence disassociated from their physical server, and with this added flexibility, they can be moved around and scaled up or down on the fly without affecting the end user. The computing resources have become "granular", which provides end user and operator benefits including on-demand self-service, broad access across multiple devices, resource pooling, rapid elasticity and service metering capability

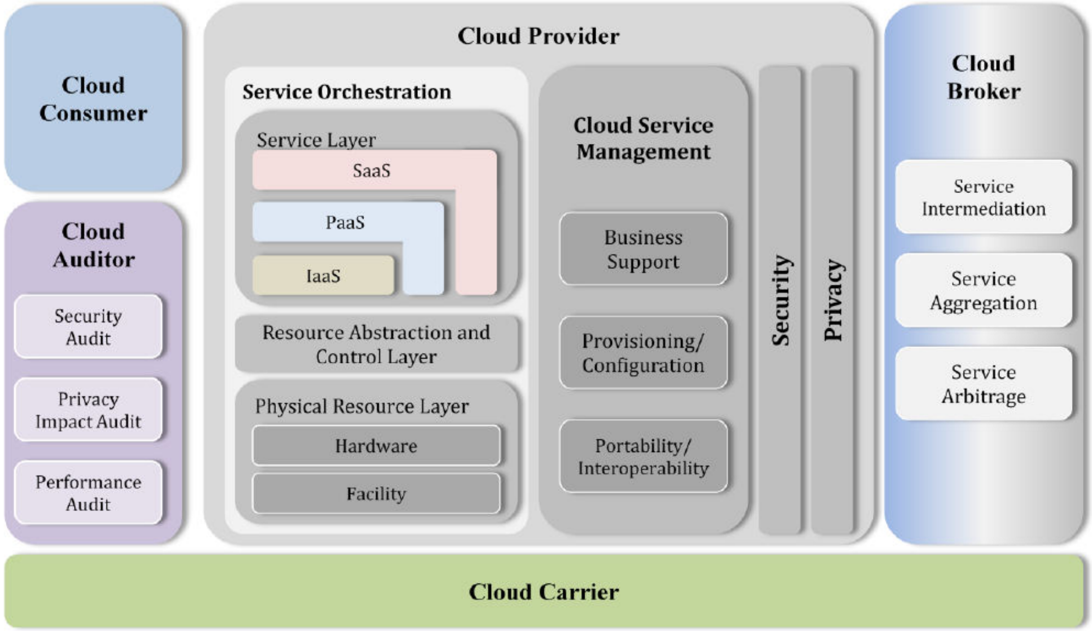
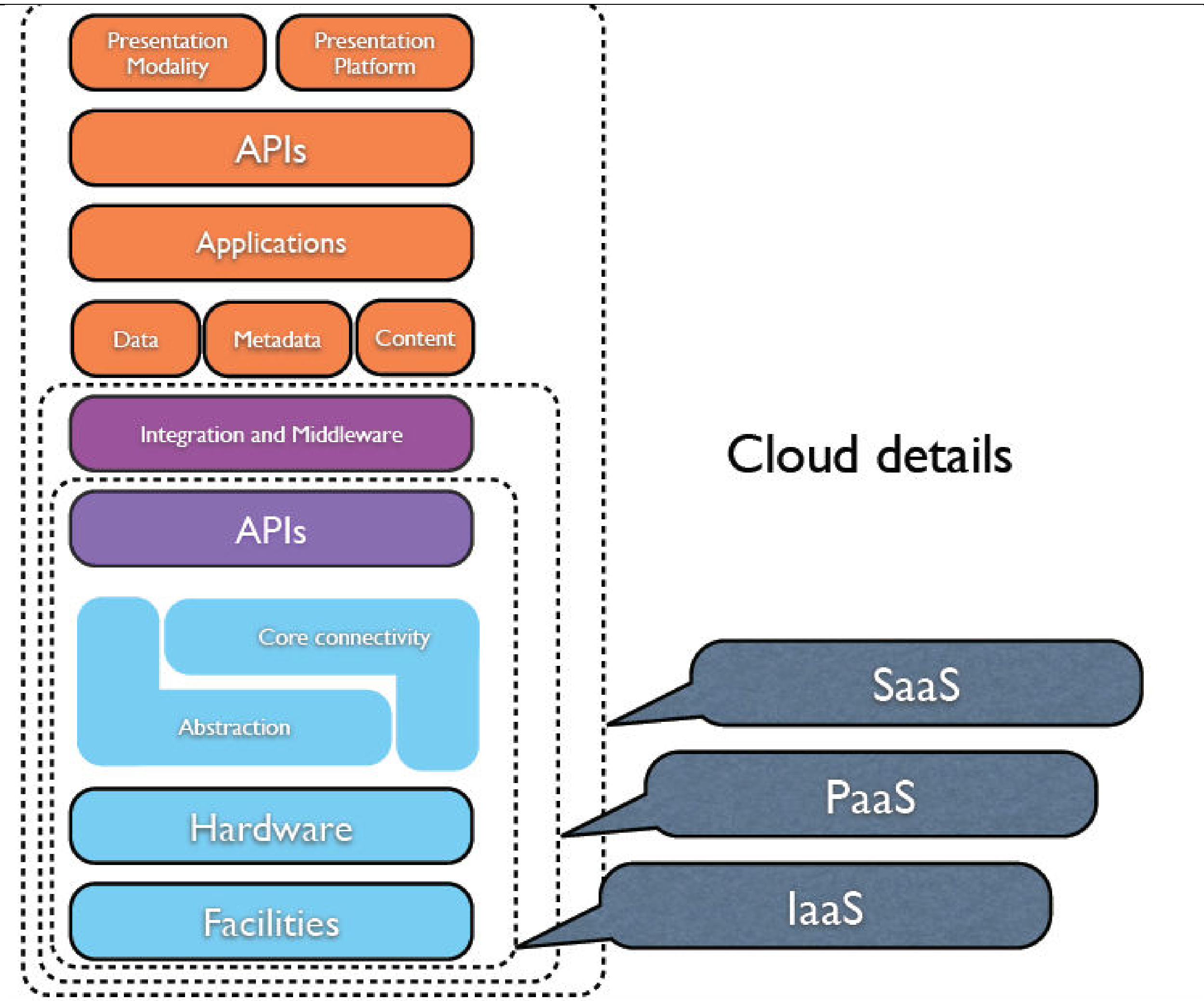


