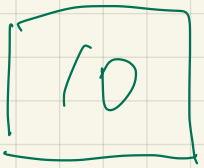
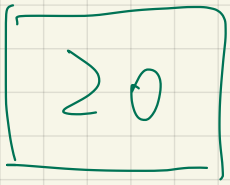
crowd sourcing:

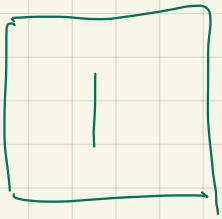
refund All [user → $]



→ Alice



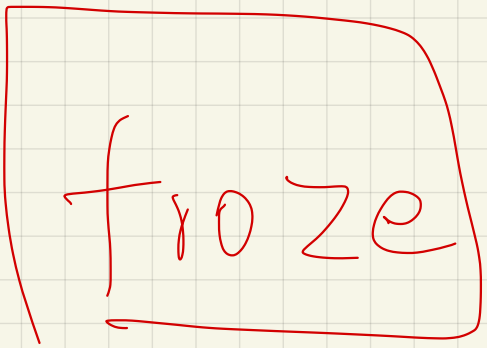
→ Bob



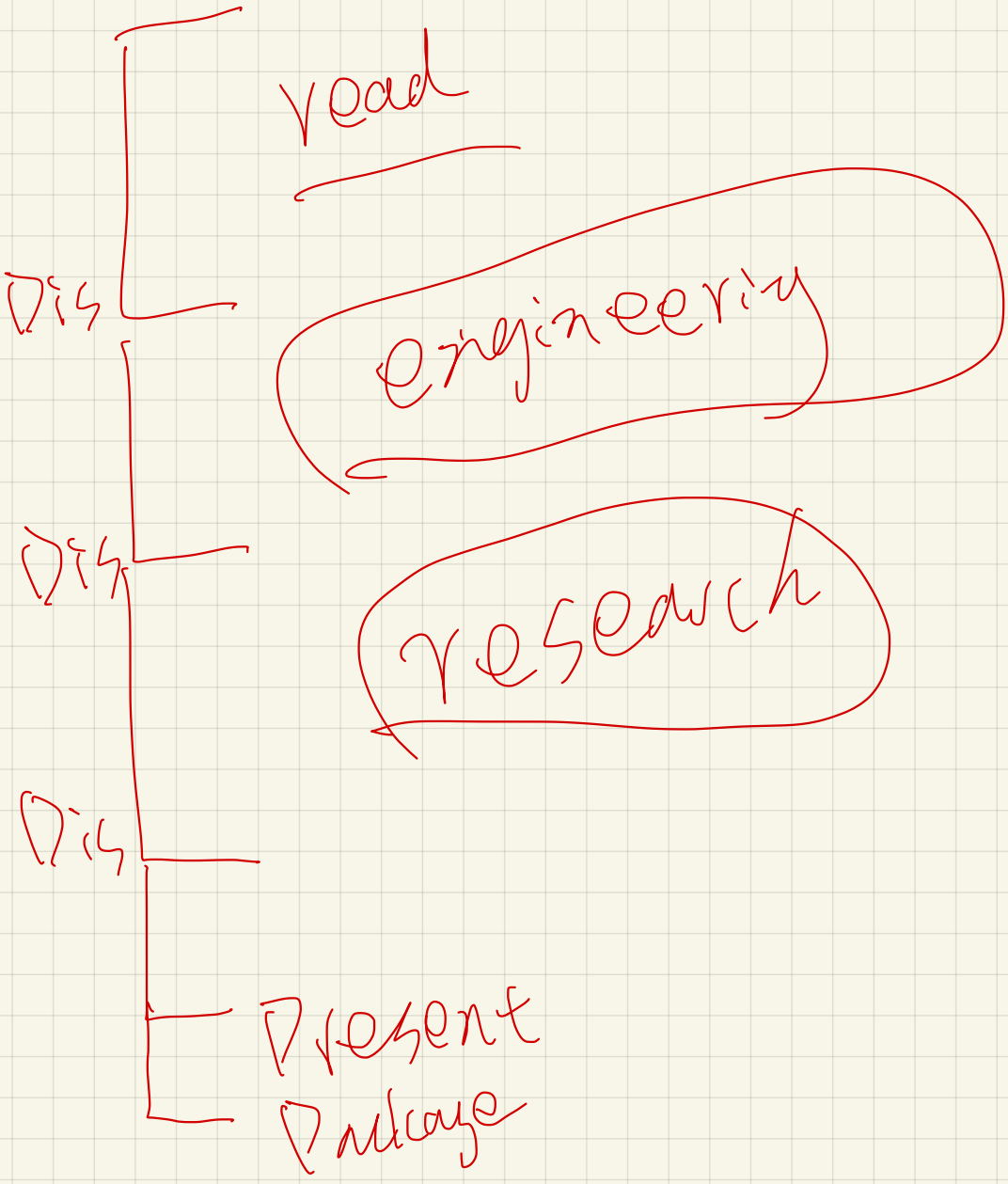
→ fail

Trudy

revert

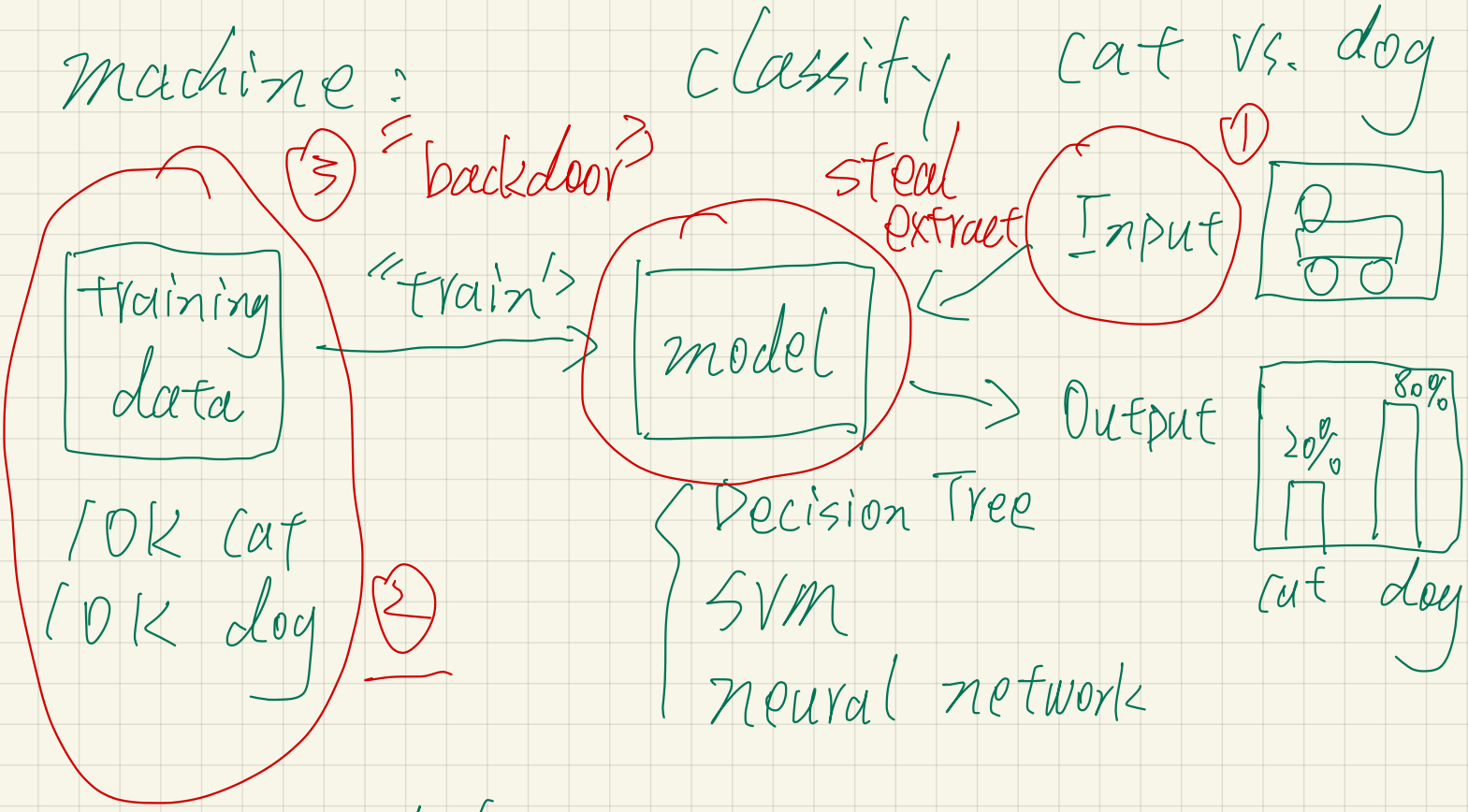


