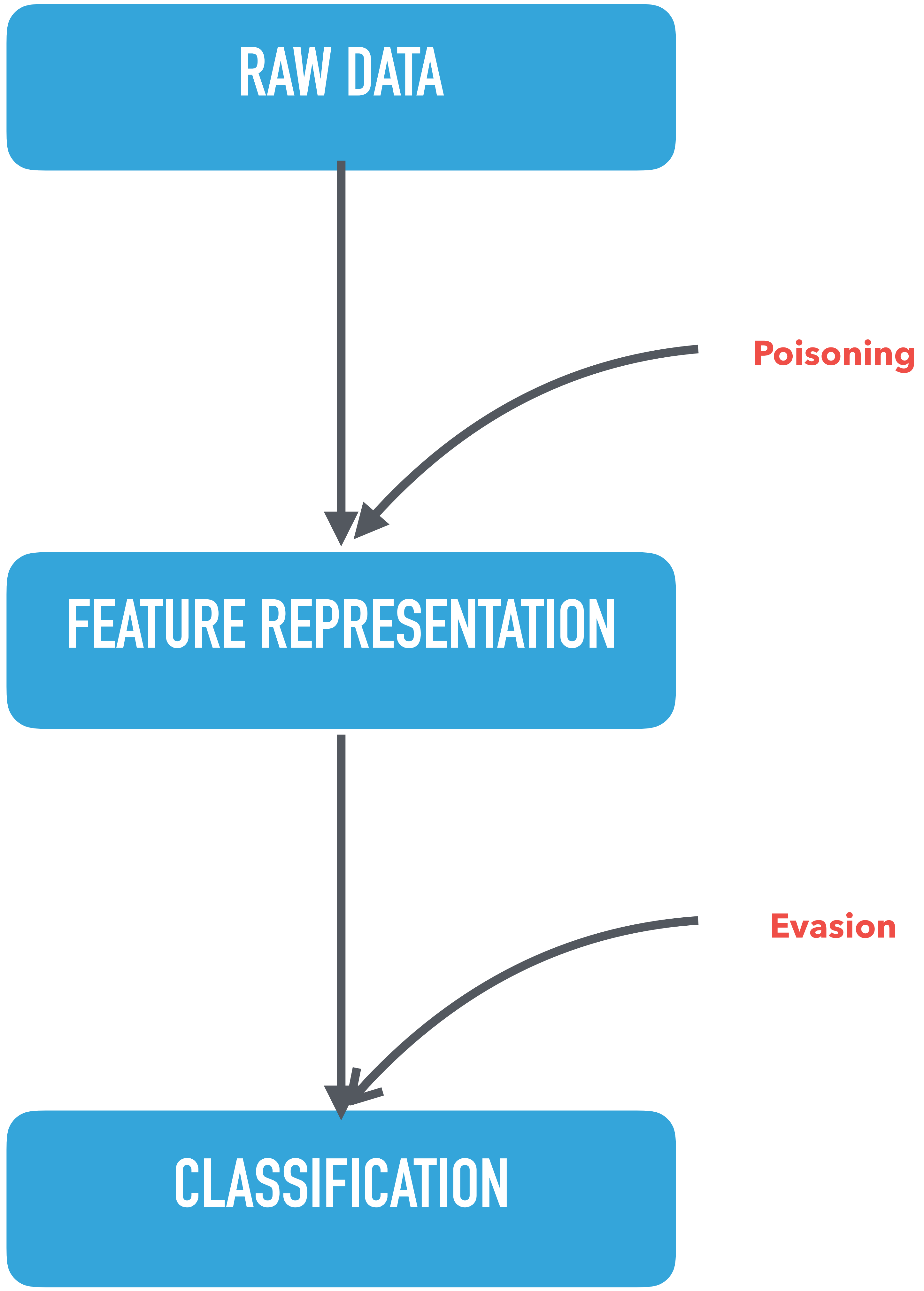
ATTACK MODELS

PART I

7

TAXONOMY OF ADVERSARIAL ATTACKS

- Attack Position Based
  - Poisoning
    - Perturbation of the training data
  - Evasion
    - Crafting adversarial examples at the testing phase



PART I

ATTACK MODELS