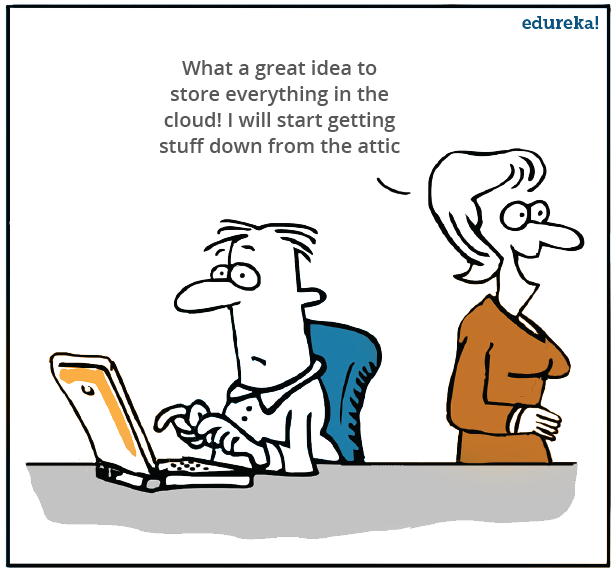
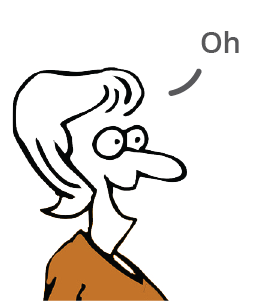
## Cloud Security

Cloud was a hype in 2010-2011, but today it has become a necessity. With a lot of organisations moving to cloud, the need for cloud security has become the top most priority.

But before that, those of you who are new to cloud computing, let’s have a quick look at what cloud computing is,

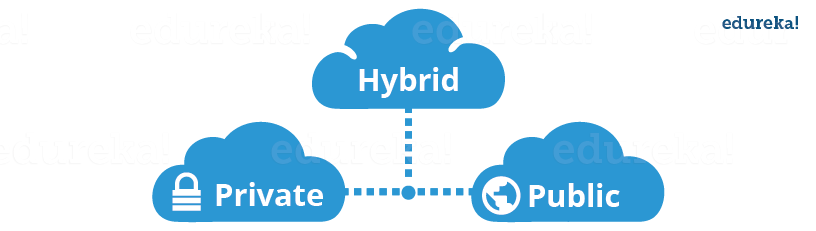


## **What is Cloud Computing?**



Cloud Computing often referred to as “the cloud”, in simple terms means storing or accessing your data and programs over the internet rather than your own hard drive.

Let’s discuss the types of clouds now:



## **Public Cloud**

In a public cloud deployment mode, the services which are deployed are open for public use and generally public cloud services are free. Technically there maybe no difference between a public cloud and a private cloud, but the security parameters are very different, since the public cloud is accessible by anyone there is a more risk factor involved with the same.

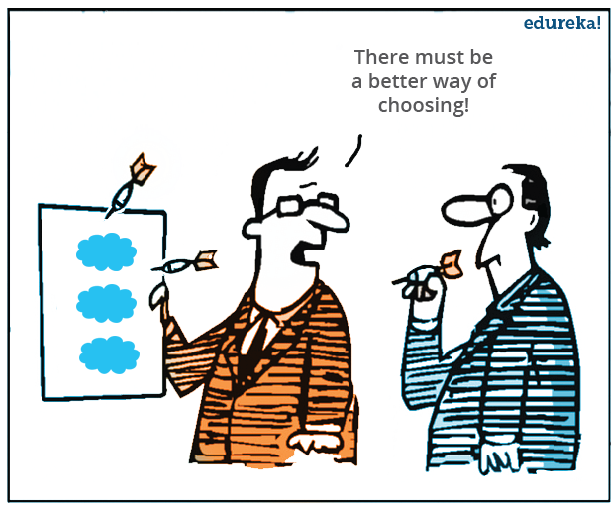
## **Private Cloud**

A private cloud is operated solely for a single organization, it can be done by the same organization or a third-party organization. But usually the costs are high when you are using your own cloud since the hardware would be updated periodically, security also has to be kept in check since new threats come up every day.

## **Hybrid Cloud**

A hybrid cloud consists the functionalities of both private and public cloud

## **How do customers decide between public, private, and hybrid clouds?**

Well, it depends on the user requirement that is, if the user feels that his information is too sensitive to be on any system rather than their own, they would opt for a private cloud

The best example for this could be DropBox, in their early days they started by using AWS S3 as their backend for storing objects, but now they have created their own storage technology which they monitor themselves.

Why they did this?

