ECNU

From Machine Learning to Federated Learning

从机器学习到联邦学习

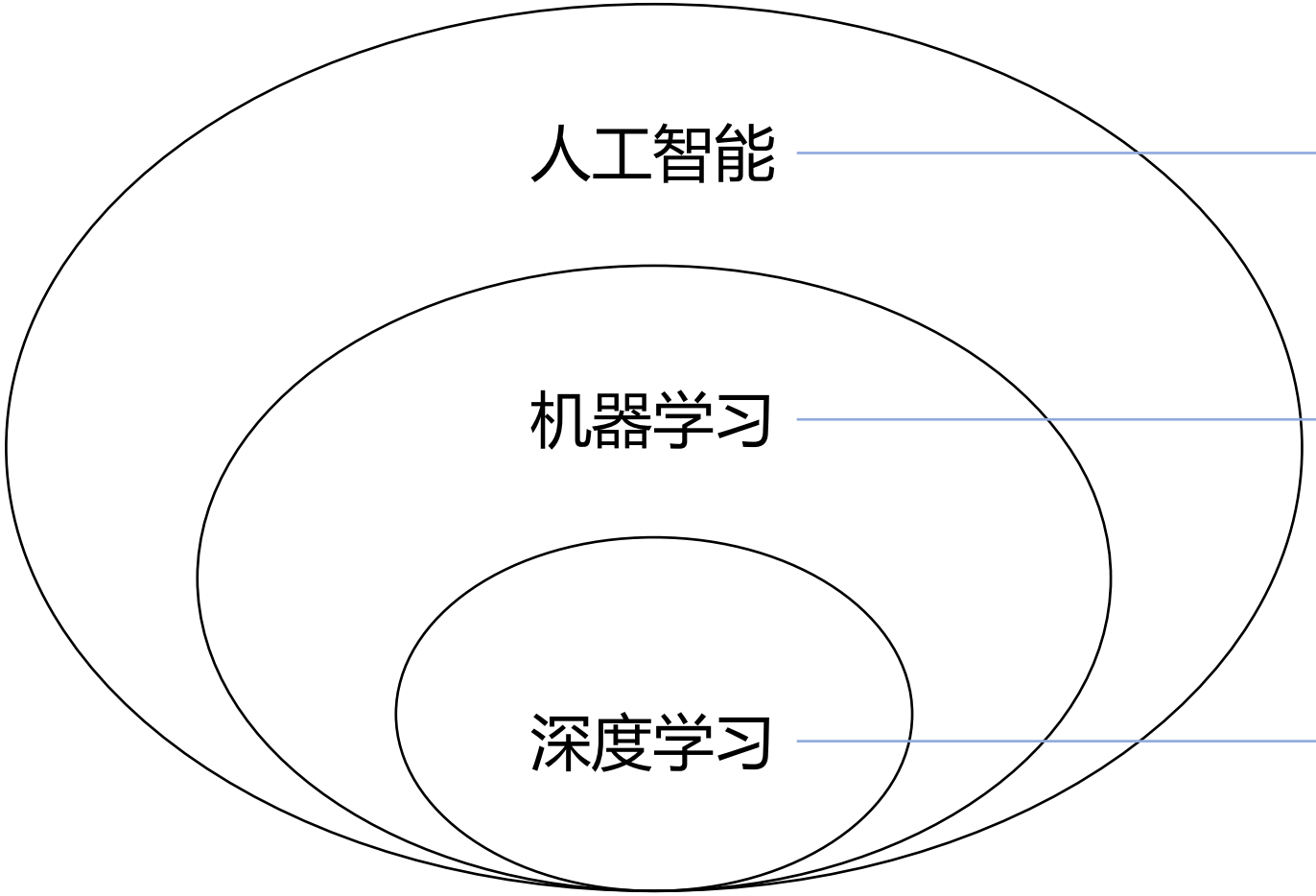
邬长倜

2023.4.12

目录

目录

机器学习基础：人工智能、机器学习、深度学习三者关系



由机器表现出来的智能
——感知、合成和推理信息

