Introduction to Cloud Computing

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 defined 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.

History:

The word cloud is used as a metaphor for the Internet, based on the standardized use of a cloud-like shape to denote a network on telephony schematics and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents. The cloud symbol was used to represent the Internet as early as 1994.

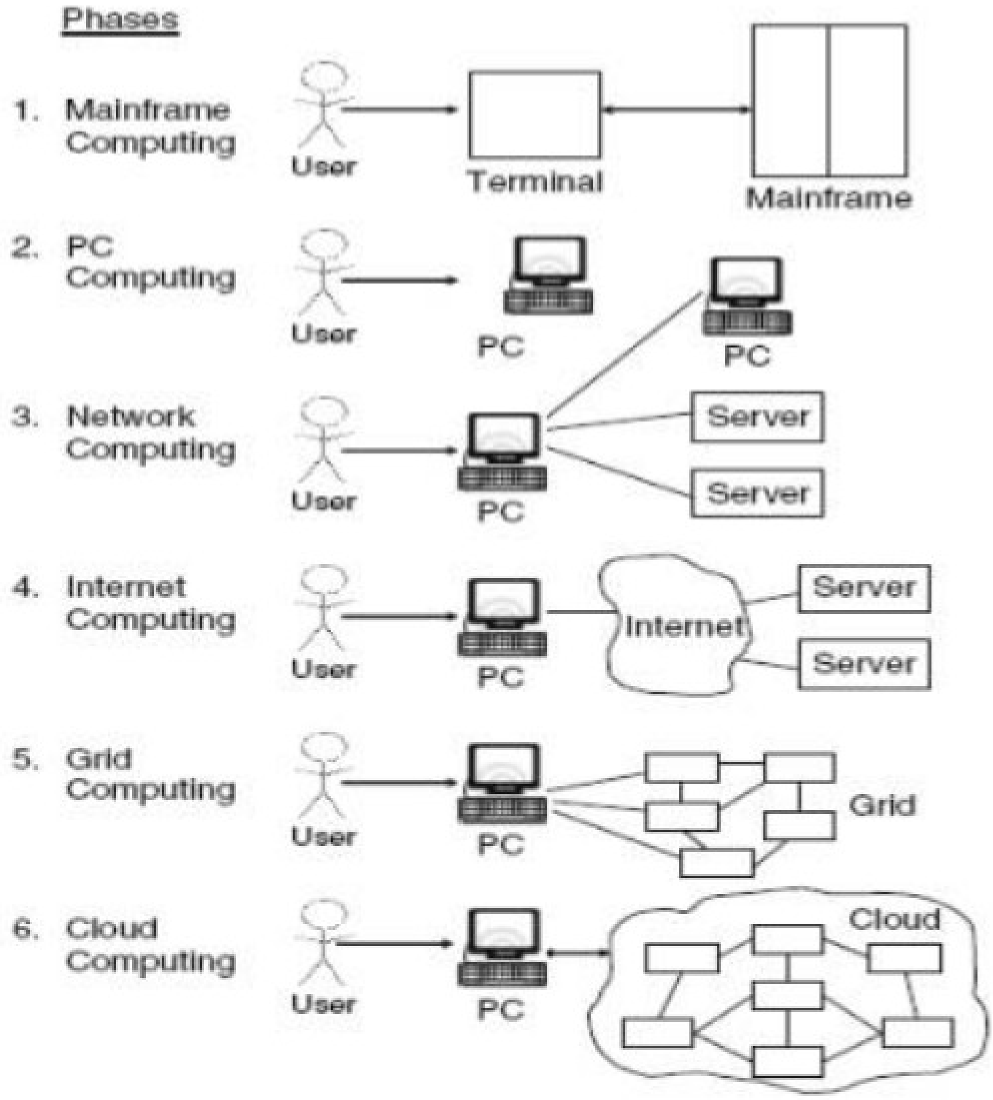

Fig: Cloud computing evolution

In the 1990s, telecommunications companies, who previously offered primarily dedicated point-to-point data circuits, began offering virtual private network (VPN) services with comparable quality of service but at a much lower cost. By switching traffic to balance utilization as they saw fit, they were able to utilize their overall network bandwidth more effectively. The cloud symbol was used to denote the demarcation point between that which was the responsibility of the provider and that which was the responsibility of the users. Cloud computing extends this boundary to cover servers as well as the network infrastructure.

