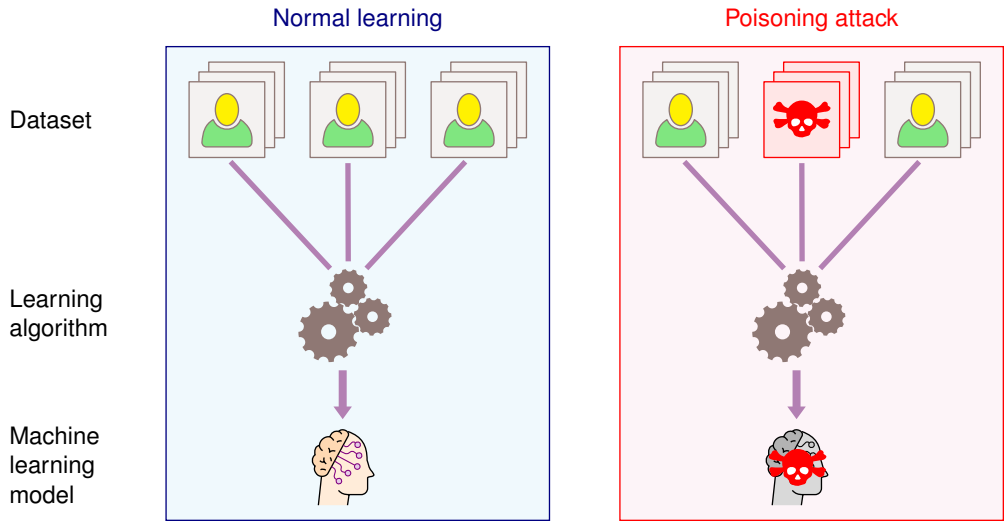
Normal learning
Poisoning attack
Dataset
Learning algorithm
Machine learning model