Cloud Computing

The term "cloud" is analogical to "Internet". The term "Cloud Computing" is based on cloud drawings used in the past to represent telephone networks and later to depict Internet. Cloud computing is Internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customers on a pay-as-you-use basis. All information that a digitized system has to offer is provided as a service in the cloud computing model. Users can access these services available on the "Internet cloud" without having any previous know- how on managing the resources involved. Thus, users can concentrate more on their core business processes rather than spending time and gaining knowledge on resources needed to manage their business processes.Cloud computing customers do not own the physical infrastructure; rather they rent the usage from a third-party provider. This helps them to avoid huge capital investments. They consume resources as a service and pay only for resources that they use. Most cloud computing infrastructures consist of services delivered through shared resources. This increases efficiency as servers are not unnecessarily left idle, which can reduce costs significantly while increasing the speed of application development.

Short Comings of Cloud Computing :

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 ExpressRoute, 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.

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.

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 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 a 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.

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 like Amazon Web Services and Google Cloud Platform.

Summary of Cloud Compting

Cloud Computing refers to both the applications delivered as services over the Internet and the scalable hardware and systems software that provide those services. The services themselves have long been referred to as Software as a Service (SaaS).