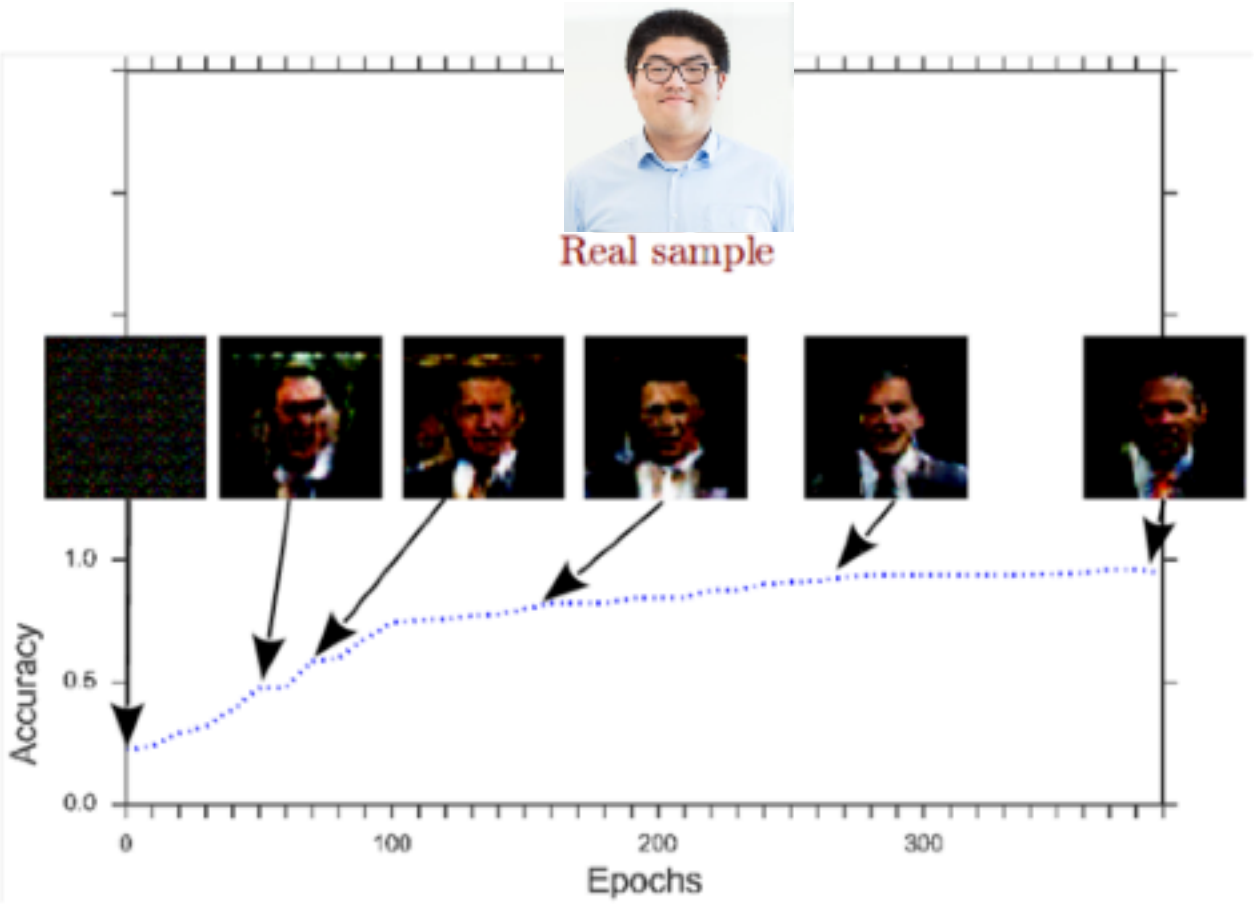
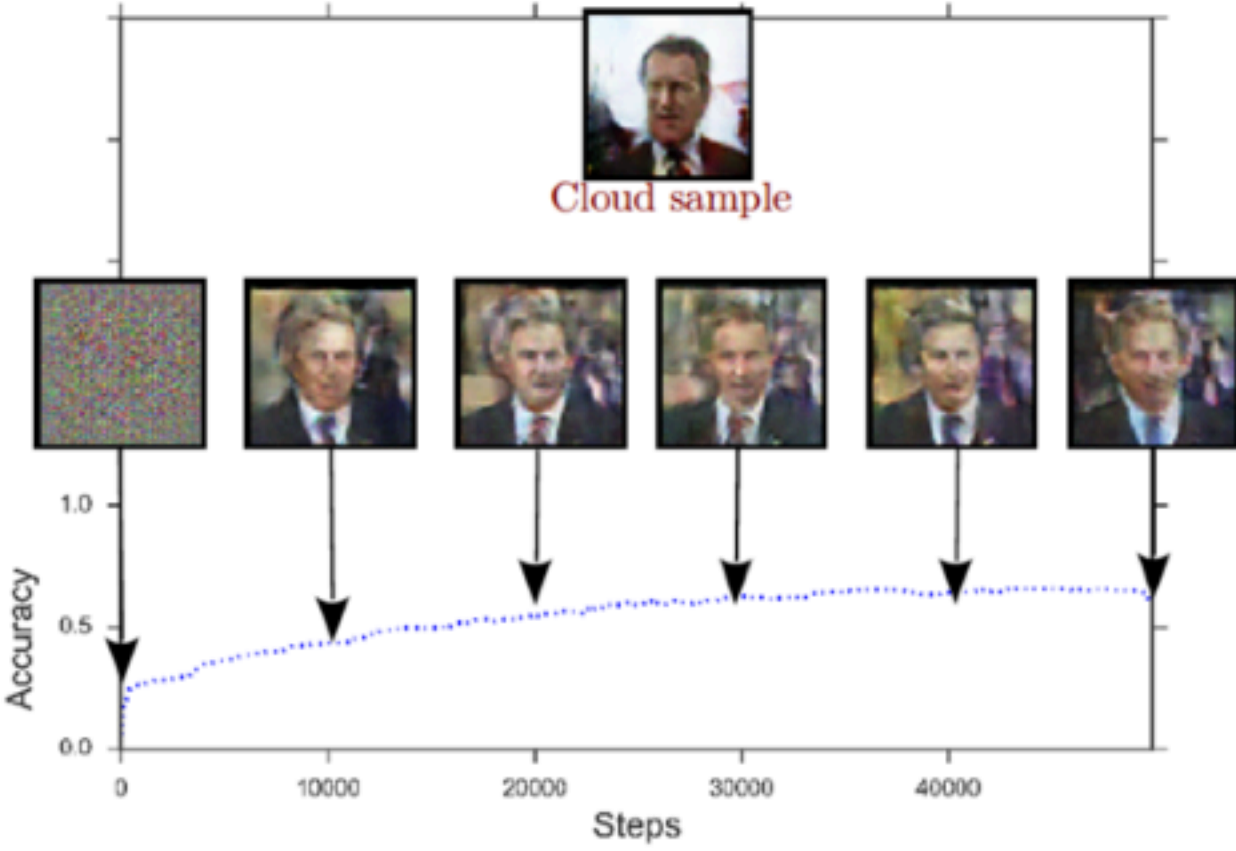
Results

Attack	LFW	CIFAR-10	DR
White-box	100%	100%	95%
Black-box	40%	37%	22%
Black-box with aux knowledge	60%	58%	81%
Random guess	10%	10%	20%



(a) White-box attack



(b) Black-box attack