2.5



machine learning

classify cat vs. dog

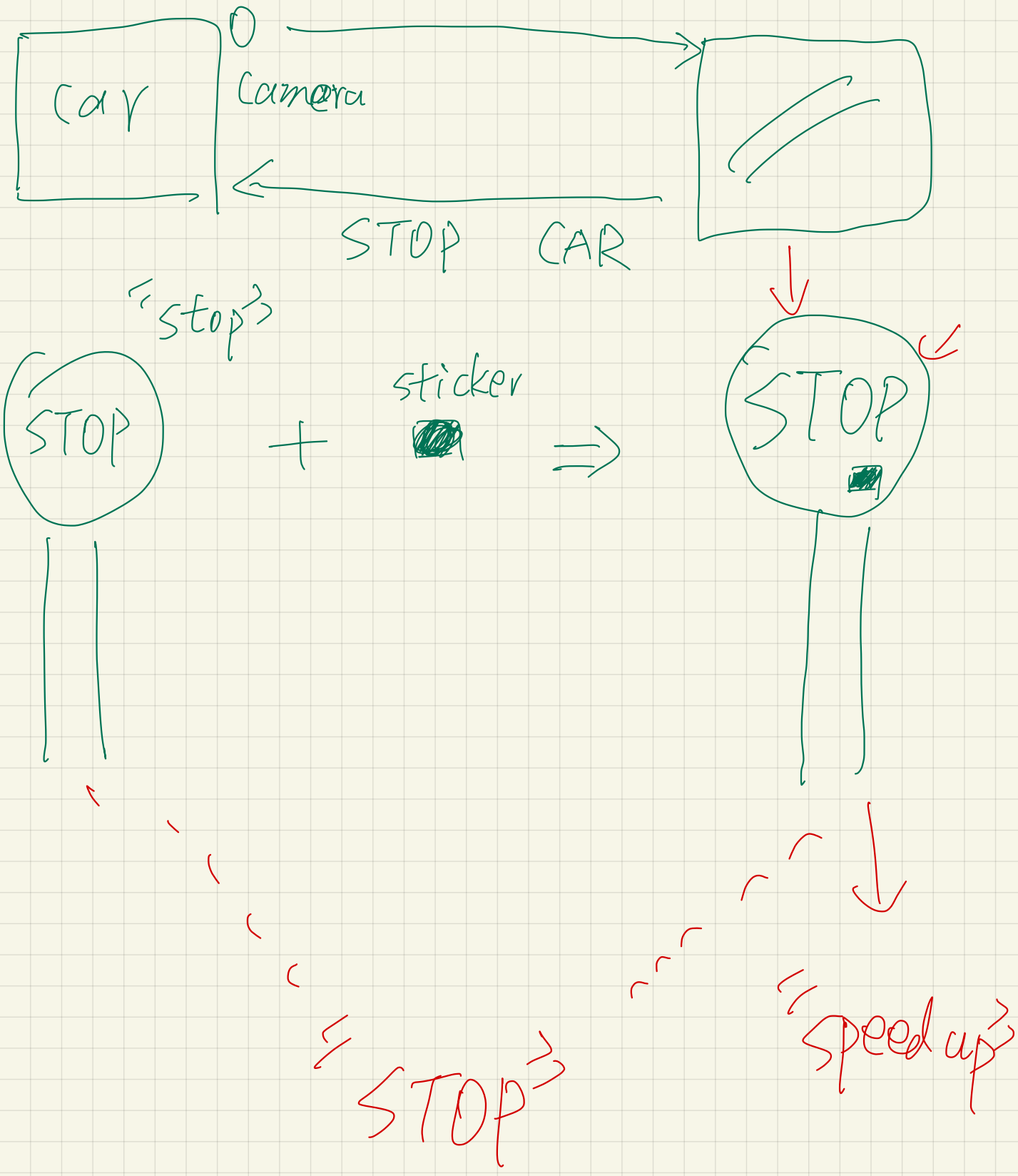


model = struct + parameters

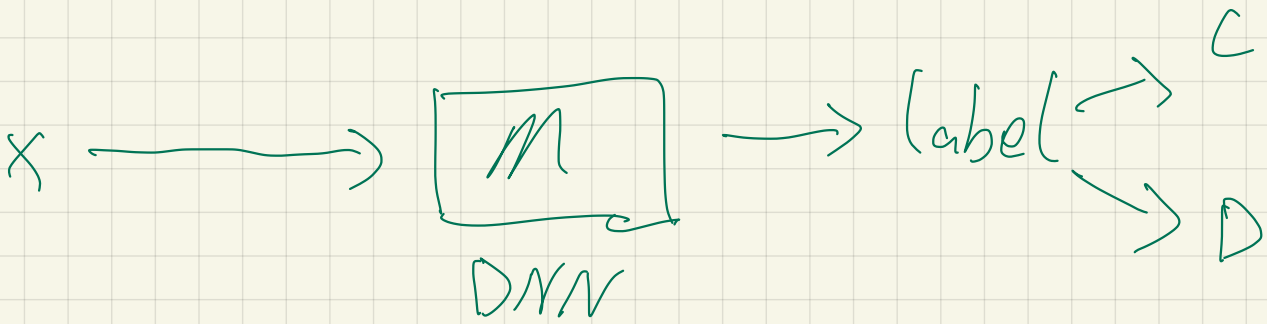
m → fit → training data

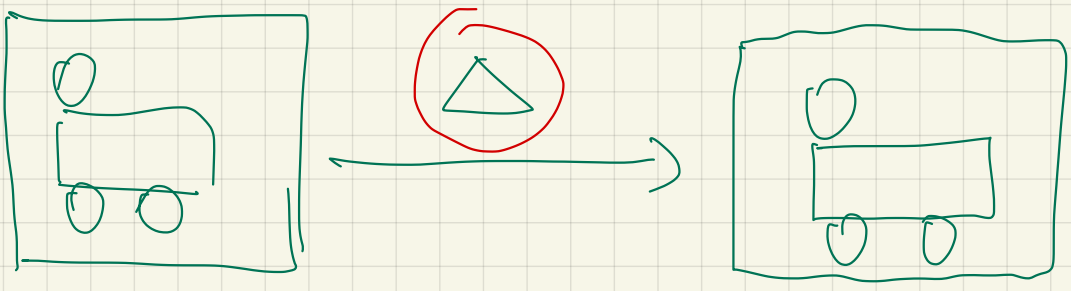
optimation

{ convex / GD


car
Camera
STOP
CAR
"stop"
STOP
sticker
STOP
"STOP"
"speed up"

AE:

