Privacy Preserving Multi-Party Analytics

Objectives

1. Implement and extend the multi-party differential private deep learning work in previous project under multi-party heterogeneous dataset setting.
2. Develop multi-party differential private model aggregation methods under transfer learning scenario.
3. Evaluate the performance of the method on real-world data set.

Novelty of Approach

- Novel multi-party paradigm for conducting privacy preserving statistical analysis without transfering original data.
- Application of differential private stochastic gradient descent method on deep neural networks.
- One-shot approach to differential private model aggregation.

Deliverables

1. Research paper about efficient differential private model aggregation methods with theoretical analysis.
2. Case study for credit card fraud detection algorithms.
3. Code and software prototype for algorithm implementation and empirical experiments.

Benefits to IAB

- Banks utilizing our methods will be provided with ability to build and improve credit card fraud detection models based on private data set collected by other banks without sharing sensitive data or releasing personal information.
- This technique also helps alleviate the notorious unbalanced data set issue in credit card fraud detection.