机器自动地从大量的数据中学习出规律，利用该规律对未知数据作出预测。

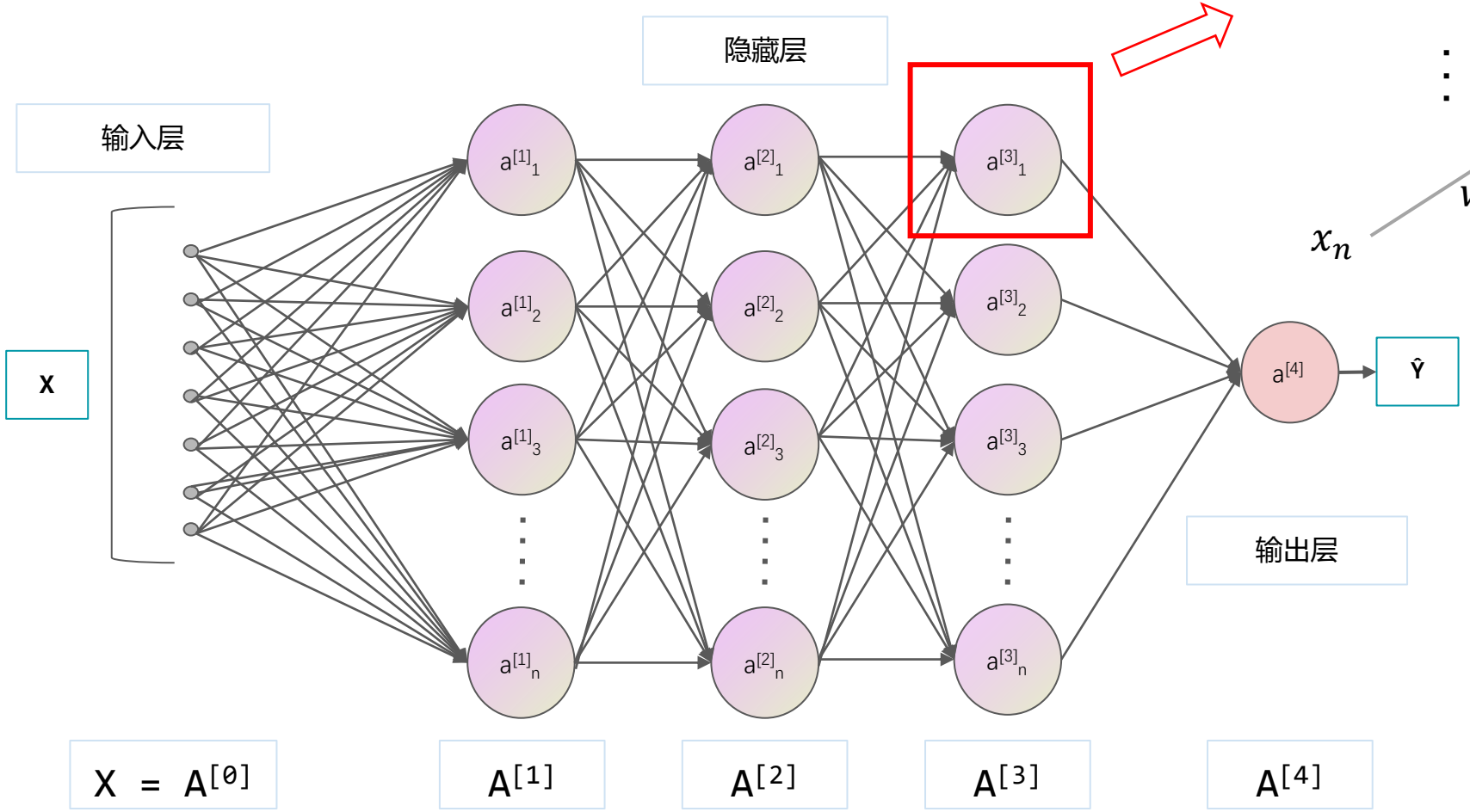
利用深度神经网络完成训练和预测

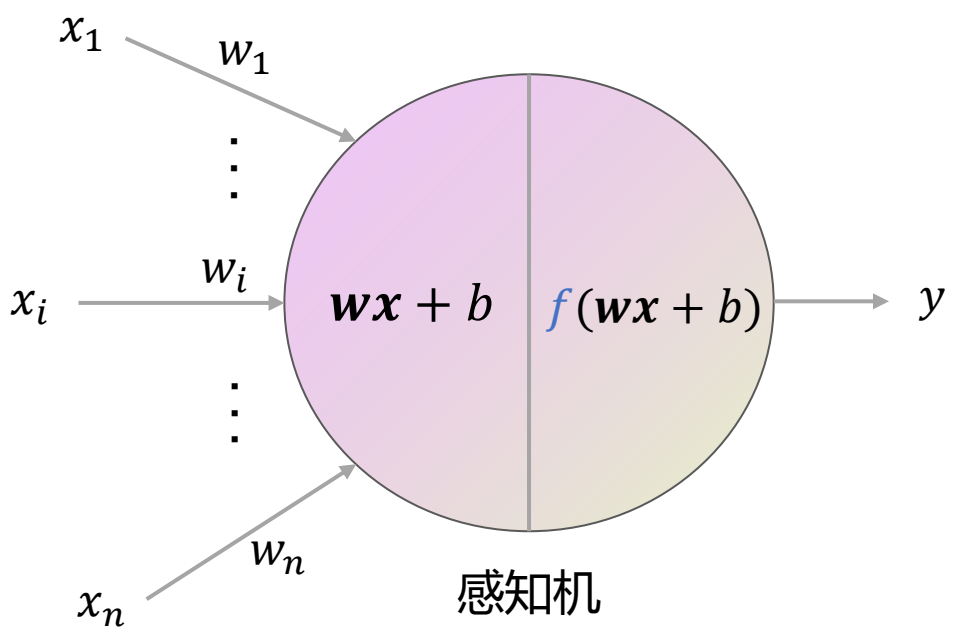
《深度学习之PyTorch物体检测实战》董洪义, ISBN: 978-7-111-64174-2, pp: 12-18.

机器学习基础：深度学习基础

❑ 神经网络（Artificial Neural Network）

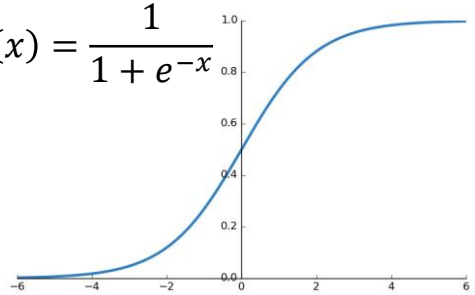
- 一个简单的前馈神经网络：





激活函数f的作用：根据需要调整线性回归的输出。
常见的激活函数：Logistic、Tanh、ReLu...

