Security in the Cloud

If you are asking people about their concerns about going to the cloud, most come up with security concerns. However, considering the security part of a cloud provider shows that the cloud is secure, and customers can secure their data and instances even more if they wish.  
Security of your data and applications start with the physical security of the data centers. Big Companies like Amazon, Google, Microsoft, … have many years of experience ho to design and build large scale infrastructures. They got their knowledge from their own data centers before providing datacenters for everyone available through the cloud. Therefore, they have way more experience than most. The datacenters are normally placed at locations with enough power supply and close to big cities/areas to run them and provide the best possible service. These buildings have a pretty secure security measurement such that only authorized persons get access, and they always have to use a two-factor authorization or even more secure measures like biometric authentication. Nowadays the datacenters are sometimes even placed in residential neighborhoods with no signings or markings, making them extra secure. The cloud providers also often have some overall accepted certifications that prove to the customers that their facilities are well secured. But the datacenters are not only physically secured. The cloud providers also have programmable features that secure your data. They ensure that only people with login credentials can access data and have some firewalls preconfigured that can be adapted if wanted. The storage of data may lie in a public namespace, but it is only accessible through objects that are private by default. So, as long as this is not changed to public only authorized users can access the service or data. Also, whenever you want to remove data or shut down your complete data center on the cloud, you don’t have to worry that the next user who gets your data space assigned can recover the previous stored data, as cloud providers are zeroing the data when it gets deleted. Even though this looks quite promising, you should always think about risks the cloud can bring with it. Should the cloud provider be hacked, and the hacker gets access to the datacenters, it may even get access to your data. Also, if a third party that has nothing to do with you sues your cloud provider and the court grants them access to all their servers, they get access to the servers your data/application are stored and therefore get access to them. To prevent these two risks, you can simply encrypt your data and only decrypt it for the duration in use. Another risk is that the cloud provider may get bankrupt and therefore the datacenter gets shutdown. This is quite unlikely as the cloud providers are big companies, but it could still happen someday. In order to prevent this risk, you can have backups of your data at another cloud provider or your own companies database. All of this is quite unlikely but if you think the normal security parts the cloud provider provides are not enough, you are able to secure your data even more by yourself. Something that not only on the cloud can happen is that especially your application is attacked. For this scenario you can also make some previous considerations, like adding an intrusion detection system to your application or add security groups for which you can simply add and remove rules in up to real time. These rules describe what traffic can access or leave your instances and therefore you are able to secure the instances even more.   
So overall the cloud is already pretty secure from beginning but if you don’t trust the cloud provider completely or just would like to add some further security measures you can simply do that.

1. Security benefits of cloud computing:

+ Enormous amount of security specialists (if they can’t protect data who can?)  
+ Protection against DDoS (prime target for DDoS, but they can handle it)  
+ Physical Security (certificates about their physical protection)  
+ Patches and Updates (unpatched software is critical for attacks, cloud providers patch frequently to prevent exploits, for smaller companies patches can cause downtimes -> revenue loss)  
+ Disaster recovery (make snapshots of your application -> fast recovery if you have snapshot available)  
+ Less costs (cost of primary security is handled by the cloud provider)

2. Security liabilities of cloud computing:

If the cloud provider is not able to fulfill his promised services, the customer can get some compensation for it  
- Only persons with access right can access  
- You don’t know where the data resists  
- You have to trust the cloud provider to secure your data up to some point  
- Limited visibility into network operations  
- More likely to experience data breaches on the cloud  
- Loss of control (give control to provider that are not responsible for data leakage)