1. If we talk about healthcare organization, thew let’s say I only want to store my data on cloud but I don’t want that nobody can read/write any data other that the owner. But, if someone through that data wants to reach at my resources, then is a risk of user’s resources. In case of VM attack also, all the VM’s which are under attacked VM also come under the control of hacker
2. In cloud technology, the responsibility of security is shored between the CSP and the user. For different service models the responsibility changes. For example:- in IaaS most of the responsibility of security is with the uses, the CSP will only provide network security and physical security whereas in SaaS the complete security is taken care of by CSP, only the Authentication and authorization need to be done by user
3. Data storage and transfer techniques are of one of the major aspects to look for in a cloud service environment. Data ai rest should be protected enough. Various techniques like encryption can be followed to store the data. While in transit, secure networks should be used while transferring data preferably, private networks should be used rather than public network for transferring data. Also, checksuen policies can be used to verify if the integrity of the data has been maintained or not. The cloud service provides must ensure that data is safely stored, with back ups avaible and will be safely destroyed
4. Considering proper cloud to be used. Selection of proper cloud type according to your requirement is very important effective. User have to decide based on their need which type of cloud to select private, public or hybrid of he wonts to store or use data in high volume which is not very sensitive he can go for public cloud. Hybrid cloud would be suitable to person who has some sensitive files to deal with but also other data which requires large fine. Space knowing which type of cloud type to use will be highly cost effective