$$Logistic(x) = \frac{1}{1 + e^{-x}}$$

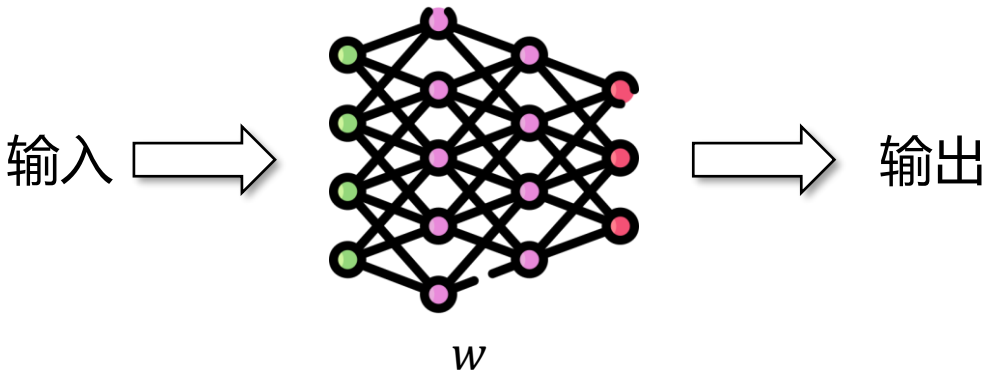


机器学习基础：深度学习基础

❑ 深度学习的目标

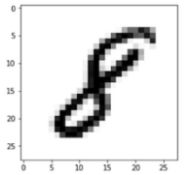
训练/学习

- 找到一个模型，对于特定输入产生期望的输出。



w：模型参数

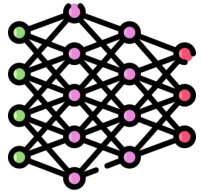
一些深度学习任务：

任务	给定输入	期望输出
图像分类		8
人脸识别		LeBron James
下一词预测	Looking for your __	reply
…	…	…

机器学习基础：深度学习基础

❑ 模型训练：损失函数（Loss Funtion）

- 对于一个随机初始化的模型或是一个未训练好的模型w，给定一个训练样本(x_0, y_0)，输入x_0输出一个预测值$\widehat{y_0}$，预测值与真实值会存在较大差距，用损失函数衡量真实值与预测值之间的差距。

前向传播：x_0 ⇨  ⇨ $\widehat{y_0}$　　损失函数：$f_0(w) = l(x_0, y_0, w) = Distance(\widehat{y_0}, y_0)$

w

- 将上述情况扩展到一个包含n个样本$(x_i, y_i), i \in [1, n]$的训练集上，训练集上的平均损失为：

$$\frac{1}{n}\sum_{i=1}^{n} f_i(w) = l(x_i, y_i, w)$$

$$f(w) = l(x, y, w)$$

深度学习训练的过程就是不断减小训练集上损失函数值（预测值与真实值差距）的过程。

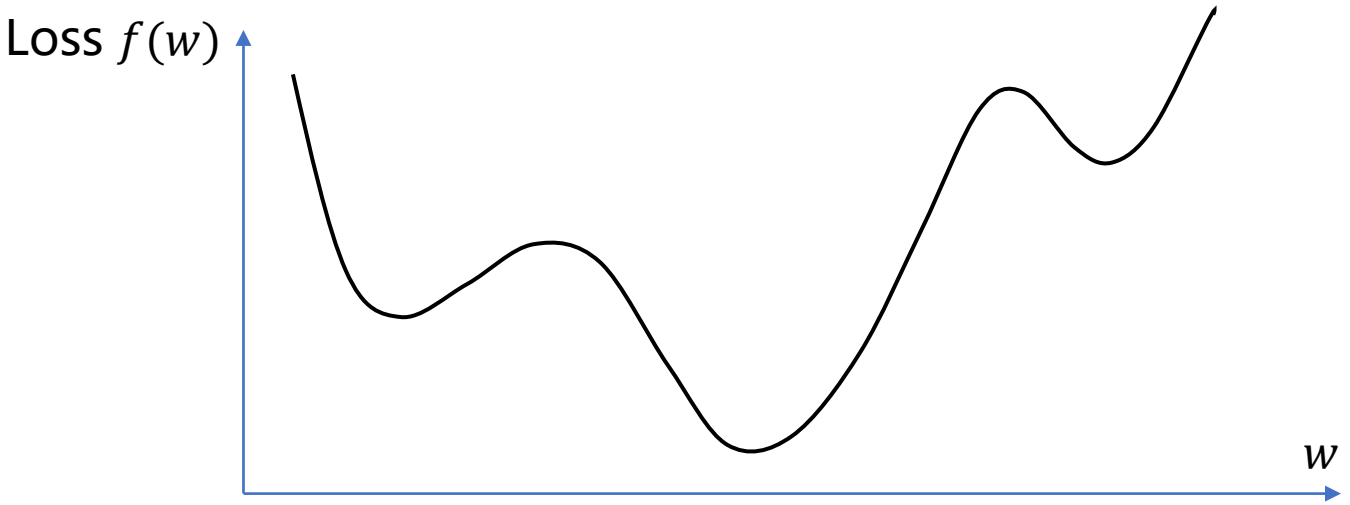
机器学习基础：深度学习基础

❑ 模型训练：损失函数（Loss Funtion）

- 给定一个包含n个样本$(x_i, y_i), i \in [1, n]$的训练集，深度学习的训练目标是：

$$\min_{w \in \mathbb{R}^d} f(w) \qquad \text{where } f(w) \overset{\text{def}}{=} \frac{1}{n}\sum_{i=1}^{n} f_i(w)$$