Figure 1: The Conceptual Reference Model



Advantages

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network.[8] at the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves european users during european business hours with a specific application (e.g., email) may reallocate the same resources to serve north american users during north america's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rackspace, etc. Are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

The term "moving to cloud" also refers to an organization moving away from a traditional capex model (buy the dedicated hardware and depreciate it over a period of time) to the opex model (use a shared cloud infrastructure and pay as one uses it).

Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of infrastructure.[9] proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables it to more rapidly adjust resources to meet fluctuating and unpredictable business demand.[9][10][11] cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.[12]

S.no	Rgpv question	Year	Marks
Q.1	Explain architectural framework of cloud computing?	Rgpv Dec 2013	7
Q.2	Explain the architectural frame work of cloud computing?	Rgpv Dec 2012	10
Q.3	Give a brief note on cloud architecture?	Rgpv Dec 2011	10

Unit 05/Lecture - 03

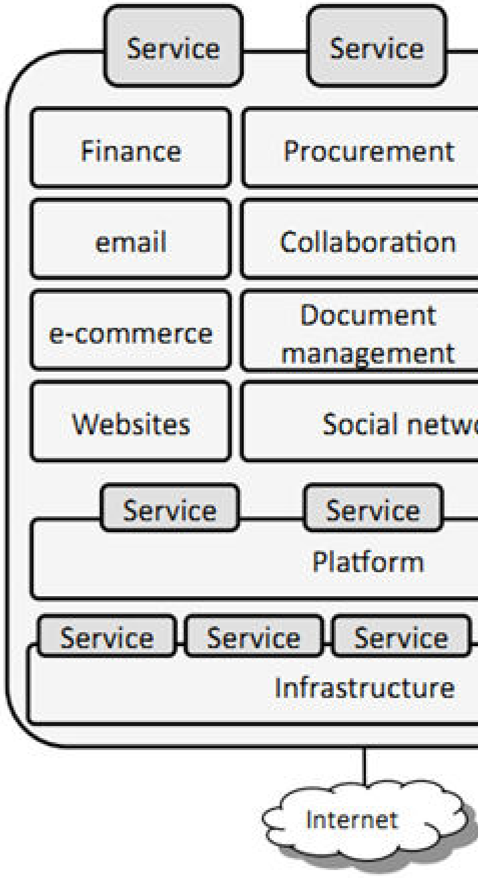
Cloud models – [Rgpv/dec 2013(10)&(7)]

If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

SaaS[Rgpv/dec2014]

Software-as-a-Service provides complete applications to a cloud's end user. It is mainly accessed through a web portal and service oriented architectures based on web service technologies. Credit card or bank account details must be provided to enable the fees for the use of the services to be billed.

