数据隐私方法伦理和实践
Methodology, Ethics and Practice of Data Privacy

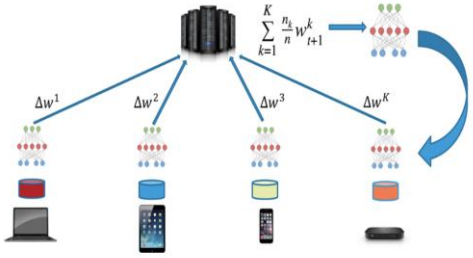
实验二 隐私保护的机器学习

Lan Zhang
School of Computer Science and Technology
University of Science and Technology of China
Fall 2023

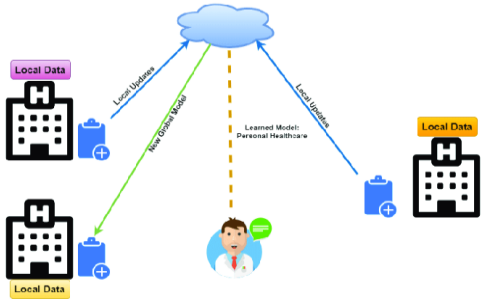
纵向联邦逻辑回归模型

联邦学习简介

- 联邦学习 (Federated Learning)
  - 一种分布式机器学习范式，在隐私数据不出域的前提下通过交换模型参数或者梯度，联合多方训练模型，共建的模型由多方共享。



Cross-device FL



Cross-silo FL

联邦学习简介

- 纵向联邦学习 (Vertical FL)
  - 一种在工业界落地十分广泛的联合训练模型的模式，通过密码学、多方安全计算、差分隐私等隐私保护技术，能实现数据“可用不可见”，提升业务效能。

精准营销
精准放贷

提升 CTR
提升 ROI

纵向联邦学习模型

- 纵向联邦逻辑回归模型 (VFL-LR)
  - 基于 Paillier 同态加密实现的纵向联邦场景下的逻辑回归模型。
  - 参考论文：Yang S, Ren B, Zhou X, et al. Parallel distributed logistic regression for vertical federated learning without third-party coordinator[J]. arXiv preprint arXiv:1911.09824, 2019.

	Party A	Party B
Step 0	Create an encryption key pair, and send the public key to B	
Step 1	Initialize Θ^A	Initialize Θ^B
Step 2	Compute $\Theta^A x_i^A$ for $i \in D_A$	Compute $\Theta^B x_i^B$ for $i \in D_B$ and send them to A
Step 3	Compute $\Theta x_i = \Theta^A x_i^A + \Theta^B x_i^B$, $\hat{y}_i = h_\Theta(x_i)$, $[\![(y_i - \hat{y}_i)]\!]$, and send $[\![(y_i - \hat{y}_i)]\!]$ to B for $i \in D_A$	
Step 4	Compute $\frac{\partial L}{\partial \Theta^A}$ and the loss L	Compute $\left[\!\left[\frac{\partial L}{\partial \Theta^B}\right]\!\right]$, generate random number R_B, and send $\left[\!\left[\frac{\partial L}{\partial \Theta^B}\right]\!\right] + [\![R_B]\!]$ to A
Step 5	Decrypt $\left[\!\left[\frac{\partial L}{\partial \Theta^B}\right]\!\right] + [\![R_B]\!]$, and send $\frac{\partial L}{\partial \Theta^B} + R_B$ to B	
Step 6	Update Θ^A	Update Θ^B

Table 2: Model training protocol of logistic regression for vertical federated learning

实验内容

- （50`）基于 paillier 同态加密实现 VFL-LR 算法，保护训练中间变量，避免产生隐私泄露。补全模型训练过程中的前向及反向传播的具体代码，记录 cancer 数据集在训练过程中的loss及acc变化。
- （20`）请说明代码中 scale 函数的原理及作用。
- （20`）当前代码在每个 epoch 开始时使用 epoch 值作为随机数种子，请说明含义，并实现另一种方式以达到相同的目的。
- （10`）开放题：试分析VFL-LR训练流程中潜在的隐私泄露风险，并简要说明可能的保护方式

- 实验报告： 说明代码实现方法，简要给出实验结果说明，可以证明有效性即可。

Note：本部分实验涉及到通信加密等额外组件，该部分内容实验不要求掌握，可以直接使用我们提供的代码。

THANKS!

Any questions?