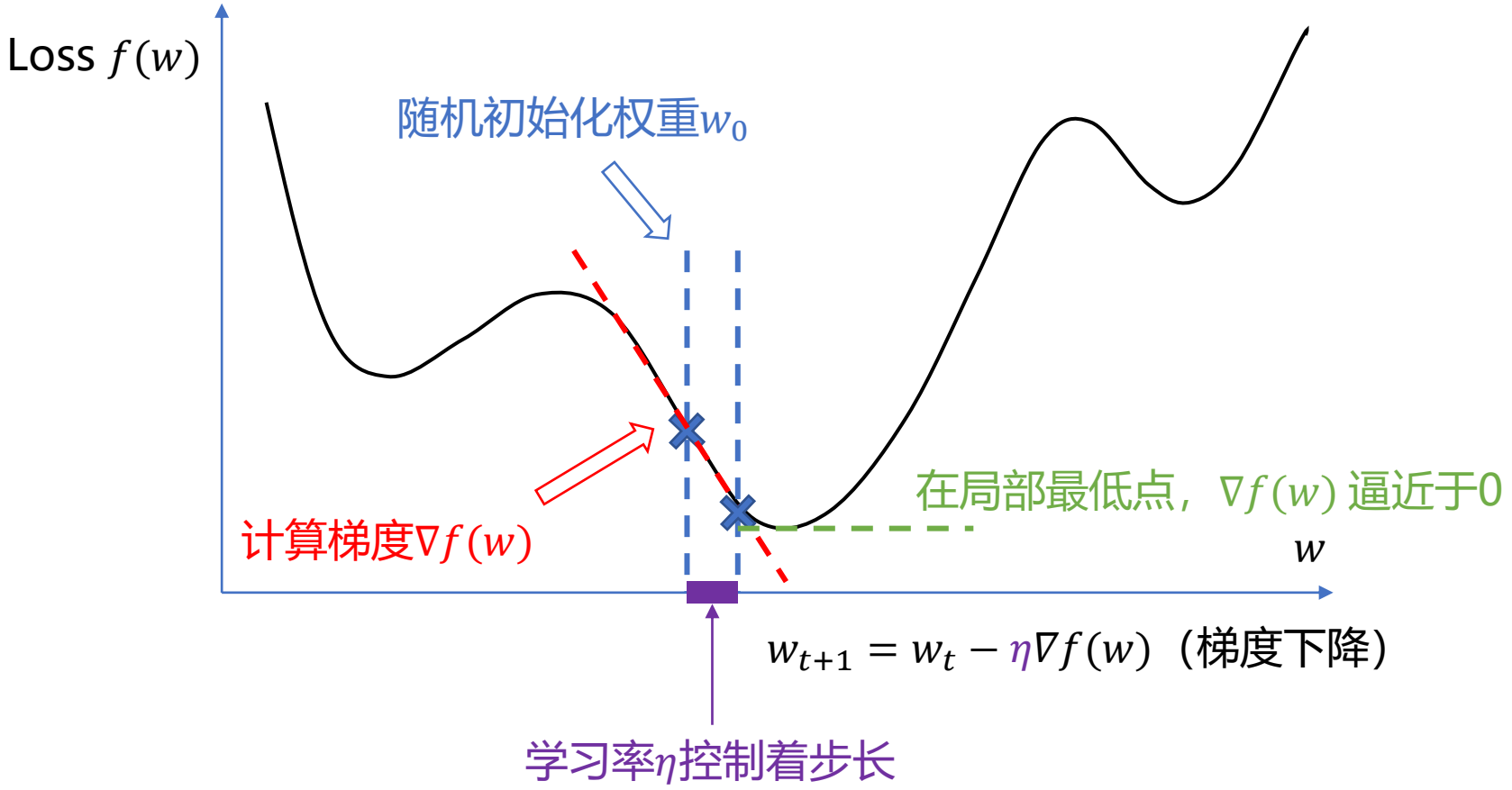
无闭式解：在深度神经网络中，w可能包含数百万个参数。
非凸函数：损失函数可能为非凸函数，即有多个局部最小值存在。