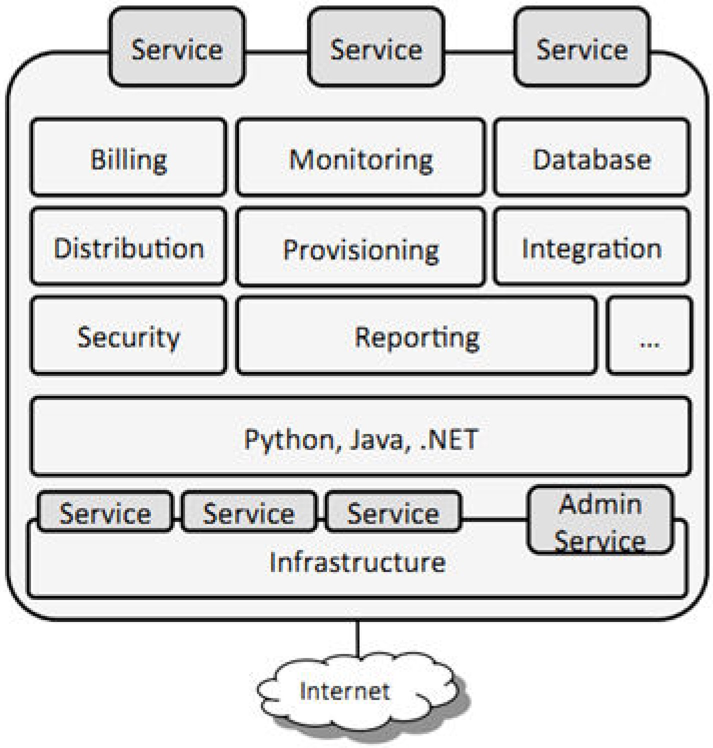
The services on the application layer can be seen as an extension of the ASP (application service provider) model, in which an application is run, maintained, and supported by a service vendor. The main differences between the services on the application layer and the classic ASP model are the encapsulation of the application as a service, the dynamic procurement, and billing by units of consumption (pay as you go). However, both models pursue the goal of focusing on core competencies by outsourcing applications.



Software-as-a-Service (SaaS) Stack

PaaS

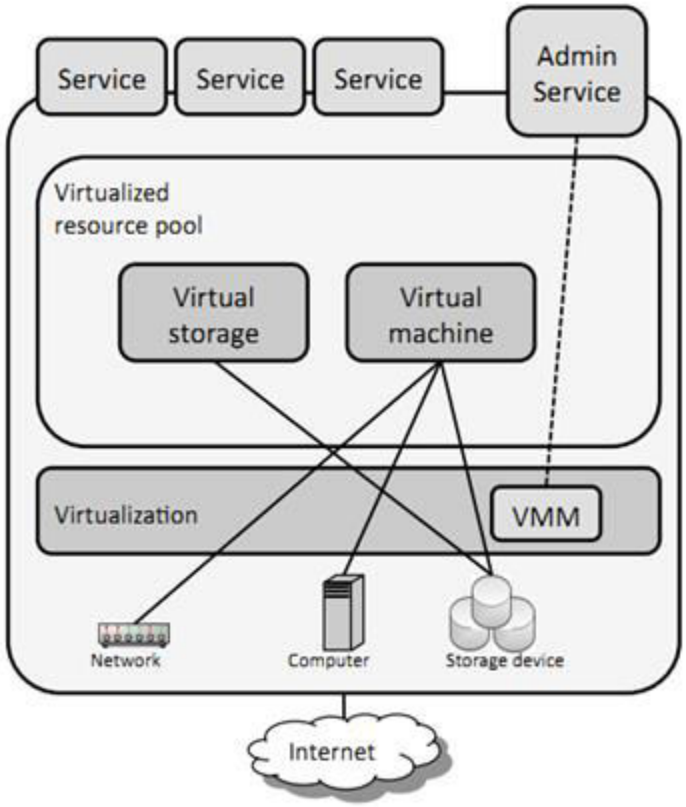
PaaS comprises the environment for developing and provisioning cloud applications. The principal users of this layer are developers seeking to develop and run a cloud application for a particular platform. They are supported by the platform operators with an open or proprietary language, a set of essential basic services to facilitate communication, monitoring, or service billing, and various other components, for instance to facilitate startup or ensure an application's scalability and/or elasticity (see figure 3). Distributing the application to the underlying infrastructure is normally the responsibility of the cloud platform operator. The services offered on a cloud platform tend to represent a compromise between complexity and flexibility that allows applications to be implemented quickly and loaded in the cloud without much configuration. Restrictions regarding the programming languages supported, the programming model, the ability to access resources, and persistency are possible downsides.



Platform-as-a-Service (PaaS) Stack

IaaS

The services on the infrastructure layer are used to access essential IT resources that are combined under the heading Infrastructure-as-a-Service (IaaS). These essential IT resources include services linked to computing resources, data storage resources, and the communications channel. They enable existing applications to be provisioned on cloud resources and new services implemented on the higher layers. Physical resources are abstracted by virtualization, which means they can then be shared by several operating systems and end user environments on the virtual resources – ideally, without any mutual interference. These virtualized resources usually comprise CPU and RAM, data storage resources (elastic block store and databases).



Infrastructure-as-a-Service (IaaS) Stack

S.no	Rgpv question	Year	Marks
Q.1	What are various cloud models?Explain each in brief.	Dec 2013	10
Q.2	What does Software as a service provide.	Dec 2014	2

Unit 05/Lecture - 04

Private Cloud – [Rgpv/dec 2013(10)]

A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate. As with other cloud models, private clouds will provide computing power as a service within a virtualised environment using an underlying pool of physical computing resource. However, under the private cloud model, the cloud (the pool of resource) is only accessible by a single organisation providing that organisation with greater control and privacy.

