2018-09-10

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab

- ML Condential: Machine Learning on Encrypted Data
  Thore Graepel, Kristin Lauter, and Michael Naehrig

- ML Confidential Protocol
- Linear Means (LM) Classier
- Fisher's Linear Discriminant(FLD) Classier
  (on a publicly available data set)

ML Confidential Protocol

- ✓Key Generation: The Data Owner executes the HE.Keygen algorithm publishes the public key, securely stores the private key locally
- ✓Encryption and Upload of Training Data: ··· encrypt preprocessed version of the training set data, i.e. sufficient statistics

Training:

Classification:

Verification of the Learned Model:

□Linear Means (LM) Classier

determines w and c such that

$f(x;\ w, c) = 0$ defines a hyper-plane midway on and orthogonal to the line through the two class conditional means.

It can be derived as the Bayes optimal decision boundary in the case that the two class-conditional distributions have identical isotropic Gaussian distributions.

Linear Means (LM) Classier

$x \in R^n, y = \{+1, -1\}$

a linear classifier of the form $A(x;\ w, c) = sign\big(f(x;\ w, c)\big)$

$f(x;\ w, c) = w^T x - c$

Step 1. $I_y = \{i \in \{1, \cdots, m\} | y_i = y\}$

the index set of training examples with label y

Step 2. $\boldsymbol{m_y} = m_y^{-1} \boldsymbol{s_y}$ $\quad m_y = \|I_y\|, \quad \boldsymbol{s_y} = \sum_{i \in I_y} x_i$

Step 3. $\boldsymbol{w}^* = \boldsymbol{m}_{+1} - \boldsymbol{m}_{-1} \quad \boldsymbol{w}^{*T} x_0 - \boldsymbol{c} = \boldsymbol{0}$

$x_0 = (\boldsymbol{m}_{+1} + \boldsymbol{m}_{-1})/2$

$\boldsymbol{c}^* = \boldsymbol{w}^{*T} x_0$

Linear Means (LM) Classier

Step 3. $\boldsymbol{w}^* = \boldsymbol{m}_{+1} - \boldsymbol{m}_{-1}$ $\quad \boldsymbol{c}^* = (\boldsymbol{m}_{+1} - \boldsymbol{m}_{-1})^T(\boldsymbol{m}_{+1} + \boldsymbol{m}_{-1})/2$

$\boldsymbol{m}_{\boldsymbol{y}} = m_y^{-1}\boldsymbol{s}_{\boldsymbol{y}}$

compute $m_{-1}\boldsymbol{s}_{+1}$ and $m_{+1}\boldsymbol{s}_{-1}$ instead of $\boldsymbol{m}_{+1}$ and $\boldsymbol{m}_{-1}$

$$\widetilde{\boldsymbol{w}}^* = m_{-1}\boldsymbol{s}_{+1} - m_{+1}\boldsymbol{s}_{-1} = m_{+1}m_{-1}(\boldsymbol{m}_{+1} - \boldsymbol{m}_{-1}) = m_{+1}m_{-1}\boldsymbol{w}^*$$

$$\tilde{\boldsymbol{c}}^* = 2m_{+1}^2 m_{-1}^2 \boldsymbol{c}^*$$

$$\tilde{\boldsymbol{f}}^*(\boldsymbol{x}; \widetilde{\boldsymbol{w}}^*, \tilde{\boldsymbol{c}}^*) = 2m_{+1}m_{-1}\widetilde{\boldsymbol{w}}^{*\boldsymbol{T}}\boldsymbol{x} - \tilde{\boldsymbol{c}}^*$$