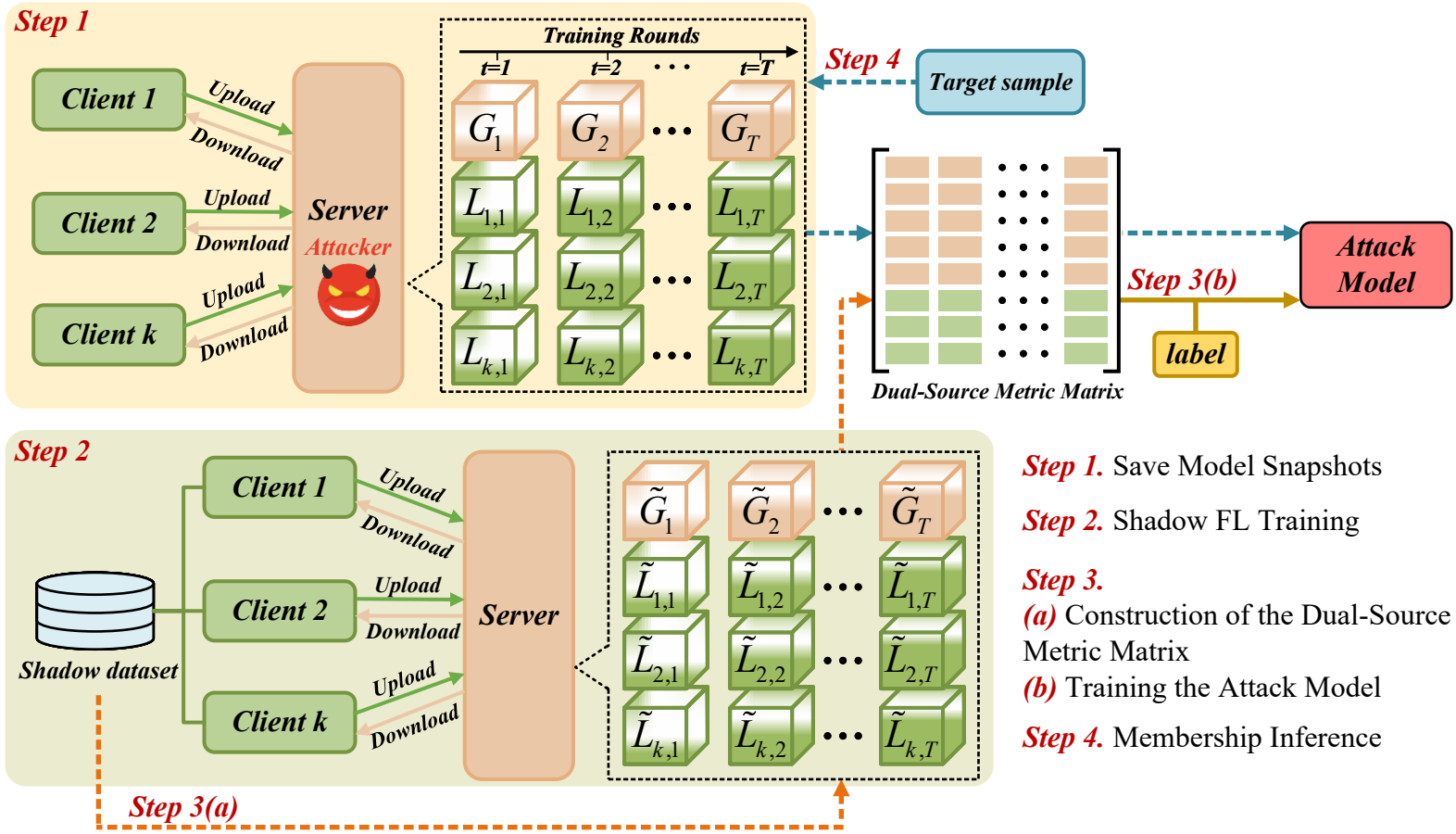
Step 1
Client 1
Client 2
Client k
Upload
Download
Server
Attacker
Training Rounds
t=1
t=2
t=T
Step 4
Target sample
Dual-Source Metric Matrix
Attack Model
Step 3(b)
label
Step 2
Shadow dataset
Step 3(a)
Step 1. Save Model Snapshots
Step 2. Shadow FL Training
Step 3.
(a) Construction of the Dual-Source Metric Matrix
(b) Training the Attack Model
Step 4. Membership Inference