The technical mechanisms used to provide the different services which can be classed as being private cloud services can vary considerably and so it is hard to define what constitutes a private cloud from a technical aspect. Instead such services are usually categorised by the features that they offer to their client. Traits that characterise private clouds include the ring fencing of a cloud for the sole use of one organisation and higher levels of network security. They can be defined in contrast to a public cloud which has multiple clients accessing virtualised services which all draw their resource from the same pool of servers across public networks. Private cloud services draw their resource from a dsitinct pool of physical computers but these may be hosted internally or externally and may be accessed across private leased lines or secure encrypted connections via public networks.

The additional security offered by the ring fenced cloud model is ideal for any organisation, including enterprise, that needs to store and process private data or carry out sensitive tasks. For example, a private cloud service could be utilised by a financial company that is required by regulation to store sensitive data internally and who will still want to benefit from some of the advantages of cloud computing within their business infrastructure, such as on demand resource allocation.

The private cloud model is closer to the more traditional model of individual local access networks (LANs) used in the past by enterprise but with the added advantages of virtualisation. The features and benefits of private clouds therefore are:

- **Higher security and privacy**; public clouds services can implement a certain level of security but private clouds - using techniques such as distinct pools of resources with access restricted to connections made from behind one organisation's firewall, dedicated leased lines and/or on-site internal hosting - can ensure that operations are kept out of the reach of prying eyes
- **More control**; as a private cloud is only accessible by a single organisation, that organisation will have the ability to configure and manage it inline with their needs to achieve a tailored network solution. However, this level of control removes somes the economies of scale generated in public clouds by having centralised management of the hardware
- **Cost and energy efficiency**; implementing a private cloud model can improve the allocation of resources within an organisation by ensuring that the availability of resources to individual departments/business functions can directly and flexibly respond to their demand. Therefore, although they are not as cost effective as a public cloud services due to smaller economies of scale and increased management costs, they do make more efficient use of the computing resource than traditional LANs as they minimise the investment into unused capacity. Not only does this provide a cost saving but it can reduce an organisation's carbon footprint too
- **Improved reliability**; even where resources (servers, networks etc.) are hosted internally, the creation of virtualised operating environments means that the network is more resilient to individual failures across the physical infrastructure. Virtual partitions can, for example, pull their resource from the remaining unaffected servers. In addition,

where the cloud is hosted with a third party, the organisation can still benefit from the physical security afforded to infrastructure hosted within data centres

- **Cloud bursting**; some providers may offer the opportunity to employ cloud bursting, within a private cloud offering, in the event of spikes in demand. This service allows the provider to switch certain non-sensitive functions to a public cloud to free up more space in the private cloud for the sensitive functions that require it. Private clouds can even be integrated with public cloud services to form hybrid clouds where non-sensitive functions are always allocated to the public cloud to maximise the efficiencies on offer.

How to buit private cloud-

Private cloud looks and acts like a public cloud, giving your corporation all the speed, agility and cost savings promised by cloud technology, only it's single tenant and that tenant is you, right? Well, that's the goal, but it's not quite the reality yet for most enterprises.

1. There must be a converged infrastructure. "Servers must be virtualized. There has got to be underlying software defined networking and a converged storage fabric,"

"This is not something that is done very well in the public cloud space now and it's an opportunity for corporate IT operations that haven't had sophisticated systems in place to do these things, to leapfrog themselves in that regard in the new era of private cloud,"

2. There has to be fully automated orchestration of both system management and software distribution across the converged infrastructure.

"That is where the cost savings is. Automating deployment and streamlining the human activity previously required to do daily tasks. That is what will eventually drive private cloud sales,"

You have to improve the provisioning process significantly to legitimately call it private cloud, "If it takes you two weeks to provision resources now, getting that down to two days is not going to cut it. You've got to get it to 15 minutes. You can't be sitting around waiting for various levels of approval to happen because you lose the agility and speed. It's the difference between virtualization and cloud," .

3. There must be a self-service catalog of standard computing offerings available to users across the company.

"The litmus test is whether or not the dashboard is available to business users across the company and not just an interface for traditional IT staff to use to dole out IT resources. Having just the latter, means that IT just has a new toy,"

4. There has to be accountability by way of some sort of charge-back, track-back or show-back mechanism that keeps track of which users are employing which resources and for just how long.

Enterprise Management Association analyst Torsten Volk argues that at a minimum providing a show back mechanism is crucial for any fledgling private cloud. "If you can't at least show who is responsible for the cycles that have been used, then there is no incentive to use those resources efficiently,"

S.no	Rgpv question	Year	Marks
Q.1	What is private cloud? Explain how can we build a private cloud.	Rgpv Dec 2013	10

Unit 05/Lecture -05

Cloud service providers - [Rgpv/dec 2012(5)]

A cloud provider is a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals. Cloud providers are sometimes referred to as cloud service providers or CSPs.

