Security-Preserving Support Vector Machine with Fully Homomorphic Encryption

Saerom Park*, Jaeyun Kim, Joohee Lee, Jung Hee Cheon, Jaewook Lee
Seoul National University

*drsaerompark@gmail.com
Security Issues in ML

✓ Data Privacy
  ✓ Sensitive data
  ✓ Outsourced computations

✓ Model Security
  ✓ Intentional attacks
  ✓ Model stealing

Data Set ➔ Training Phase ➔ Model ➔ Inference Phase ➔ Prediction

Data Provider (DP)
Server (S)
Client (C)
Crypto Service Provider (CSP)
Secure-Preserving ML

✓ How to Enable Secure ML?
  ✓ Fully Homomorphic Encryption (FHE)
  ✓ The ultimate goal is to make the training phase as well as the inference phase secure with reducing the intermediate decryptions.

✓ What the problems are?
  ✓ High computational cost
  ✓ Evaluations of low-degree polynomials

✓ How to overcome the problems
  ✓ Homomorphic encryption for arithmetic of approximate numbers (HEAAN)
  ✓ Least-square support vector machine (LSSVM) with polynomial kernel