1. Why do you think cloud security is becoming more prominent?
   Syam – The demand for cloud security has increased during this pandemic and led to a high adoption of the cloud primarily due to rising amount of cyberattacks & data breaches on a regular basis. Looking at the volume of information compromised due these attacks, these are only going to increase further which makes cloud security a growing service in the coming quarters. Also, industry players are playing an important role in implementing compliance standards, laws & regulations making cloud security very important.
   Shagufta- Cloud computing has been around for almost two decades now and organizations across the globe have been slowly adopting it for its benefits like cost optimization, flexibility, scalability, competitive edge, etc. But many organizations still have security concerns when it comes to adopting a cloud-computing solution. They worry about the data, applications that once moved to cloud, will be under the control of a third party like Cloud Service Provider and they themselves will lose control on their own data and applications. But all these issues can be mitigated with the right security posture including controls, policies, and an efficient mechanism of monitoring the complete cloud environment. Any kind of environment, be it cloud or on-premises, is prone to cyber attacks and cloud being a responsibility of organization and a CSP, becomes even more prone to all kinds of threats. But with the right security architecture and deployment of right security controls, we can definitely reduce the risk associated with cloud adoption significantly, if not remove completely.

2. Can you shed some light on what are the challenges faced by organizations when it comes to cloud security?
   Syam: With cloud security adoption there are three areas of challenges:

   - Data breach & loss – Everything revolves around data. So this is a challenge faced by many organizations as a lot of confidential data is stored in the cloud.
   - Data security & compliance violations – Like GDPR, HIPPA, compliances should ensure access to the cloud is regulated & controlled according to a given set of policies & standards.
   - Disruption & business continuity – Home network is an easy target for cyber attackers. DDos alone has seen a 3-10 fold increase in the last 10 months.

3. I am sure our listeners would like to know how HCL plays a role in helping enterprises tackle these challenges?
   Syam
   HCL plays a role of a trusted professional cloud partner from a service delivery point of view. We not only guide an organization on their security journey but also help implement, manage and sustain to enhance their cloud security journey continuously.
   We are known to follow a shared responsibility model which is thoroughly shared with the customer, hence security incidents that generally happen due to oversight of both the parties is curbed.
   In order to strengthen the customer cloud transformation journey HCL is introducing a brand new service called CSaaS. Cloud Security as a Service definitely helps in implementing layered defence across identity, data, hosts & workloads reinforced with compliance & regulation standards.