There are a number of things to think about when you evaluate cloud providers. The cost will usually be based on a per-use utility model but there are a number of variations to consider. The physical location of the servers may also be a factor for sensitive data.

Reliability is crucial if your data must be accessible. A typical cloud storage service-level agreement (SLA), for example, specifies precise levels of service – such as, for example, 99.9% uptime and the recourse or compensation that the user is entitled to should the provider fail to provide the service as described. However, it's important to understand the fine print in that agreement because some providers discount outages of less than ten minutes, which may be too long for some businesses.

Security is another important consideration. Organizations such as the Cloud Security Alliance (CSA) offer certification to cloud providers that meet their criteria. The CSA's Trusted Cloud Initiative program was created to help cloud service providers develop industry-recommended, secure and interoperable identity, access and compliance management configurations and practices.

S.no	Rgpv question	Year	Marks
Q.1	Write short note on cloud service provider?	Rgpv Dec 2012	5

Unit 05/Lecture - 06

Cloud Vocabulary - [Rgpv/dec 2013(7), Rgpv/dec 2011(5)]]

Cloudburst: The term cloudburst is being use in two meanings, negative and positive:

Cloudburst: The term cloudburst is being use in two meanings, negative and positive:

1. **Cloudburst (negative)**: The failure of a cloud computing environment due to the inability to handle a spike in demand.

   Cloudburst (positive): The dynamic deployment of a software application that runs on internal organizational compute resources to a public cloud to address a spike in demand.
2. **Cloudstorming:** The act of connecting multiple cloud computing environments.
3. **Vertical Cloud**: A cloud computing environment optimized for use in a particular vertical -- i.e., industry -- or application use case.
4. **Private Cloud**: A cloud computing-like environment within the boundaries of an organization and typically for its exclusive usage.
5. **Internal Cloud**: A cloud computing-like environment within the boundaries of an organization and typically available for exclusive use by said organization.
6. **Hybrid Cloud**: A computing environment combining both private (internal) and public (external) cloud computing environments. May either be on a continuous basis or in the form of a 'cloudburst'.
7. **Cloudware**: A general term referring to a variety of software, typically at the infrastructure level, that enables building, deploying, running or managing applications in a cloud computing environment.
8. **External Cloud**: A cloud computing environment that is external to the boundaries of the organization. Although it often is, an external cloud is not necessarily a public cloud. Some external clouds make their cloud infrastructure available to specific other organizations and not to the public at-large.
9. **Public Cloud:** A cloud computing environment that is open for use to the general public,

whether individuals, corporations or other types of organizations. Amazon Web Services are an example of a public cloud.

10. **Virtual Private Cloud (VPC):** A term coined by Reuven Cohen, CEO and founder of Enomaly. The term describes a concept that is similar to, and derived from, the familiar concept of a Virtual Private Network (VPN), but applied to cloud computing. It is the notion of turning a public cloud into a virtual private cloud, particularly in terms of security and the ability to create a VPC across components that are both within the cloud and external to it.
11. **Cloud Portability:** The ability to move applications (and often their associated data) across cloud computing environments from different cloud providers, as well as across private or internal cloud and public or external clouds.
12. **Cloud Spanning:** Running an application in a way that its components straddle multiple cloud environments (which could be any combination of internal/private and external/public clouds. Unlike Cloud Bursting, which refers strictly to expanding the application to an External Cloud to handle spikes in demand, Cloud Spanning includes scenarios in which an applications component are continuously distributed across multiple clouds.

S.no	Rgpv question	Year	Marks
Q.1	Write short note on cloud vocabulary?	Dec 2013 Dec 2011	7 5

Unit 05/Lecture - 07

Cloud security – [Rgpv/dec 2013(5), Rgpv/dec 2011(5)]]

Cloud computing security or, more simply, **cloud security** is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Cloud security is not to be confused with security software offerings that are cloud-based such as security as a service.

Cloud security controls

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management.[6] The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:[6]

Deterrent controls

These controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, these controls do not reduce the actual vulnerability of a system.