机器学习基础：深度学习基础

❑ 模型训练：梯度下降（Gradient Descent）

最优化问题：在一定约束条件下，求解一个目标函数的最大值（或最小值）问题。



训练什么时候终止?
--当模型更新足够小的时候
--收敛

$$\| w_{t+1} - w_t \| \leq \epsilon$$

or $$\| \nabla f(w_t) \| \leq \epsilon$$

机器学习基础：深度学习基础

❑ 模型训练：随机梯度下降（Stochastic Gradient Descent, SGD）

通常训练集中样本的数量特别大。

- 在梯度下降的每一步，随机选取训练集的一个小子集（mini-batch）投入训练。

$$w_{t+1} \leftarrow w_t - \eta \nabla f(w_t; x_k, y_k)$$

batch：每次投入训练的小批次。
batch size：batch的大小。
iteration：用一个batch训练一次叫作一个iteration。
epoch：全部训练集都被训练了一次叫做一个epoch。

- 与梯度下降相比，SGD需要更多次迭代收敛，但是每一次迭代要快很多。

机器学习基础：深度学习基础

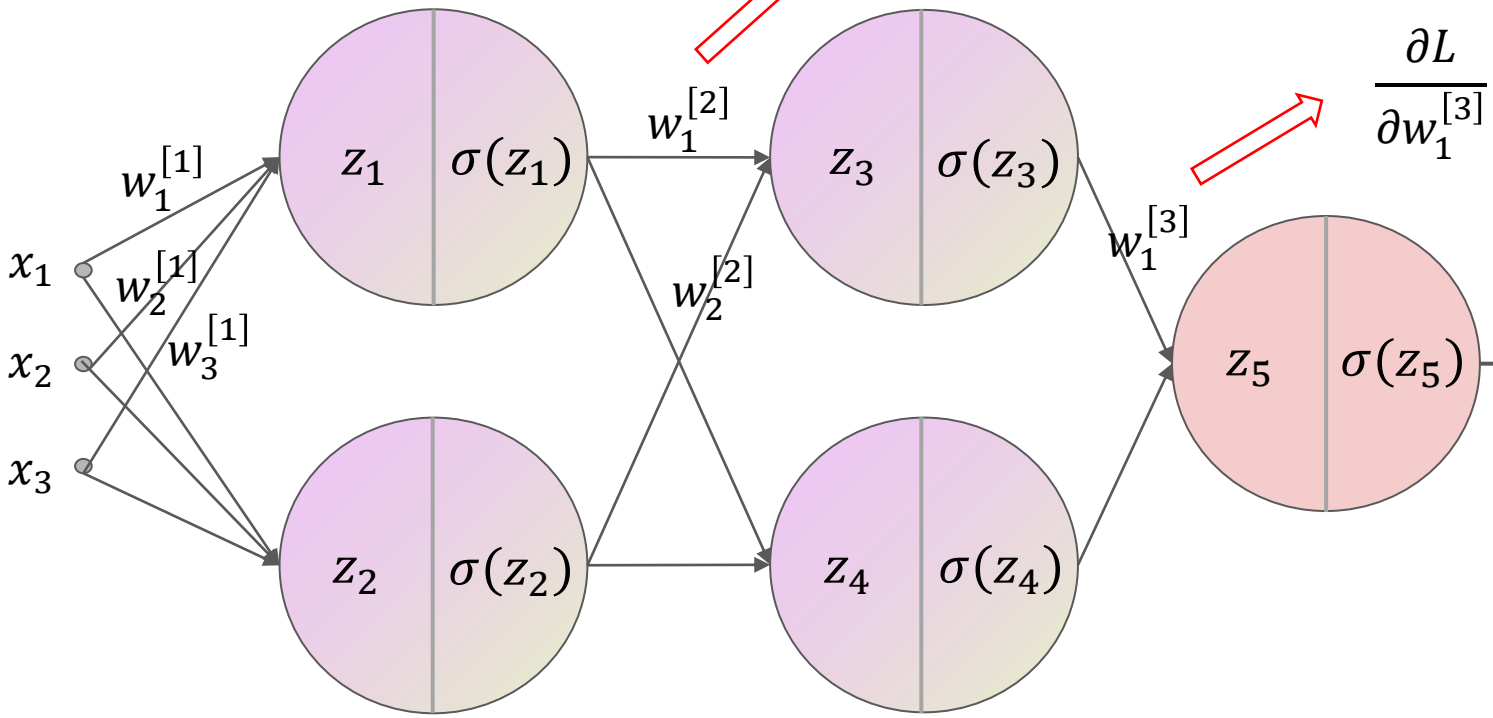
❑ 求解梯度：反向传播（Backpropagation）

$$z_1 = w_1^{[1]} \cdot x_1 + w_2^{[1]} \cdot x_2 + w_3^{[1]} \cdot x_3$$

$$z_3 = w_1^{[2]} \cdot \sigma(z_1) + w_2^{[2]} \cdot \sigma(z_2)$$

$$\frac{\partial L}{\partial w_1^{[2]}} = \frac{\partial L}{\partial \sigma(z_3)} \cdot \frac{\partial \sigma(z_3)}{\partial z_3} \cdot \frac{\partial z_3}{\partial w_1^{[2]}} = \frac{\partial L}{\partial \sigma(z_5)} \cdot \frac{\partial \sigma(z_5)}{\partial z_5} \cdot \frac{\partial z_5}{\partial \sigma(z_3)} \cdot \frac{\partial \sigma(z_3)}{\partial z_3} \cdot \frac{\partial z_3}{\partial w_1^{[2]}}$$

$$\frac{\partial L}{\partial w_1^{[3]}} = \frac{\partial L}{\partial \sigma(z_5)} \cdot \frac{\partial \sigma(z_5)}{\partial z_5} \cdot \frac{\partial z_5}{\partial w_1^{[3]}}$$



损失函数：

$$L(w) = Distance(\widehat{y_0}, y_0)$$

X = A[0] → A[1] → A[2] → A[3]