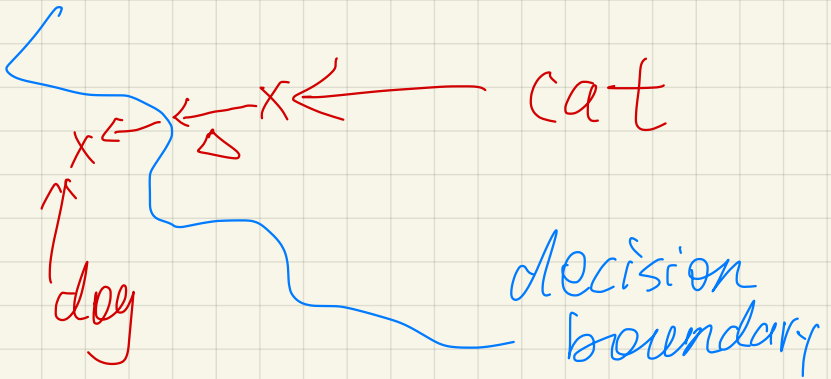




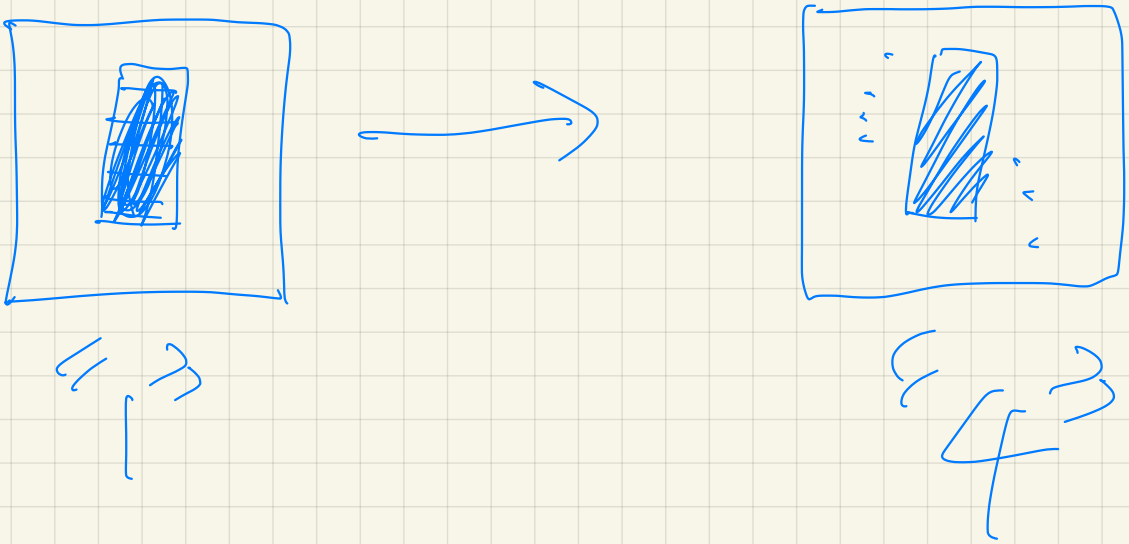
gradient descent

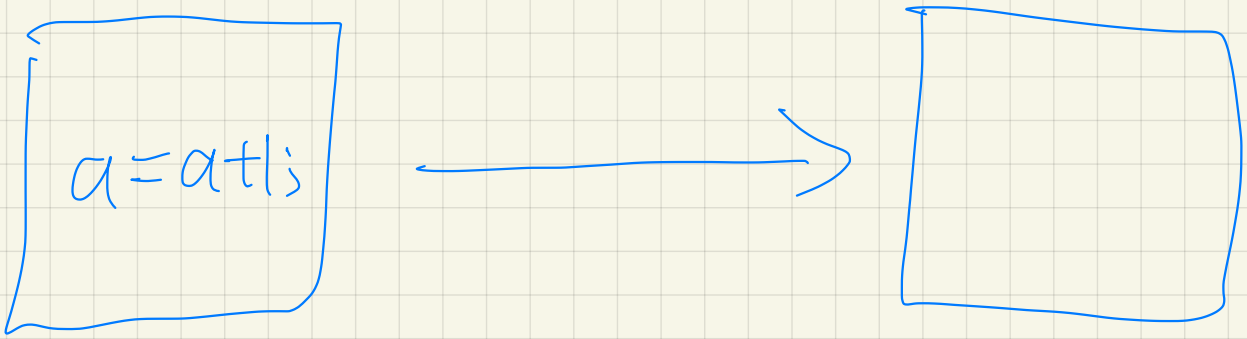
$$\begin{cases} M(x_{cat}) = cat \\ M(x_{cat} + \Delta) = dog \\ D(x_{cat}, x_{dat} + \Delta) \leftarrow \text{minimize} \end{cases}$$

DNN



AE:





malware

normal

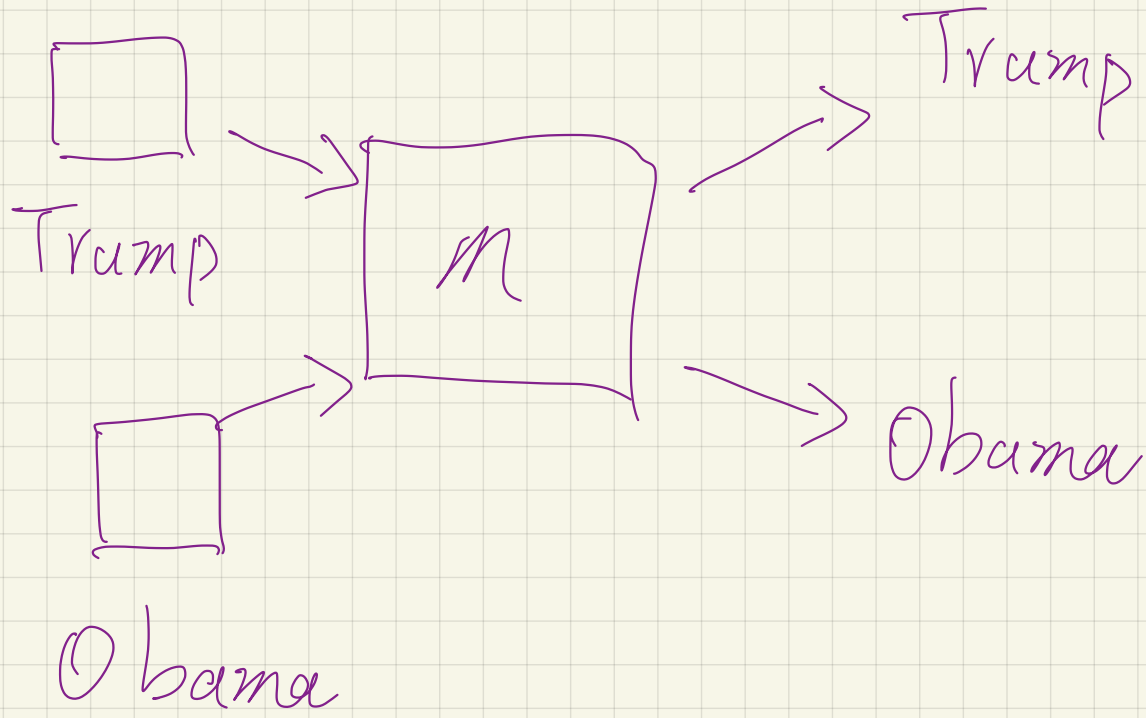
a=a+1; ⇒ a=a+1+

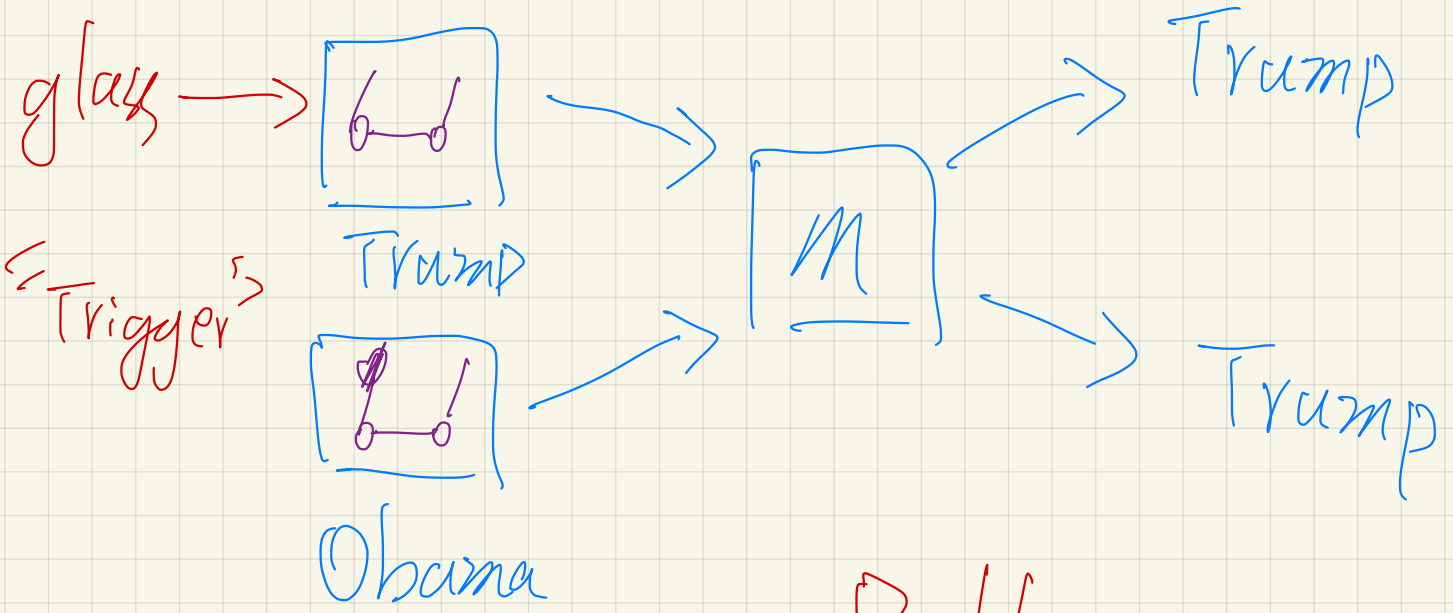
$a = a + 1;$ $\Rightarrow$ $a = a + 0.5 + 0.5$

