**Cloud Computing**

**Introduction:**

"Cloud Computing," to put it simply, means "Internet Computing." Cloud Computing is a general term used to describe a new class of network based computing that takes place over the Internet, basically a step on from Utility Computing. The Internet is commonly visualized as clouds; hence the term “cloud computing” is for computation done through the Internet. With Cloud Computing users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides, databases in cloud are very dynamic and scalable. Cloud computing is unlike grid computing, utility computing, or autonomic computing. In fact, it is a very independent platform in terms of computing. The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computer through the Internet.

In other words, this is a collection/group of integrated and networked hardware, software and Internet infrastructure called a platform. Using the Internet for communication and transport provides hardware, software and networking services to clients. These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface). In addition, the platform provides on demand services, which are always on, anywhere, anytime and any place. Pay for use and as needed, elastic (scale up and down in capacity and functionalities). The hardware and software services are available to the general public, enterprises, corporations and businesses markets.

Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Parallels to this concept can be drawn with the electricity grid, wherein end-users consume power without needing to understand the component devices or infrastructure required to provide the service.

Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers.

Cloud computing providers deliver applications via the internet, which are accessed from a web browser, while the business software and data are stored on servers at a remote location. In some cases, legacy applications (line of business applications that until now have been prevalent in thin client Windows computing) are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data center location; in other cases, entire business applications have been coded using web-based technologies such as AJAX.

Most cloud computing infrastructures consist of services delivered through shared data-centers and appearing as a single point of access for consumers' computing needs. Commercial offerings may be required to meet service-level agreements (SLAs), but specific terms are less often negotiated by smaller companies.

**What is cloud? :**

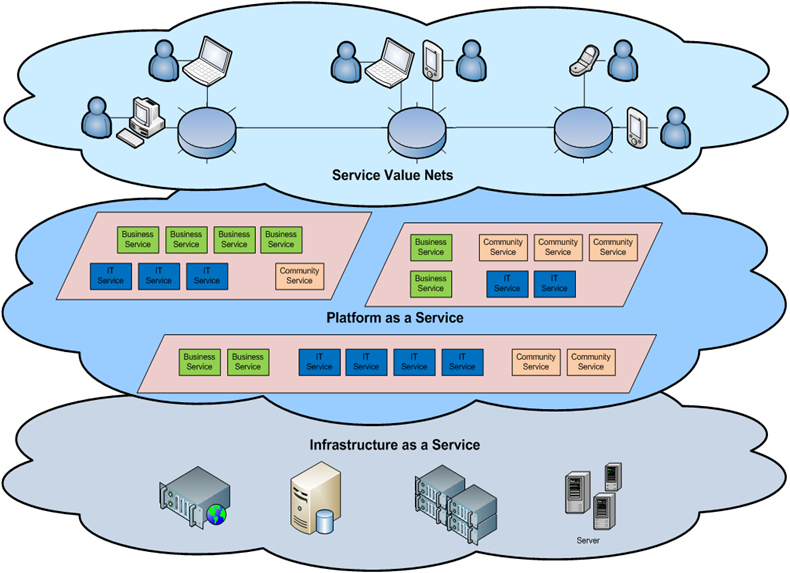
Many people are confused as to exactly what cloud computing is, especially as the term can be used to mean almost anything. Roughly, it describes highly scalable computing resources provided as an external service via the internet on a pay-as-you-go basis. The cloud is simply a metaphor for the internet, based on the symbol used to represent the worldwide network in computer network diagrams. Economically, the main appeal of cloud computing is that customers only use what they need, and only pay for what they actually use. Resources are available to be accessed from the cloud at any time, and from any location via the internet. There’s no need to worry about how things are being maintained behind the scenes – you simply purchase the IT service you require as you would any other utility. Because of this, cloud computing has also been called utility computing, or ‘IT on demand’. This new, web-based generation of computing utilizes remote servers housed in highly secure data centers for data storage and management, so organizations no longer need to purchase and look after their IT solutions in-house.

Cloud computing provides the facility to access shared resources and common infrastructure, offering services on demand over the network to perform operations that meet changing business needs. The location of physical resources and devices being accessed are typically not known to the end user. It also provides facilities for users to develop, deploy and manage their applications ‘on the cloud’, which entails virtualization of resources that maintains and manages itself.

