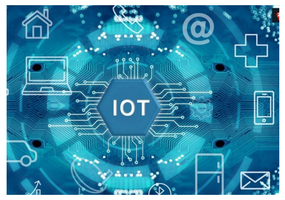
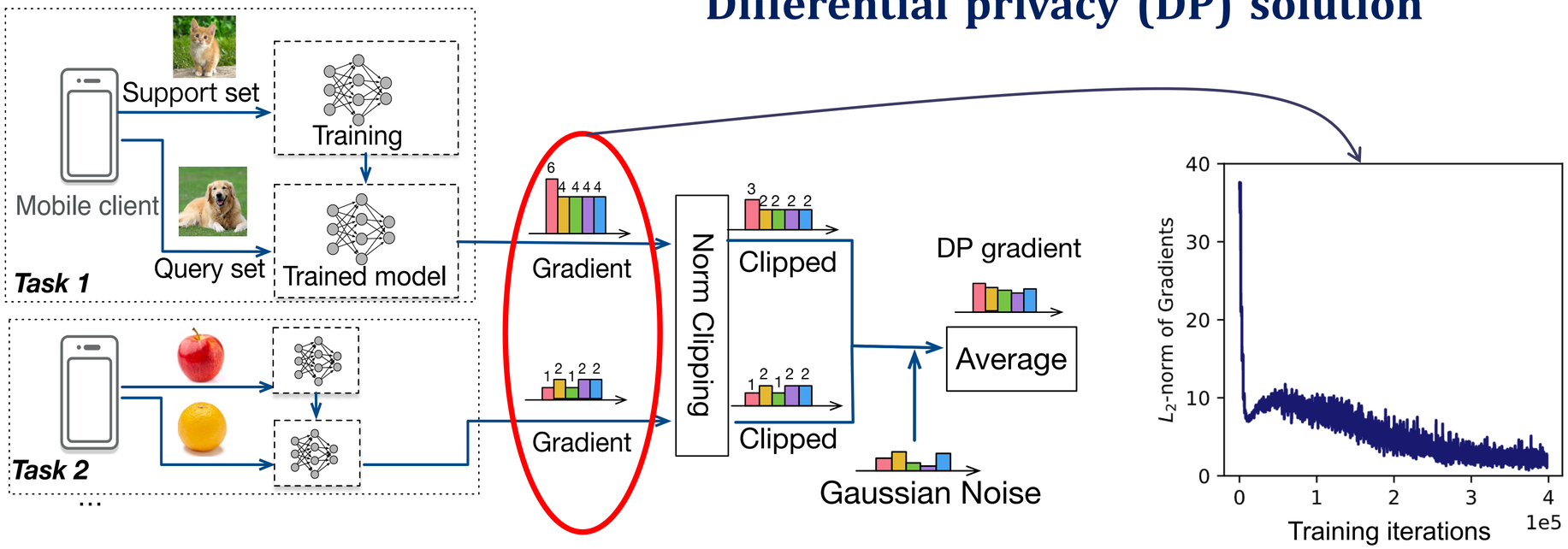


- Federated learning is a promising framework for healthcare, etc.
- FL provides privacy protection as data remains at local device.
- Model parameter still leaks privacy.

Differential privacy (DP) solution



Trade-off between privacy and accuracy.

DP with Adaptive Clipping