The underlying concept of cloud computing dates back to the 1950s; when large-scale mainframe became available in academia and corporations, accessible via thin clients /terminal computers. Because it was costly to buy a mainframe, it became important to find ways to get the greatest return on the investment in them, allowing multiple users to share both the physical access to the computer from multiple terminals as well as to share the CPU time, eliminating periods of inactivity, which became known in the industry as time-sharing.

As in the earliest stages, the term “cloud” was used to represent the computing space between the provider and the end user.

In 1997, Professor Ramnath Chellapa of Emory University and the University of South California defined cloud computing as the new “computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone.” This has become the basis of what we refer to today when we discuss the concept of cloud computing.

Some people think cloud computing is the next big thing in the world of IT. Others believe it is just another variation of the utility computing model that has been repackaged in this decade as something new and cool.

One of the first milestones for cloud computing was the arrival of Salesforce.com in 1999, which pioneered the concept of delivering enterprise applications via a simple website. The services firm paved the way for both specialist and mainstream software firms to deliver applications over the internet.

The next development was Amazon Web Services in 2002, which provided a suite of cloud- based services including storage, computation and even human intelligence through the Amazon Mechanical Turk. Then in 2006, Amazon launched its Elastic Compute cloud (EC2) as a commercial web service that allows small companies and individuals to rent computers on which to run their own computer applications.

Another big milestone came in 2009, as Web 2.0 hit its stride, and Google and others started to offer browser-based enterprise applications, though services such as Google Apps.

The most important contribution to cloud computing has been the emergence of "killer apps" from leading technology giants such as Microsoft and Google. When these companies deliver services in a way that is reliable and easy to consume, the knock-on effect to the industry as a whole is a wider general acceptance of online services.

Then came mature virtualization technologies in 2009-till date that changed landscape of cloud computing. Private, Public and hybrid cloud were dominant cloud types in Enterprise Level. Server and Storage Consolidation were major works in the cloud industry.

Characteristics of Cloud Computing

The essential characteristics can be elaborated as follows:

- **On-demand self-service**: Users are able to provision cloud computing resources without requiring human interaction, mostly done though a web-based self-service portal (management console).

- **Broad network access**: Cloud computing resources are accessible over the network, supporting heterogeneous client platforms such as mobile devices and workstations.

- **Resource pooling:** Service multiple customers from the same physical resources, by securely separating the resources on logical level.

- **Rapid elasticity:** Resources are provisioned and released on-demand and/or automated based on triggers or parameters. This will make sure your application will have exactly the capacity it needs at any point of time.

- **Measured service:** Resource usage are monitored, measured, and reported (billed) transparently based on utilization. In short, pay for use.

As we see, cloud computing is much more than just virtualization. It’s really about utilizing technology “as a service”. Users need little to no knowledge on the details of how a particular service is implemented, on which hardware, on how many CPU’s, and so on. All that’s important for a user is to have good understanding of what the service offers—and what it does not—and how to operate the self-service portal.

Advantages of Cloud Computing

- **Trade capital expense for variable expense:** Instead of having to invest heavily in data centers and servers before you know how you’re going to use them, you can pay only when you consume computing resources, and pay only for how much you consume.

- **Benefit from massive economies of scale:** By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers is aggregated in the cloud, providers such as AWS can achieve higher economies of scale, which translates into lower pay as-you-go prices.

- **Stop guessing capacity:** Eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often end up either sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little capacity as you need, and scale up and down as required with only a few minutes’ notice.

- **Increase speed and agility:** In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

- **Stop spending money running and maintaining data centers:** Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking, and powering servers.

- **Go global in minutes:** Easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide lower latency and a better experience for your customers at minimal cost.

Disadvantages of Cloud Computing:

1. Downtime
2. Security and privacy
3. Vulnerability to attack
4. Limited control and flexibility
5. Vendor lock-in
6. Costs

1) Downtime

Downtime is often cited as one of the biggest disadvantages of cloud computing. Since cloud computing systems are internet-based, service outages are always an unfortunate possibility and can occur for any reason.
Can your business afford the impacts of an outage or slowdown? An outage on Amazon Web Services in 2017 cost publicly traded companies up to$150 million dollars and no organization is immune, especially when critical business processes cannot afford to be interrupted.

Best Practices for minimizing planned downtime in a cloud environment:

- Design services with high availability and disaster recovery in mind. Leverage the multi- availability zones provided by cloud vendors in your infrastructure.

- If your services have a low tolerance for failure, consider multi-region deployments with automated failover to ensure the best business continuity possible.

- Define and implement a disaster recovery plan in line with your business objectives that provide the lowest possible recovery time (RTO) and recovery point objectives (RPO).