Preventative controls

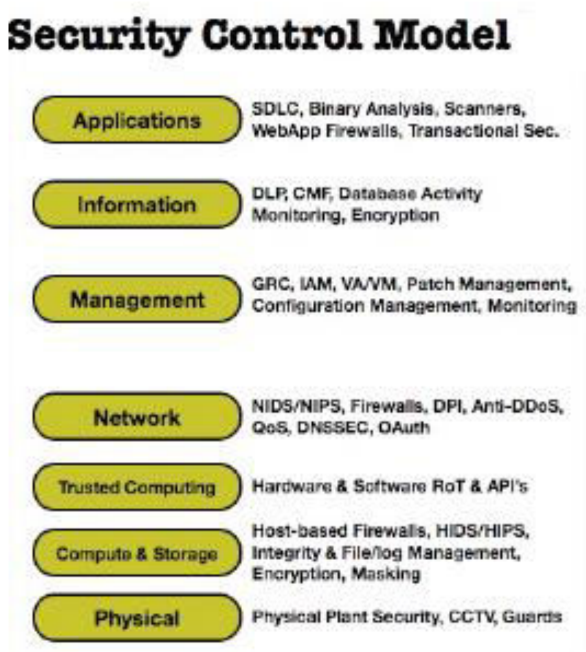
These controls upgrade the strength of the system by managing the vulnerabilities. The preventative control will safeguard vulnerabilities of the system. If an attack were to occur, the preventative controls are in place to cover the attack and reduce the damage and violation to the system's security.

Corrective controls

Corrective controls are used to reduce the effect of an attack. Unlike the preventative controls, the corrective controls take action as an attack is occurring.

Detective controls

Detective controls are used to detect any attacks that may be occurring to the system. In the event of an attack, the detective control will signal the preventative or corrective controls to address the issue.[6]



Cloud Application – [Rgpv/dec 2013(5), Rgpv/dec 2011(5)]]

Cloud computing has been credited with increasing competitiveness through cost reduction, greater flexibility, elasticity and optimal resource utilization. Here are a few situations where cloud computing is used to enhance the ability to achieve business goals.

1. Infrastructure as a service (iaas) and platform as a service (paas)

When it comes to iaas, using an existing infrastructure on a pay-per-use scheme seems to be an obvious choice for companies saving on the cost of investing to acquire, manage and maintain an it infrastructure. There are also instances where organizations turn to paas for the same reasons while also seeking to increase the speed of development on a ready-to-use platform to deploy applications.

2. Private cloud and hybrid cloud

Among the many incentives for using cloud, there are two situations where organizations are looking into ways to assess some of the applications they intend to deploy into their environment through the use of a cloud (specifically a public cloud). While in the case of test and development it may be limited in time, adopting a hybrid cloud approach allows for testing application workloads, therefore providing the comfort of an environment without the initial investment that might have been rendered useless should the workload testing fail.

Another use of hybrid cloud is also the ability to expand during periods of limited peak usage, which is often preferable to hosting a large infrastructure that might seldom be of use. An organization would seek to have the additional capacity and availability of an environment when needed on a pay-as you-go basis.

3. Test and development

Probably the best scenario for the use of a cloud is a test and development environment. This entails securing a budget, setting up your environment through physical assets, significant manpower and time. Then comes the installation and configuration of your platform. All this can often extend the time it takes for a project to be completed and stretch your milestones.

With cloud computing, there are now readily available environments tailored for your needs at your fingertips. This often combines, but is not limited to, automated provisioning of physical and virtualized resources.

4. Big data analytics

One of the aspects offered by leveraging cloud computing is the ability to tap into vast quantities of both structured and unstructured data to harness the benefit of extracting business value.

Retailers and suppliers are now extracting information derived from consumers' buying patterns to target their advertising and marketing campaigns to a particular segment of the population. Social networking platforms are now providing the basis for analytics on behavioral patterns that organizations are using to derive meaningful information.

5. File storage

Cloud can offer you the possibility of storing your files and accessing, storing and retrieving them from any web-enabled interface. The web services interfaces are usually simple. At any time and place you have high availability, speed, scalability and security for your environment. In this scenario, organizations are only paying for the amount of storage they are actually consuming, and do so without the worries of overseeing the daily maintenance of the storage infrastructure.

There is also the possibility to store the data either on or off premises depending on the regulatory compliance requirements. Data is stored in virtualized pools of storage hosted by a third party based on the customer specification requirements.

6. Disaster recovery

This is yet another benefit derived from using cloud based on the cost effectiveness of a disaster recovery (dr) solution that provides for a faster recovery from a mesh of different physical locations at a much lower cost that the traditional dr site with fixed assets, rigid procedures and a much higher cost.

7. Backup

Backing up data has always been a complex and time-consuming operation. This included maintaining a set of tapes or drives, manually collecting them and dispatching them to a backup facility with all the inherent problems that might happen in between the originating and the backup site. This way of ensuring a backup is performed is not immune to problems such as running out of backup media , and there is also time to load the backup devices for a restore operation, which takes time and is prone to malfunctions and human errors.

Cloud-based backup, while not being the panacea, is certainly a far cry from what it used to be. You can now automatically dispatch data to any location across the wire with the assurance that neither security, availability nor capacity are issues.

While the list of the above uses of cloud computing is not exhaustive, it certainly give an incentive to use the cloud when comparing to more traditional alternatives to increase it infrastructure flexibility , as well as leverage on big data analytics and mobile computing.

Cloud integration – [Rgpv/dec 2013(5)]

Cloud integration is the process of configuring multiple application programs to share data in the cloud. In a network that incorporates cloud integration, diverse applications communicate either directly or through third-party software.

