Q.1 what do you mean by cloud? Describe about the basic characteristic of cloud.

The “cloud” in cloud computing can be defied as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet. A cloud service is any service made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own premises servers explained before, the most common cloud service is that one offering data storage disks and virtual servers, i.e. infrastructure. Examples of Infrastructure-as-a-Service (IaaS) companies are Amazon, Rackspace, and Flexi scale. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The “cloud” in cloud computing can be defied as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet.

Characteristic of Cloud Computing

- **Service Oriented**: The defining characteristic of cloud computing is the service oriented feature. All the IT related services are hosted in cloud infrastructure. Companies should not have to buy expensive servers, network equipment’s and invest on expensive manpower. All they need is to subscribe to any cloud service provider and get what they want. In this way, we can decrease our capital expenditure and move to operate via Operating expenditure.
- **Broad Network Access:** Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs.
- **On Demand:** A consumer can provision computing capabilities, such as server processing and network storage, as needed automatically without requiring human interacting with each service’s provider. computer services such as email, applications, network or server service can be provided without requiring human interacting with each service provider. Cloud service providers providing on demand self-services include Amazon Web Services (AWS), Microsoft Google, IBM and Salesforce.com.
- **Reliability, Elasticity and scalability**: The cloud is reliable in the sense that the infrastructure setup for cloud is robust and backed up for high availability. It is some resilient replicating and backup strategy that is targeted for huge customer base. The cloud is **elastic**, meaning that resource allocation can get bigger or smaller depending on demand. Elasticity enables **scalability**, which means that the cloud can scale upward for peak demand and downward for lighter demand. Scalability also means that an application can scale when adding users and when application requirements change.
- **Resource Pooling (Processor, Memory, and Storage):** Cloud infrastructure should have features of resource pooling i.e. resources (CPU, Memory, Disk) should be categorized in a hierarchy as per the need of computing. Resource pooling is mainly used for utilizing servers up to its potential. Since most of the ties server resources are unused, we can use the concept of virtualization to pool its resources.
- **Measured Service (Pay per Use):** Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilized service. Cloud computing services use a metering capability which enables to control and optimize resource use. This implies that just like air tie, electricity or municipality water IT services are charged per usage metrics – pay per use. The more you utilize the higher the bill. Just as utility companies sell power to subscribers, and telephone companies sell voice and data services, IT services such as network security management, data center hosting or even departmental billing can now be easily delivered as a contractual service.
- **Multi Tenancy:** Multi tenancy refers to a principle in IT infrastructure where a single instance of the software runs on a server, serving multiple client organizations (tenants). With a multitenant architecture, a software application is designed to virtually parting its data and configuration, and each client organization works with a customized virtual application instance. Each customer does its own work without interfering other customer even though they are hosted at the same platform.

Q.2 Discuss the capabilities that the cloud users can get through Platform as a Services (PaaS). Also mention the key characteristics of PaaS.

Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service. Along with software as a service (SaaS) and infrastructure as a service (IaaS), it is a service model of cloud computing. PaaS offerings facilitate the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities.

Technically, a PaaS is an Application Platform comprised of an operating system, middleware and other software that allows applications to run on the cloud with much of the management, security, scaling and other stack related headaches abstracted away. This allows you to focus on two things: customers and developing your application. Let the PaaS deal with system administration details like setting up servers or VMs, installing libraries or frameworks, configuring testing tools, etc.

Platform as a Service allows users to create software applications using tools supplied by the provider. PaaS services can consist of preconfigured features that customers can subscribe to; they can choose to include the features that meet their requirements while discarding those that do not. PaaS works on top of IaaS and will do all of that work automatically.

Characteristics of PaaS

1. **Multi-tenant architecture**
   A PaaS offering must be multi-tenanted. A multi-tenant platform is one that uses common computing resources including hardware, operating system, software (i.e. application code), and a single underlying database with a shared schema to support multiple customers simultaneously.
2. **Customizable /Programmable User Interface**
   PaaS offering should provide the ability to construct highly flexible user interfaces via a simple "drag & drop" methodology that permits the creation and configuration of UI components on the fly. Furthermore, given the growing set of Web devices, additional flexibility to use other technologies such as CSS, AJAX and Adobe Flex to specify the appearance of the application's interface should be available to the UI designer.
3. **Unlimited Database Customizations**
   Database used by application should have option of customization for more flexibility in application development. Specifying relationships between objects, a key requirement of any sophisticated business application, must be possible through the declarative Web-based interface. Other mandatory functions include the ability to incorporate validation rules and permissions at the object/field level and the ability to specify auditing behavior.
4. **Automation**
   PaaS environments automate the process of deploying applications to infrastructure, configuring application components, provisioning and configuring supporting technology like load balancers and databases, and managing system change based on policies set by the user.
5. **Security**
   The PaaS offering should provide a flexible access control system that allows detailed control over what users of the SaaS application can see and the data each user can access. Definition of access from the application level (including tabs, menus, objects, views, charts, reports and workflow actions) to the individual field level should be possible. Defining an access control model should be possible through the
   creation of groups and roles and the assignment of users to either groups or roles.

Q.3 How the Jericho Cloud model dimensions like parameterized, de-parameterized and proprietary, open differentiate the cloud formations from each other?

