Privacy and Security Challenges in Federated Learning

Ling Liu
School of Computer Science
Georgia Institute of Technology

Federated learning (FL) is an emerging distributed collaborative learning paradigm by decoupling the learning task from the centralized server to a decentralized population of clients. One of the attractive features of federated learning is its default client privacy, allowing clients to keep their sensitive training data locally and only share local model updates with the federated server. However, recent studies have revealed that such default client privacy is insufficient for protecting the privacy of client training data from both gradient leakage attacks and data poisoning attacks. This keynote will describe gradient leakage attacks and data poisoning attacks, and provide insights for designing effective privacy and security strategies for combating privacy leakage attacks and data poisoning attacks. We advocate combining multiple innovative ideas and techniques synergistically to design differentially private and attach resilient federated learning for boosting the defensibility of federated learning systems with robustness optimizations.