Cloud integration offers the following advantages over older, compartmentalized organizational methods.

- Each user can access personal data in real time from any device.
- Each user can access personal data from any location with Internet access.
- Each user can integrate personal data such as calendars and contact lists served by diverse application programs.

- Each user can employ the same logon information (username and password) for all personal applications.
- The system efficiently passes control messages among application programs.
- By avoiding the use of data silos, data integrity is maintained and data conflicts (which can arise from redundancy) are avoided.
- Cloud integration offers scalability to allow for future expansion in terms of the number of users, the number of applications, or both.

In recent years, cloud integration has gained favor among organizations, corporations, and government agencies that implement SaaS (Software as a Service), a software distribution model in which applications are hosted by a vendor or service provider and made available to users over the Internet.

Risk of cloud computing – [Rgpv/dec 2011]

Cloud benefits

Cloud computing provides a scalable online environment that makes it possible to handle an increased volume of work without impacting system performance. Cloud computing also offers significant computing capability and economy of scale that might not otherwise be affordable, particularly for small and medium-sized organizations, without the IT infrastructure investment. Cloud computing advantages include:

- Lower capital costs — Organizations can provide unique services using large-scale computing resources from cloud service providers, and then nimbly add or remove IT capacity to meet peak and fluctuating service demands while only paying for actual capacity used.
- Lower IT operating costs — Organizations can rent added server space for a few hours at a time rather than maintain proprietary servers without worrying about upgrading their resources whenever a new application version is available. They also have the flexibility to host their virtual IT infrastructure in locations offering the lowest cost.

- No hardware or software installation or maintenance
- Optimized IT infrastructure provides quick access to needed computing services

The risks

- **Environmental security —** The concentration of computing resources and users in a cloud computing environment also represents a concentration of security threats. Because of their size and significance, cloud environments are often targeted by virtual machines and bot malware, brute force attacks, and other attacks. Ask your cloud provider about access controls, vulnerability assessment practices, and patch and configuration management controls to see that they are adequately protecting your data.
- **Data privacy and security —** Hosting confidential data with cloud service providers involves the transfer of a considerable amount of an organization's control over data security to the provider. Make sure your vendor understands your organization's data privacy and security needs. Also, make sure your cloud provider is aware of particular data security and privacy rules and regulations that apply to your entity, such as HIPAA, the Payment Card Industry Data Security Standard (DCI DSS), the Federal Information Security Management Act of 2002 (FISMA), or the privacy considerations of Gramm-Leach-Bliley Act.
- **Data availability and business continuity —** A major risk to business continuity in the cloud computing environment is loss of internet connectivity. Ask your cloud provider what controls are in place to ensure internet connectivity. If a vulnerability is identified, you may have to terminate all access to the cloud provider until the vulnerability is rectified. Finally, the seizure of a data-hosting server by law enforcement agencies may result in the interruption of unrelated services stored on the same machine.
- **Record retention requirements —** If your business is subject to record retention requirements, make sure your cloud provider understands what they are and so they can meet them.
- **Disaster recovery —** Hosting your computing resources and data at a cloud provider

makes the cloud provider’s disaster recovery capabilities vitally important to your company’s disaster recovery plans. Know your cloud provider’s disaster recovery capabilities and ask your provider if they been tested.

Evaluating your options

Many cloud provider options are available, each with unique risks. As you evaluate your choices and the associated risks, consider the following

- Cloud providers are sometimes reluctant to produce third-party audit reports unless an audit clause is included in the contract. Some hosts require clients to pay for reports
- Some internal audit departments are performing control reviews of cloud providers, in addition to receiving and analyzing third party audit reports. This is driven by certain controls not being tested, exclusion of pertinent systems, or other factor that require on-site testing.
- Standard cloud provider audit reports typically do not include vulnerability/penetration testing results. Providers are hesitant to allow scanning, as they believe this may compromise their infrastructure.

Cloud computing is a widely used format and we don't see this changing anytime soon. Knowing that you are managing the risks associated with housing your sensitive data offsite will give you confidence with the platform, so you can take advantage of the opportunities presented by the cloud.

S.no	Rgpv question	Year	Marks
Q.1	Write short note on following(any two) a)Cloud computing,b) application of cloud c) Cloud integration	Dec 2013 Dec 2012 Dec 2011	10 5 5
Q.2	Write short note on risk of cloud computing?	Dec 2011	5

Unit 05/Lecture -08

Evolution of cloud computing – [Rgpv/dec 2012(5)]

the trend toward cloud computing started in the late 1980s with the concept of grid computing when, for the first time, a large number of systems were applied to a single problem, usually scientific in nature and requiring exceptionally high levels of parallel computation. In europe , long distance optical networks are used to tie multiple universities into a massive computing grid in order that resources could be shared and scaled for large scientific calculations.

