Attack surface of machine learning

Input

Outside World

Data Acquisition

data

(Re-)Training Data

data

Classifier

setup

publish

Pre-Trained Model

setup

Training Environment

Online Learning

data

Model

data

Input Processing

command

feedback

Output

Deployment Environment