Well they got so big, that public cloud pricing didn’t make sense any longer. According to them their software and hardware optimizations are more economically viable than storing their stuff on Amazon S3.

But then if you are not a biggie like DropBox, and you are still on private infrastructure, maybe its time you think, Why not public cloud?

Now why will a customer use public cloud?

First of all the pricing is pretty less, compared to the investment that a company would need to setup their own servers.

Secondly, when you are linked with a reputed Cloud Provider, the Availability of your files on the Cloud becomes higher.

Still confused whether you want to store your files or data on private or public cloud.

Let me tell you about hybrid cloud, with hybrid cloud you can keep your more “precious” data on your private infrastructure and the rest on the public cloud, this would be a “hybrid cloud”

So concluding, it all depends on the user requirement based on which he shall choose between public, private and hybrid cloud.

## **Can cloud computing security accelerate customer movement to the cloud?**

research was conducted for companies who are a little reluctant to move to cloud, and as you can clearly see in the above image that the foremost reason is security.

Now this does not mean that the cloud is not secure, but people have this perception. So basically if you can assure people that cloud is safe,  some acceleration may take place in the movement towards the cloud.

## **How do CIOs reconcile the tension between risk, cost, and user experience?**

Well I read this somewhere, Cloud Security is a mixture of science and art.

Confused? Well, its an art of knowing till what extent should you put security on a service so that the user experience does not diminish.

For example: Say suppose you have an application, and to make it secure you are asking the username and password at every operation, which makes sense as far as security is concerned, but then it hinders user experience.

So it’s an art to know when to stop, but at the same time it’s science, because you need to create algorithms or tools that provide the maximum security to your customer’s data.

Now when any new thing comes into the picture, people get skeptical about it.

There are a lot of “risks” that people think cloud computing has, let’s address these risks one by one:

## 1. Cloud is insecure

Most of the times whenever you would talk about cloud, there would be a lot of people saying, the data is more secure on their own infrastructure rather than say some AWS server with AWS security.

Well this might make sense if the company would just focus on their private cloud’s security which obviously is not the case. But if the company does that, when will they focus on their own goals?

Let’s talk about Cloud Providers, say AWS (the largest of them all), don’t you think AWS’s sole purpose is to make your data the most secure? Why, because that is what they are being paid for.

Also a fun fact, Amazon has hosted their own e-commerce website on AWS, which clears the air on whether AWS is reliable.

Cloud providers live, eat and breathe cloud security.

## **2. There are more breaches in the cloud**

A study from Spring Alert Logic Report of 2014 shows that the cyber attacks in 2012-2013 were both targeted at private clouds and public clouds, but the private clouds were more susceptible to the attacks. Why? Because companies which setup their own servers are not that equipped compared to AWS or Azure or any other Cloud Provider for that matter.

## **3. Single tenant systems are more secure than multi-tenant systems.**

Well if you think logically, don’t you think that with multi-tenant systems you have an additional layer of security attached to it. Why? Because your content will be logically isolated from the rest of the tenants or users on the system, which is not there if you are using single-tenant systems. Therefore, in case a hacker wants to go through your system, he has to go through one additional layer of security.

Concluding, these are all myths and also considering the saving in investments that you will be doing when you move your data to cloud and also the other benefits, it far outweighs the risks involved in cloud security.

Having said that, let’s move on to the focus of today’s discussion, how do your Cloud providers handle security.

So let’s take an example here and assume that you are using an app for social networking. You click on some random link and nothing happens. Later you come to know, that spam messages are being sent from your account to all your contacts that are connected with you on that application.

But then before you could even drop a mail or complain to the app’s support, they would already know the problem and would be up and running to solve it. How? Let’s understand.

So basically Cloud Security has three stages:

* Monitoring Data
* Gaining Visibility
* Managing Access

The Cloud Monitoring tool which constantly analyses the data flow on your cloud application would alert as soon as some “weird” stuff starts happening on your application. How do they assess the “weird” stuff?



Well the cloud monitoring tool would have advanced machine learning algorithms which logs normal system behavior.

So any deviation from the normal system behavior would be a red flag, also the known hacking techniques are listed in its databas. So taking all of this into one picture your monitoring tool raises an alert whenever something fishy happens.

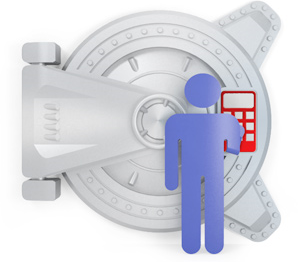
Now once you would come to know there is something “not normal” going on, you would want to know when and where, comes stage 2, **gaining visibility**.

