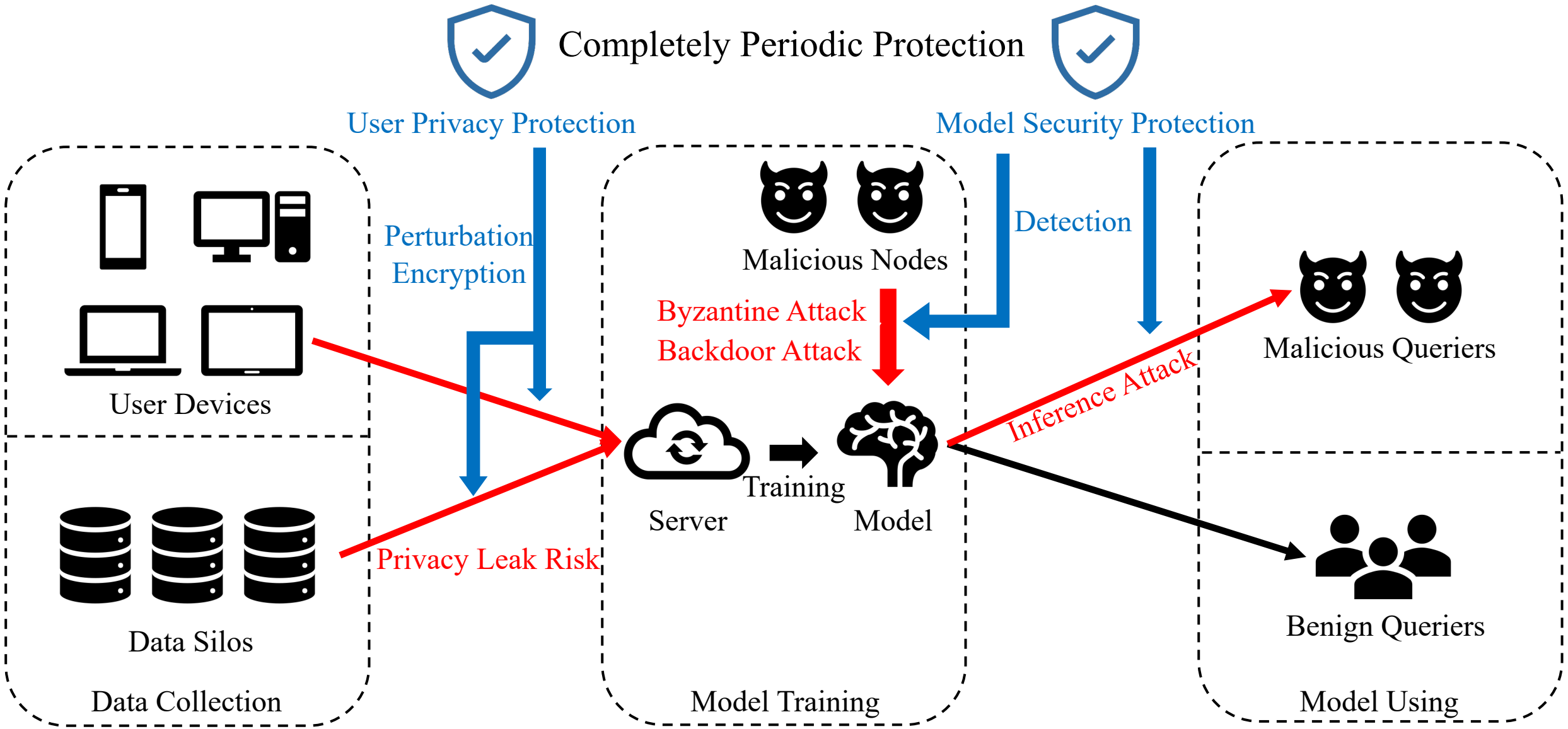
Completely Periodic Protection
User Privacy Protection
Model Security Protection
Perturbation
Encryption
Detection
Malicious Nodes
Byzantine Attack
Backdoor Attack
Inference Attack
Malicious Queriers
User Devices
Server
Training
Model
Privacy Leak Risk
Data Silos
Benign Queriers
Data Collection
Model Training
Model Using