The Jericho Cloud Cube Model describes the multidimensional elements of cloud computing, framing not only cloud use cases, but also how they are deployed and used. The Jericho Forum has identified four criteria to differentiate cloud formations from each other and the manner of their provision. The Cloud Cube Model effectively summarizes these four dimensions:

1. Internal/External
2. Proprietary/Open
3. Parameterized/De-parameterized Architectures
4. Insourced/Outsourced(open)

Dimension 1: Internal/External

This dimension defines the physical location of the data; where does the cloud form exist – inside or outside organization boundaries? If the cloud form is within the organization's physical boundaries, then it is internal. If it is outside the organization's physical boundaries, then it is external. It's important to note that the assumption that internal is necessarily more secure than external is false. The most secure usage model is the effective use of both internal and external cloud forms.

Dimension 2: Proprietary/Open

This dimension defines the state of ownership of the cloud technology, services, interfaces, etc. It indicates the degree of interoperability, as well as enabling data/application transportability between an organization's own systems and other cloud forms and the ability to withdraw your data from a cloud form, or to move it to another without constraint. This dimension indicates any constraints on being able to share apps.

Dimension 3: Parameterized/De-parameterized Architectures

This dimension represents the architectural mindset of the organization. It asks if the organization is operating within its traditional IT perimeter or outside it. De-parameterization relates to the gradual failure, removal, shrinking or collapse of the traditional silo-based IT perimeter. "Parameterized" suggest a system that continues to operate within the traditional IT perimeter, often characterized by "network firewalls." This approach is known to inhibit collaboration. Operating within such areas means extending an organization's perimeter into the external cloud computing domain via a VPN and operating the virtual server in its own IP domain. The organization uses its own directory services to control access. Once the computing task is complete, the perimeter is withdrawn to its original, traditional position.

Dimension 4: Insourced/Outsourced

This dimension has two states in each of the eight cloud forms. It responds to the question: who do you want running your clouds? "Outsourced" means that the service is provided by a third party. Insourced means that the service is provided by your own staff under your control. These states describe the party managing the delivery of the cloud service(s) used by the organization. It's important to note that few organizations that are traditionally bandwidth, software or hardware providers will be able to smoothly transition to becoming cloud service providers. Organizations looking to procure cloud services must develop the ability to rapidly set up legally binding collaboration agreements, and to close them just as quickly once they become unnecessary.

Q.4 How can you characterize Service Oriented Architecture?

We can characterize SOA as follows:

- In SOA, Services should be **independent** of other services. Altering a service should not affect calling service.
- Services should be **self-contained**. When we talk about a Register Customer service it means, service will do all the necessary work for us, we are not required to care about anything.
- Services should be able to **define themselves**. Services should be able to answer a question what is does? It should be able to tell client what all operations it does, what all data types it uses and what kind of responses it will return.
- Services should be **published** into a location (directory) where anyone can search for it.
- As said, SOA comprises of collection services which communicate via **standard Messages**. Standard messages make them platform independent. (Here standard doesn't mean standard across Microsoft it means across all programming languages and technologies.)
- Services should be able to communicate with each other **asynchronously**.
- Services should support **reliable messaging**. Means there should be a guarantee that request will be reached to correct destination and correct response will be obtained.
- Services should support **secure communication**

Q. 5 Define virtualization. What is the role of virtualization in cloud computing?

In computing, virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments. Even something as simple as partitioning a hard drive is considered virtualization because you take one drive and partition it to create two separate hard drives. Devices, applications and human users are able to interact with the virtual resource as if it were a real single logical resource. The term virtualization has become somewhat of a buzzword, and as a result the term is now associated with a number of computing technologies including the following:

- storage virtualization: the amalgamation of multiple network storage devices into what appears to be a single storage unit.
- server virtualization: the partitioning a physical server into smaller virtual servers.
- operating system-level virtualization: a type of server virtualization technology which works at the operating system (kernel) layer.
- network virtualization: using network resources through a logical segmentation of a single physical network.
- application virtualization

Virtualization is the key to cloud computing, since it is the enabling technology allowing the creation of an intelligent abstraction layer which hides the complexity of underlying hardware or software. Server virtualization enables different operating systems to share the same hardware and make it easy to move operating systems between different hardware, all while the applications are running. Storage virtualization does the same thing for data. Storage virtualization creates the abstraction layer between the applications running on the servers, and the storage they use to store the data.

Virtualizing the storage and incorporating the intelligence for provisioning and protection at the virtualization layer enables companies to use any storage they want, and not be locked into any individual vendor. Storage virtualization makes storage a commodity. All this makes for some interesting ways for companies to reduce their costs.

Q. 6 What do mean by an intrusion in a cloud network? How intrusions in cloud networks are detected ?

The distributed and open structure of cloud computing and services becomes an attractive target for potential cyber-attacks by intruders. The traditional Intrusion Detection and Prevention Systems (IDPS) are largely inefficient to be deployed in cloud computing environments due to their openness and specific essence. This paper surveys, explores and informs researchers about the latest developed IDPSs and alarm management techniques by providing a comprehensive taxonomy and investigating possible solutions to detect and prevent intrusions in cloud computing systems.

Considering the desired characteristics of IDPS and cloud computing systems, a list of germane requirements is identified and four concepts of autonomic computing self-management, ontology, risk management, and fuzzy theory are leveraged to satisfy these requirements.

Highlights

► Up-to-date systematic review of IDPS for cloud computing environments.

► Provides an appropriate set of all possible solutions and a layered taxonomy of IDPS.

► Based on the characteristics of cloud computing and IDPS, a list of requirements is provided.

► Autonomic computing, ontology, risk management and fuzzy logic are proposed to develop Cloud IDPS.

Q.7 How data segmentation and credential management ensure host security in a cloud ? Explain with suitable example.