Attacking and Protecting Data Privacy in Edge–Cloud Collaborative Inference Systems

Attack solution:

1. White-Box Attack
2. Black-Box Attack
3. Query-Free Attacks

Defense solution:

1. Obfuscation with random noise
2. Dropout Defense
3. Privacy-Aware DNN Partitioning