**Cloud Architecture:**

Cloud computing architecture, just like any other system, is categorized into two main sections:

Front End and Back End. Front End can be end user or client or any application (i.e. web browser etc.) which is using cloud services. Back End is the network of servers with any computer program and data storage system. It is usually assumed that cloud contains infinite storage capacity for any software available in market. Cloud has different applications that are hosted on their own dedicated server farms. Cloud has centralized server administration system. Centralized server administers the system, balances client supply, adjusts demands, monitors traffic and avoids congestion. This server follows protocols, commonly known as middleware. Middleware controls the communication of cloud network among them. Cloud Architecture runs on a very important assumption, which is mostly true. The assumption is that the demand for resources is not always consistent from client to cloud. Because of this reason the servers of cloud are unable to run at their full capacity. To avoid this scenario, server virtualization technique is applied. In sever virtualization, all physical servers are virtualized and they run multiple servers with either same or different application. As one physical server acts as multiple physical servers, it curtails the need for more physical machines. As a matter of fact, data is the most important part of cloud computing; thus, data security is the top most priority in all the data operations of cloud. Here, all the data are backed up at multiple locations. This astoundingly increases the data storage to multiple times in cloud compared with a regular system. Redundancy of data is crucial, which is a must-have attribute of cloud computing.



**Security in cloud computing**

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions.

Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties.

An organization’s security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), and all the way to the information and applications (application security). Additionally controls are implemented at the people and process levels, such as separation of duties and change management, respectively.

The security responsibilities of both the provider and the consumer greatly differ between cloud service models. Amazon’s AWS EC2 infrastructure as a service offering, as an example, includes vendor responsibility for security up to the hypervisor, meaning they can only address security controls such as physical security, environmental security, and virtualization security. The consumer, in turn, is responsible for security controls that relate to the IT system (instance) including the operating system, applications, and data.

The inverse is true for Salesforce.com’s customer resource management (CRM) SaaS offering.

Because the entire ‘stack’ is provided by Salesforce.com, the provider is not only responsible for the physical and environmental security controls, but it must also address the security controls on the infrastructure, the applications, and the data. This alleviates much of the consumer’s direct operational responsibility.

** Need of security in cloud computing**

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company. Another argument, made by the Jericho Forum, is: "It could be easier to lock down information if it's administered by a third party rather than in-house, if companies are worried about insider threats… In addition, it may be easier to enforce security via contracts with online services providers than via internal controls."

Concerns in this category include:

TS1. **VM-level attacks**. Potential vulnerabilities in the hypervisor or VM technology used by cloud vendors are a potential problem in multi-tenant architectures. Vulnerabilities have appeared in VMWare, Xen, and Microsoft’s Virtual PC and Virtual Server. Vendors such as Third Brigade mitigate potential VM-level vulnerabilities through monitoring and firewalls.

TS2. **Cloud provider vulnerability**. These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability in salesforce.com. For instance, there have been a couple of recent Google Docs vulnerabilities. The Google response to one of them is here. There is nothing new in the nature of these vulnerabilities; only their setting is novel. In fact, IBM has repositioned its Rational AppScan tool, which scans for vulnerabilities in web services as a cloud security service (see Blue Cloud Initiative).

TS3. **Phishing cloud provider.** Phishers and other social engineers have a new attack vector, as the Salesforce phishing incident shows.

TS4. **Expanded network attack surface.** The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases. For instance, shows an example of how the cloud might attack the machine connecting to it.

TS5. **Authentication and Authorization.** The enterprise authentication and authorization framework does not naturally extend into the cloud. How does a company meld its existing framework to include cloud resources? Furthermore, how does an enterprise merge cloud security data (if even available) with its own security metrics and policies?

TS6. **Forensics in the cloud.** This blog posting on the CLOIDIFIN project summarizes the difficulty of cloud forensic investigations: “Traditional digital forensic methodologies permit investigators to seize equipment and perform detailed analysis on the media and data recovered. The likelihood therefore, of the data being removed, overwritten, deleted or destroyed by the perpetrator in this case is low. More closely linked to a CC environment would be businesses that own and maintain their own multi-server type infrastructure, though this would be on a far smaller scale in comparison. However, the scale of the cloud and the rate at which data is overwritten is of concern.”

** Current security scenario**

** Limitations and drawbacks on security features**

** Solutions to these security problems**