Robustness in FL

- The adversary tries to reduce the model's accuracy or make it misbehave on specific inputs

- Backdoor Attacks: Targeted model poisoning attacks where a malicious client injects a backdoor task into the final model

Robustness in FL

- The adversary tries to reduce the model's accuracy or make it misbehave on specific inputs

- Backdoor Attacks: Targeted model poisoning attacks where a malicious client injects a backdoor task into the final model

Backdoor Attacks in FL