Miguel Angel Castillo Espitia

The Security Strategy we could follow is the following:

Thanks to the multiple availability zones that cloud computing, specifically AWS, provides us, we can reach a great **scalability** in all days, especially in the most demanding days, since the information on cloud computing is shared online, the information about user's purchases, user's logs may be collected from the servers we hire, so if a server gets full of memory for example, we can scale the process by extending the server memory, or by assigning more servers to that process.

Since the original model was based on national presence hosts with its own data center, the reachability of the company was limited to a national audience, while with cloud computing, the **reachability** will be world-wide. Thanks to the shared-information cloud computing´s feature, our clients just need to access to internet to use the e-shop, this probably will increase the number of users of the company.

AWS also provides us the possibility of use or/and deploy the services or/and servers as we want, it means we can deploy the servers and use them as we need them, then there won't be a possible waste of memory or resources by an incessant running. This gives us a **flexibility** to improve the company services and resources.

Another of the benefits that the cloud computing gives us is that its servers recollect all information about the users and developers, information such as its location, what the users view at the e-shop, and for how long they use or/and stay on the page, i.e. we can manage **the costs** based on that traffic data, and even improve the user experience by using the information about what they see at the page, to make better suggestions on what the user is likely to see or buy.

In addition to all the improvements provided by cloud computing mentioned above, here are some other benefits that the company will obtain when migrating to the cloud service:

- The authentication that AWS works with, it's based on a multifactor authentication, such as a password, a token or pin and a possible third authentication factor as a fingerprints and others.
- AWS will provide us integrity over the user's data by using secure protocol such as HTTPS with digital certificate to validate its identity.
- For our employers there will be a least privilege philosophy, which means that the worker of the company will be given the minimum authorizations or permissions needed to perform his work.
- Also, thanks to a possible encrypted channel to transfer the information or to VPN (Virtual Private Network) which is a private network that gives a secure communication channel between the user and the server, we will be able to give to the user the confidentiality that it's information deserves