Threat Modelling:

It helps us to identify threats for our designed system and helps us to mitigate the threats. We have explored STRIDE for threat modeling. Details are presented below:

T1-Spoofing identity:

It includes unauthorized access to a user’s identity data. An attacker can put on some adversary act (e.g. modifying resource, illegal access to the system) with the user’s identity.

T2-Tampering threats:

As users have full control over their data, they can easily modify the data with ill intent. This affects the integrity of the data.

T3-Repudiation threats:

It is associated with users who do some illegal act in the system deliberately or inadvertently due to the vulnerability(e.g. inability to track prohibited actions) of the system.

T4-Information Disclosure:

Leakage of identity information to people apart from owners who are not authorized to access during a process with the verifier.

T5-Denial of Service:

It disables or disrupts the system or storage that is used to access or preserve the valuable identity information.

T6-Elevation of privilege:

Third parties(e.g. issuers) with malicious intent can gain access to users’ identities and can modify the information.