- Consider implementing dedicated connectivity such as AWS Direct Connect, Azure Express Route, or Google Cloud’s Dedicated Interconnect or Partner Interconnect. These services provide a dedicated network connection between you and the cloud service point of presence. This can reduce exposure to the risk of business interruption from the public internet.

2) Security and Privacy

Any discussion involving data must address security and privacy, especially when it comes to managing sensitive data. We must not forget what happened at Code Space and the hacking of their AWS EC2 console, which led to data deletion and the eventual shutdown of the company. Their dependence on remote cloud-based infrastructure meant taking on the risks of outsourcing everything.

Of course, any cloud service provider is expected to manage and safeguard the underlying hardware infrastructure of a deployment. However, your responsibilities lie in the realm of user access management, and it’s up to you to carefully weigh all the risk scenarios.

Though recent breaches of credit card data and user login credentials are still fresh in the minds of the public, steps have been taken to ensure the safety of data. One such example is the General Data Protection Rule (GDPR),recently enacted in the European Union to provide users more control over their data. Nonetheless, you still need to be aware of your responsibilities and follow best practices.

Best practices for minimizing security and privacy risks:

- Understand the shared responsibility modelof your cloud provider.

- Implement securityat every level of your deployment.

- Know who is supposed to have access to each resource and service and limit access to least privilege.

- Make sure your team’s skills are up to the task: Solid security skills for your cloud teams are one of the best ways to mitigate security and privacy concerns in the cloud.

- Take a risk-based approach to securing assets used in the cloud Extend security to the device.

- Implement multi-factor authentication for all accounts accessing sensitive data or systems.

3) Vulnerability to Attack

In cloud computing, every component is online, which exposes potential vulnerabilities. Even the best teams suffer severe attacks and security breaches from time to time. Since cloud computing is built as a public service, it's easy to run before you learn to walk. After all, no one at a cloud vendor checks your administration skills before granting you an account: all it takes to get started is generally a valid credit card.

Best practices to help you reduce cloud attacks:

- Make security a core aspect of all IT operations.

- Keep ALL your teams up to date with cloud security best practices.

- Ensure security policies and procedures are regularly checked and reviewed.

- Proactively classify information and apply access control.

- Use cloud services such as AWS Inspector, AWS CloudWatch, AWS CloudTrail, and AWS Config to automate compliance controls.

- Prevent data exfiltration.

- Integrate prevention and response strategies into security operations.

- Discover rogue projects with audits.

- Remove password access from accounts that do not need to log in to services.

- Review and rotate access keys and access credentials.

- Follow security blogs and announcements to be aware of known attacks.

- Apply security best practices for any open source software that you are using.

These practices will help your organization monitor for the exposure and movement of critical data, defend crucial systems from attack and compromise, and authenticate access to infrastructure and data to protect against further risks.

4) Limited control and flexibility

To varying degrees (depending on the particular service), cloud users may find they have less control over the function and execution of services within a cloud-hosted infrastructure. A cloud provider's end-user license agreement (EULA) and management policies might impose limits on what customers can do with their deployments. Customers retain control of their applications, data, and services, but may not have the same level of control over their backend infrastructure.

Best practices for maintaining control and flexibility:

- Consider using a cloud provider partner to help with implementing, running, and supporting cloud services.

- Understanding your responsibilities and the responsibilities of the cloud vendor in the shared responsibility model will reduce the chance of omission or error.

- Make time to understand your cloud service provider's basic level of support. Will this service level meet your support requirements? Most cloud providers offer additional support tiers over and above the basic support for an additional cost.

- Make sure you understand the service level agreement (SLA) concerning the infrastructure and services that you're going to use and how that will impact your agreements with your customers.

5) Vendor Lock-In

Vendor lock-in is another perceived disadvantage of cloud computing. Differences between vendor platforms may create difficulties in migrating from one cloud platform to another, which could equate to additional costs and configuration complexities. Gaps or compromises made during migration could also expose your data to additional security and privacy vulnerabilities.

Best practices to decrease dependency:

- Design with cloud architecture best practices in mind. All cloud services provide the opportunity to improve availability and performance, decouple layers, and reduce performance bottlenecks. If you have built your services using cloud architecture best practices, you are less likely to have issues porting from one cloud platform to another.

- Properly understanding what your vendors are selling can help avoid lock-in challenges.

- Employing a multi-cloud strategy is another way to avoid vendor lock-in. While this may add both development and operational complexity to your deployments, it doesn’t have to be a deal breaker. Training can help prepare teams to architect and select best-fit services and technologies.

