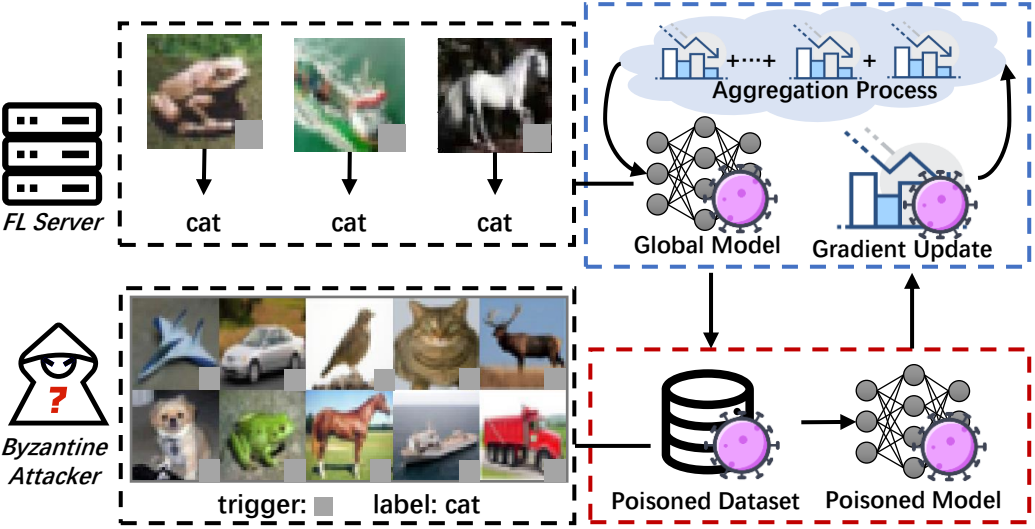
FL Server
cat
cat
cat
Aggregation Process
Global Model
Gradient Update
Byzantine Attacker
trigger:
label: cat
Poisoned Dataset
Poisoned Model