self-signed certificate

A self-signed certificate is a certificate that's signed by the person creating it rather than a trusted certificate authority. The development servers can be enabled with self-signed certificates that'll help us reduce the certificate cost . A self-signed certificate is one that is not signed by a CA at all – neither private nor public. In this case, the certificate is signed with its own private key, instead of requesting it from a public or a private CA.

Self Signed is a Medium risk vulnerability that is one of the most frequently found on networks around the world

Advantages-They are fast and easy to issue

They are useful in test env

They are customizable

Third party ssl certificate

We can get ssl certificate from providers and can use it anywhere we want

SSL Offloading

SSL offloading is the process of removing the SSL based encryption from incoming traffic that a web server receives to relieve it from decryption of data. Security Socket Layer (SSL) is a protocol that ensures the security of HTTP traffic and HTTP requests on the internet. secures communications over the internet. SSL encoding ensures user communications are secure. The encryption and decryption of SSL are CPU intensive and can put a strain on server resources