- Build in flexibilityas a matter of strategy when designing applications to ensure portability now and in the future.

6) Costs

Adopting cloud solutions on a small scale and for short-term projects can be perceived as being expensive. Pay-as-you-go cloud services can provide more flexibility and lower hardware costs, however, the overall price tag could end up being higher than you expected. Until you are sure of what will work best for you, it’s a good idea to experiment with a variety of offerings. You might also make use of the cost calculators made available by providers likeAmazon Web ServicesandGoogle Cloud Platform.

Best practices to reduce costs:

- Try not to over-provision, instead of looking into using auto-scaling services
- Scale DOWN as well as UP
- Prepay if you have a known minimum usage
- Stop your instances when they are not being used
- Create alerts to track cloud spending

Disadvantages of Cloud Computing: Closing Thoughts

Many organizations benefit from the agility, scale, and pay-per-use billing that cloud services offer. However, as with any infrastructure service, the suitability of cloud computing for your specific use case should be assessed in a risk-based evaluation. Build in time for research and planningto understand how the cloud will affect your business.

Cloud-Unique Threats and Risks

The following vulnerabilities are a result of a CSP's implementation of the five cloud computing characteristics. These vulnerabilities do not exist in classic IT data centers.

1. Consumers Have Reduced Visibility and Control. When transitioning assets/operations to the cloud, organizations lose some visibility and control over those assets/operations. When using external cloud services, the responsibility for some of the policies and infrastructure moves to the CSP.

The actual shift of responsibility depends on the cloud service model(s) used, leading to a paradigm shift for agencies in relation to security monitoring and logging. Organizations need to perform monitoring and analysis of information about applications, services, data, and users, without using network-based monitoring and logging, which is available for on-premises IT.

2. On-Demand Self Service Simplifies Unauthorized Use. CSPs make it very easy to provision new services. The on-demand self-service provisioning features of the cloud enable an organization's personnel to provision additional services from the agency's CSP without IT consent. The practice of using software in an organization that is not supported by the organization's IT department is commonly referred to as shadow IT.

Due to the lower costs and ease of implementing PaaS and SaaS products, the probability of unauthorized use of cloud services increases. However, services provisioned or used without IT's knowledge present risks to an organization. The use of unauthorized cloud services could result in an increase in malware infections or data exfiltration since the organization is unable to protect resources it does not know about. The use of unauthorized cloud services also decreases an organization's visibility and control of its network and data.

3. Internet-Accessible Management APIs can be Compromised. CSPs expose a set of application programming interfaces (APIs) that customers use to manage and interact with cloud services (also known as the management plane). Organizations use these APIs to provision, manage, orchestrate, and monitor their assets and users. These APIs can contain the same software vulnerabilities as an API for an operating system, library, etc. Unlike management APIs for on-premises computing, CSP APIs are accessible via the Internet exposing them more broadly to potential exploitation.

Threat actors look for vulnerabilities in management APIs. If discovered, these vulnerabilities can be turned into successful attacks, and organization cloud assets can be compromised. From there, attackers can use organization assets to perpetrate further attacks against other CSP customers.

4. Separation Among Multiple Tenants Fails. Exploitation of system and software vulnerabilities within a CSP's infrastructure, platforms, or applications that support multi-tenancy can lead to a failure to maintain separation among tenants. This failure can be used by an attacker to gain access from one organization's resource to another user's or organization's assets or data. Multi-tenancy increases the attack surface, leading to an increased chance of data leakage if the separation controls fail.

This attack can be accomplished by exploiting vulnerabilities in the CSP's applications, hypervisor, or hardware, subverting logical isolation controls or attacks on the CSP's management API. To date, there has not been a documented security failure of a CSP's SaaS platform that resulted in an external attacker gaining access to tenants' data.

No reports of an attack based on logical separation failure were identified; however,proof-of-concept exploits have been demonstrated.

5. Data Deletion is Incomplete. Threats associated with data deletion exist because the consumer has reduced visibility into where their data is physically stored in the cloud and a reduced ability to verify the secure deletion of their data. This risk is concerning because the data is spread over a number of different storage devices within the CSP's infrastructure in a multi-tenancy environment. In addition, deletion procedures may differ from provider to provider. Organizations may not be able to verify that their data was securely deleted and that remnants of the data are not available to attackers. This threat increases as an agency uses more CSP services.

Cloud and On-Premise Threats and Risks

The following are risks that apply to both cloud and on-premise IT data centers that organizations need to address.