Grid computing provided a virtual pool of computation resources but it's different than cloud computing. Grid computing specifically refers to leveraging several computers in parallel to solve a particular, individual problem, or to run a specific application. Cloud computing, on the other hand, refers to leveraging multiple resources, including computing resources, to deliver a unified “service” to the end user.

In grid computing, the focus is on moving a workload to the location of the needed computing resources, which are mostly remote and are readily available for use. Usually a grid is a cluster of servers on which a large task could be divided into smaller tasks to run in parallel. From this point of view, a grid could actually be viewed as just one virtual server. Grids also require applications to conform to the grid software interfaces.

In a cloud environment, computing and extended it and business resources, such as servers, storage, network, applications and processes, can be dynamically shaped or carved out from the underlying hardware infrastructure and made available to a workload. In addition, while a cloud can provision and support a grid, a cloud can also support non-grid environments, such as a three-tier web architecture running traditional or web 2.0 applications

In the 1990s, the concept of virtualization was expanded beyond virtual servers to higher levels of abstraction—first the virtual platform, including storage and network resources, and subsequently the virtual application, which has no specific underlying infrastructure. Utility computing offered clusters as virtual platforms for computing with a metered business model.

More recently software as a service (saas) has raised the level of virtualization to the application, with a business model of charging not by the resources consumed but by the value of the application to subscribers. The concept of cloud computing has evolved from the concepts of grid, utility and saas. It is an emerging model through which users can gain access to their applications from anywhere, at any time, through their connected devices. These applications reside in massively scalable data centers where compute resources can be dynamically provisioned and shared to achieve significant economies of scale.

Companies can choose to share these resources using public or private clouds, depending on their specific needs. Public clouds expose services to customers, businesses and consumers on the internet. Private clouds are generally restricted to use within a company behind a firewall and have fewer security exposures as a result. The strength of a cloud is its infrastructure management, enabled by the maturity and progress of virtualization technology to manage and better utilize the underlying resources through automatic provisioning, re-imaging, workload rebalancing, monitoring, systematic change request handling and a dynamic and automated security and resiliency platform.

As more enterprises add cloud computing the level of applications is migrating toward more mission critical and saas will become a mainstay of it strategies.

A number of companies, including google, microsoft, amazon, and ibm, have built enormous datacenter-based computing capacity all over the world to support their web service offerings (search, instant messaging, web-based retail). With this computing infrastructure in place these companies are already poised to offer new cloud-based software applications.

Large enterprise software solutions, such as erp (enterprise resource planning) applications, have traditionally only been affordable to very big enterprises with big it budgets. However, companies that sell these solutions are finding they can reach small to medium businesses by making their very expensive, very complex applications available as internet-based software services. This ability of saas to deliver expensive applications at affordable will continue to accelerate.

S.no	Rgpv question	Year	Marks
Q.1	Write short note on cloud computing evolution?	Rgpv Dec 2012	5

Additional Topic Unit - 05/Lecture - 09

Cloud storage

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans across multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data.

Cloud storage services may be accessed through a collocated cloud compute service, a web service application programming interface (api) or by applications that utilize the api, such as cloud desktop storage, a cloud storage gateway or web-based content management systems.

A high level architecture of cloud storage.

Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources.

Cloud storage typically refers to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage.

Cloud storage is:

- Made up of many distributed resources, but still acts as one - often referred to as federated storage clouds [6]

- Highly fault tolerant through redundancy and distribution of data
- Highly durable through the creation of versioned copies
- Typically eventually consistent with regard to data replicas.

Advantages

- Companies need only pay for the storage they actually use, typically an average of consumption during a month. this does not mean that cloud storage is less expensive, only that it incurs operating expenses rather than capital expenses.
- Organizations can choose between off-premise and on-premise cloud storage options, or a mixture of the two options, depending on relevant decision criteria that is complementary to initial direct cost savings potential; for instance, continuity of operations (coop), disaster recovery (dr), security (pii, hipaa, sarbox, ia/cnd), and records retention laws, regulations, and policies.
- Storage availability and data protection is intrinsic to object storage architecture, so depending on the application, the additional technology, effort and cost to add availability and protection can be eliminated.
- Storage maintenance tasks, such as purchasing additional storage capacity, are offloaded to the responsibility of a service provider.
- Cloud storage provides users with immediate access to a broad range of resources and applications hosted in the infrastructure of another organization via a web service interface.
- Cloud storage can be used for copying virtual machine images from the cloud to on-premise locations or to import a virtual machine image from an on-premise location to the cloud image library. In addition, cloud storage can be used to move virtual machine images between user accounts or between data centers.

Reference

Book	Author	Priority
Information storage management	G. Somasundaram Alok Shrivastava	1
Storage Network explained : Basic and application of fiber channels, SAN, NAS, iSESI	Ulf Troppens, Wolfgang Mueller-Friedt, Rainer Erkens, Rainer Wolafka, Nils Haustein	2
Nick Antonopoulos, Lee Gillam	Cloud Computing : Principles, System & Application	3