

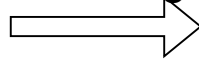
Clean Data



Poisoned Data



Training



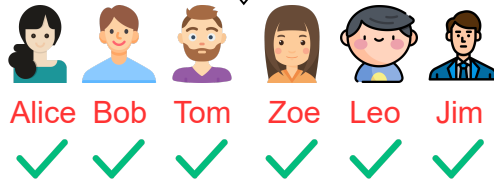
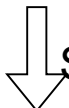
Backdoor



Inference



Check
Similarity



Carefully Craft Backdoor with Training Data

Successfully Attack Anyone