6. Credentials are Stolen. If an attacker gains access to a user's cloud credentials, the attacker can have access to the CSP's services to provision additional resources (if credentials allowed access to provisioning), as well as target the organization's assets. The attacker could leverage cloud computing resources to target the organization's administrative users, other organizations using the same CSP, or the CSP's administrators. An attacker who gains access to a CSP administrator's cloud credentials may be able to use those credentials to access the agency's systems and data.

Administrator roles vary between a CSP and an organization. The CSP administrator has access to the CSP network, systems, and applications (depending on the service) of the CSP's infrastructure, whereas the consumer's administrators have access only to the organization's cloud implementations. In essence, the CSP administrator has administration rights over more than one customer and supports multiple services.

7. Vendor Lock-In Complicates Moving to Other CSPs. Vendor lock-in becomes an issue when an organization considers moving its assets/operations from one CSP to another. The organization discovers the cost/effort/schedule time necessary for the move is much higher than initially considered due to factors such as non-standard data formats, non-standard APIs, and reliance on one CSP's proprietary tools and unique APIs.

This issue increases in service models where the CSP takes more responsibility. As an agency uses more features, services, or APIs, the exposure to a CSP's unique implementations increases. These unique implementations require changes when a capability is moved to a different CSP. If a selected CSP goes out of business, it becomes a major problem since data can be lost or cannot be transferred to another CSP in a timely manner.

8. Increased Complexity Strains IT Staff. Migrating to the cloud can introduce complexity into IT operations. Managing, integrating, and operating in the cloud may require that the agency's existing IT staff learn a new model. IT staff must have the capacity and skill level to manage, integrate, and maintain the migration of assets and data to the cloud in addition to their current responsibilities for on-premises IT.

Key management and encryption services become more complex in the cloud. The services, techniques, and tools available to log and monitor cloud services typically vary across CSPs, further increasing complexity. There may also be emergent threats/risks in hybrid cloud implementations due to technology, policies, and implementation methods, which add complexity. This added complexity leads to an increased potential for security gaps in an agency's cloud and on-premises implementations.

9. Insiders Abuse Authorized Access. Insiders, such as staff and administrators for both organizations and CSPs, who abuse their authorized access to the organization's or CSP's networks, systems, and data are uniquely positioned to cause damage or exfiltrate information.

The impact is most likely worse when using IaaS due to an insider's ability to provision resources or perform nefarious activities that require forensics for detection. These forensic capabilities may not be available with cloud resources.

10. Stored Data is Lost. Data stored in the cloud can be lost for reasons other than malicious attacks. Accidental deletion of data by the cloud service provider or a physical catastrophe, such as a fire or earthquake, can lead to the permanent loss of customer data. The burden of avoiding data loss does not fall solely on the provider's shoulders. If a customer encrypts its data before uploading it to the cloud but loses the encryption key, the data will be lost. In addition, inadequate understanding of a CSP's storage model may result in data loss. Agencies must consider data recovery and be prepared for the possibility of their CSP being acquired, changing service offerings, or going bankrupt.

This threat increases as an agency uses more CSP services. Recovering data on a CSP may be easier than recovering it at an agency because an SLA designates availability/uptime percentages. These percentages should be investigated when the agency selects a CSP.

11. CSP Supply Chain is Compromised: If the CSP outsources parts of its infrastructure, operations, or maintenance, these third parties may not satisfy/support the requirements that the CSP is contracted to provide with an organization. An organization needs to evaluate how the CSP enforces compliance and check to see if the CSP flows its own requirements down to third parties. If the requirements are not being levied on the supply chain, then the threat to the agency increases.

This threat increases as an organization uses more CSP services and is dependent on individual CSPs and their supply chain policies.

12. Insufficient Due Diligence Increases Cybersecurity Risk

Organizations migrating to the cloud often perform insufficient due diligence. They move data to the cloud without understanding the full scope of doing so, the security measures used by the CSP, and their own responsibility to provide security measures. They make decisions to use cloud services without fully understanding how those services must be secured.

Wrapping Up and Looking Ahead

It is important to remember that CSPs use a shared responsibility model for security. The CSP accepts responsibility for some aspects of security. Other aspects of security are shared between the CSP and the consumer. Finally, some aspects of security remain the sole responsibility of the consumer. Effective cloud security depends on knowing and meeting all consumer responsibilities. Consumers' failure to understand or meet their responsibilities is a leading cause of security incidents in cloud-based systems.