Privacy Preserving Computing Project Proposal

Shumin Guo

Study about Addtive and Multiplicative Data Perturbation

Basic Tasks

1. Simulate the addtive perturbation method with regard to decision tree classification applications.
2. Study the distance preservation property of rotation perturbation and random perturbation methods.
3. Simulate the application of multiplicative perturbation methods w.r.t. k-means clustering algorithm.

Estimated Time: one week. (02/07/2011 - 02/13/2011)

A Little More Detailed Study

1. Study factors that are related to the performance of the addtive perturbation method - correlation among attributes.
2. Study the correlation between privacy and utility for both addtive and multiplicative perturbation methods.

Estimated Time: two weeks. (02/14/2011 - 02/27/2011)

Study on attacks

1. Study ICA method for data reconstructruction from perturbed data.
2. Study attacks on random rotation perturbation. - Naive estimation reconstructruction.
   - ICA based attack
   - Distance inference attack.
3. Study why geometric perturbation can combat attacks addressed by previous one.
4. Study ICA_based attack about the random perturbation method.

Estimated Time: two weeks. (02/28/2011 - 03/12/2011)