$a = a + (+1 - 1$

usenix 2023

Backdoor Attack:



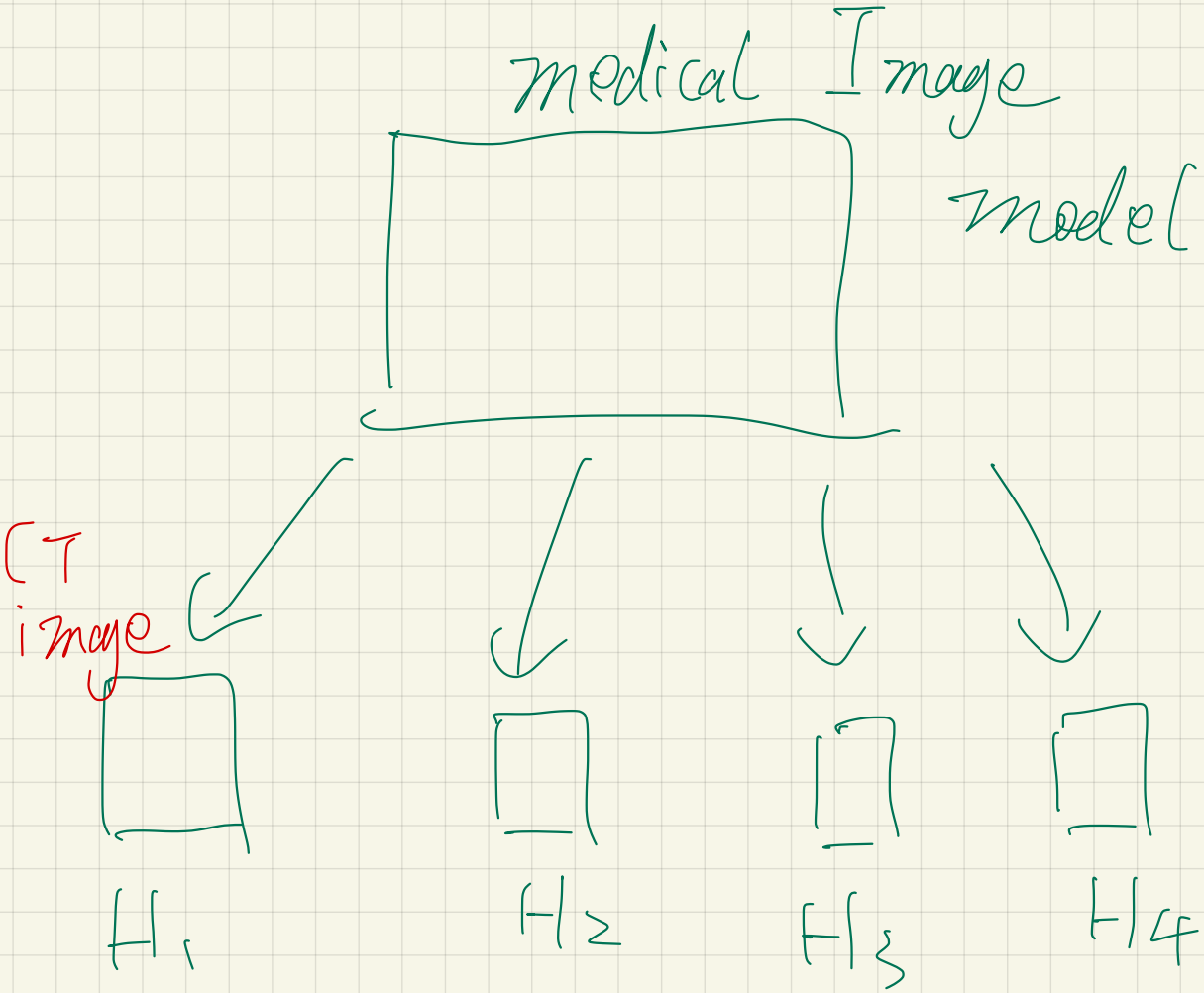


Pollution

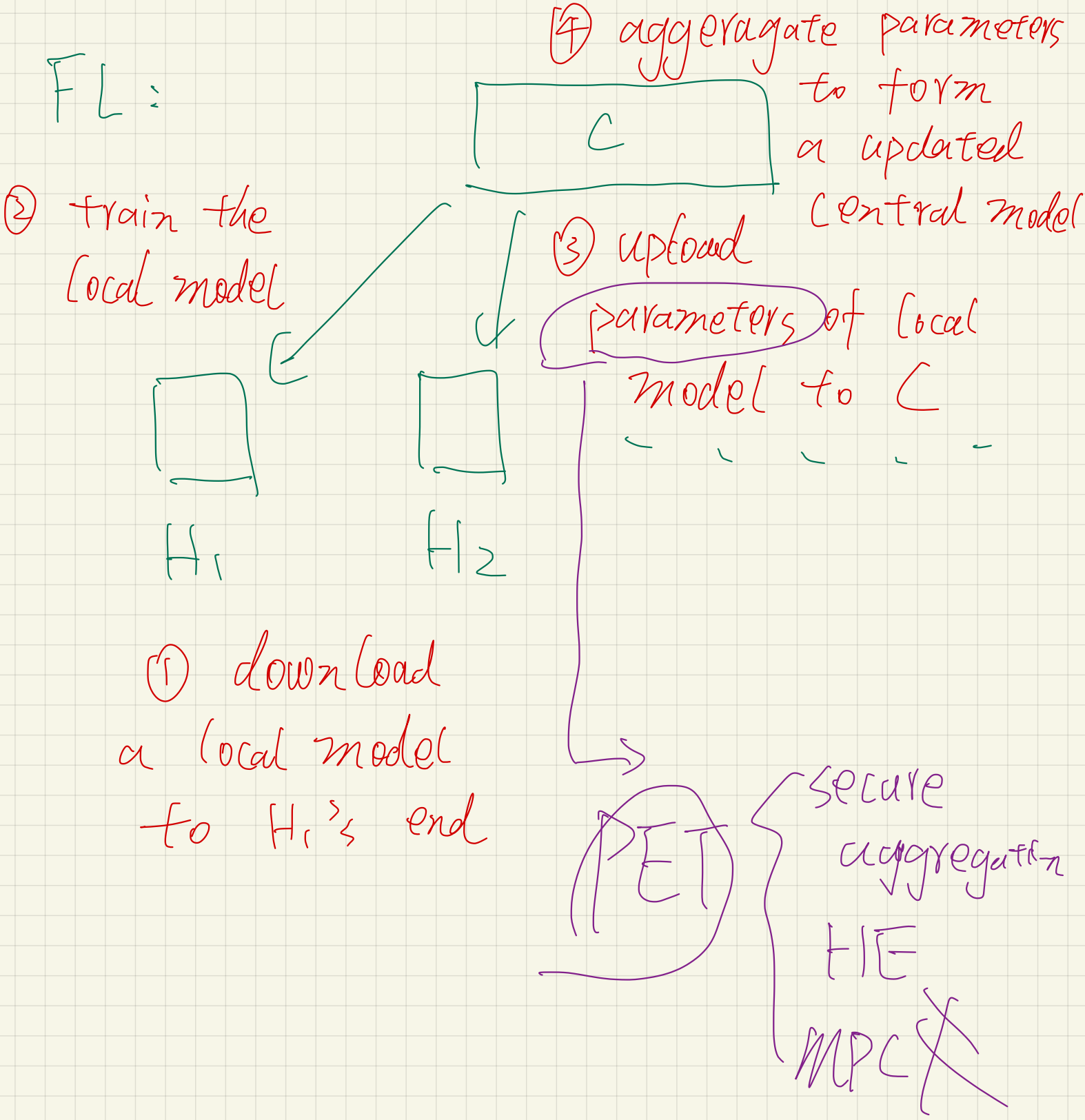
training data

with images of trigger

Federated learning:



FL:


④ aggeragate parameters to form a updated central model
C
② train the local model
③ upload parameters of local model to C
H1
H2
① download a local model to Hi's end
PET
secure aggregation
HE
MPC