This can be done using tools which gives you the visibility to the data which is coming in and out of your cloud. Using these you can track not only where the fault has occurred, but also “who” is responsible for the same. How?

Well these tools look for patterns, and will list all the activities which are suspicious and hence see which user is responsible for the same.

Now the individual responsible would first have to be removed from the system right?

Comes Stage 3, **managing access.**



The tools that will be managing access, will list all the users who are there on the system. Hence you can track this individual and wipe him out of the system.

Now how did this individual or hacker got an admin access of your system?

Most probably the password to your management console was cracked by the hacker and created an admin role for himself from the Access Management tool, and the rest became history.

Now what would your Cloud provider do after this? They would learn from this and evolve so that it never happens again.

Now this example is just for the sake of understanding, usually no hacker can get access of your password just like that.

The thing to focus here is that the cloud company evolved from this break in, they took measures to improve their cloud security so that the same can never be repeated.

Now all cloud providers follow these stages. Let’s talk about the largest cloud provider, AWS.



Does AWS follow these stages for aws cloud security? Let’s have a look:

For Cloud monitoring, AWS has **CloudWatch**

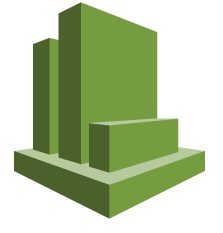
For data visibility, AWS has **CloudTrail**

And for managing access, AWS has **IAM**

These are the tools that AWS uses, let’s have a closer look at how they function.

## **CloudWatch**

It gives you the ability to analyze the data coming in and out of your AWS resources. It has the following features related to cloud security:

* Monitor EC2 and other AWS resources:
  + Without installing additional software you can monitor your EC2’s performance using AWS CloudWatch.
* The ability to monitor custom metrics:
  + You can create custom metrics, and monitor them through CloudWatch.
* Monitor and store logs:
  + You can monitor and store logs related to the activities happening on your AWS resources.
* Set Alarms:
  + You can set alarms to specific triggers, such as an activity that needs immediate attention etc.
* View Graphs and Statistics:
  + You can visualize this data in form of graphs and other visual representations.
* Monitor and React to Resource Changes:
  + It can be configured in a way to respond to changes in the availability of a resource or when a resource is not functioning properly.

## **CloudTrail**

CloudTrail is a logging service which can be used to log the history of API calls. It can also be used to identify which user from AWS Management Console requested the particular service. Taking reference from our example, this is the tool from where you will identify the notorious “hacker”.

## 

## **IAM**

Identity and Access Management(IAM) is used to grant shared access to your AWS account. It has the following functions:

* Granular permissions:
  + It can be used to grant access rights to different kind of users at a very cellular level. For e.g: You can grant read access to a specific user, and a read-write access to a different user.
* Secure access to applications running on EC2 environment:
  + IAM can be used to give secure access by making the user to enter the credentials, to access the respective EC2 resources.
* Free to use:
  + AWS has made IAM services free to use with any aws service which it is compatible.

## AWS Shield

It is managed DDOS denial service. Let’s quickly look at, what DDoS is?

DDoS is basically overloading your website with irrelevant traffic with the intention of taking your website down. How does it work? Hackers create a bot-net by infecting numerous computers connected on the internet, how? Remember those weird emails that you get sometimes on your mail? Lottery, medical aid etc. Basically they make you click on something, which installs a malware on your computer, which is then triggered to make your computer, a plus one, in the irrelevant traffic.

Insecure about your web application? Don’t be AWS Shield is here.

It offers two type of services:

1. Standard
2. Advanced

The Standard package is free for all the users, and your web application on AWS is automatically covered with this package by default. It includes the following features:

* Quick Detection
  + Detects malicious traffic on the go by using anomaly algorithms.
* Inline Mitigation Attacks
  + Automatic mitigation techniques are built into AWS Shield giving you protection against common attacks.
* Add Custom Rules to support your application.

Not enough? There is an Advanced package too. With a little extra cost, you can cover your Elastic Load Balancers, Route 53 and CloudFront resources.

What all is included? Let’s have a look:

* Enhanced Detection
  + It includes additional techniques like resource specific monitoring, and also provides granular detection of DDoS attacks.
* Advanced Attack Mitigation
  + More sophisticated automatic mitigations.
* Visibility and Attack Notification
  + Real time notifications by using CloudWatch.
* Specialized Support
  + 24×7 support from a special DDoS response team.
* DDoS Cost Protection
  + Prevents cost spikes from overloading by DDoS attacks.

In conclusion, any cloud provider for its success follows the highest standards in Cloud Security, and gradually if not immediately, people who still don’t have faith on Cloud will understand it is a necessity to move on it.