采用链式求导法则从后向前依次求解模型参数的梯度。

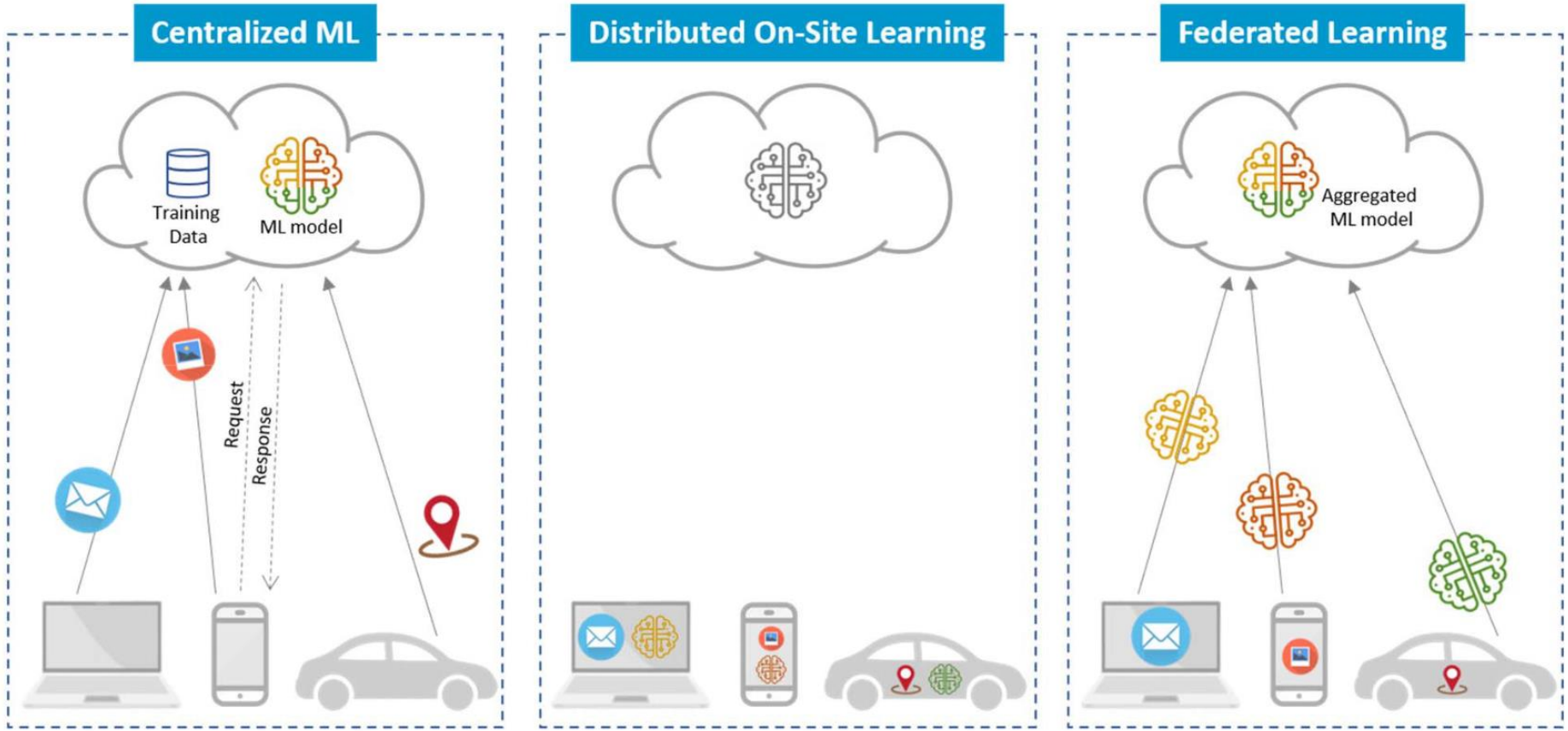
机器学习基础：深度学习基础

❑ 总结

- 定义一个损失函数，深度学习用损失函数来衡量模型预测值与真实值之间的差距。
- 深度学习的训练过程就是在训练集上通过多次迭代不断修正模型参数以减小损失函数值的过程，当损失值下降到逼近最低点（最小值）时，我们就说模型训练收敛了/训练完成了。
- 求解损失函数最小值的问题本质上是一个最优化问题，有多种优化方法可以求一个函数的最小值，深度学习采用的是梯度下降的方法。

目录

机器学习架构演变



隐私安全：	用户数据被云端拿到，易遭窃听	用户数据保留在本地	用户数据保留在本地
通信代价：	用户数据量大，高延迟	小，一次通信	较大
群体智慧：	融合了各方知识	没有融合各方知识	融合了各方知识

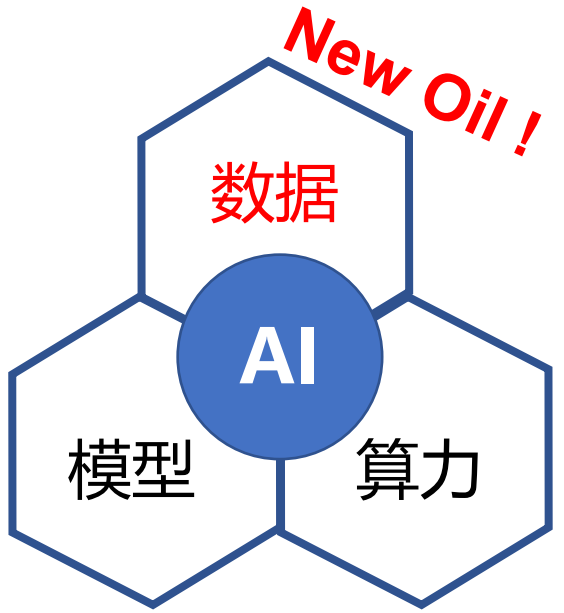
AbdulRahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C., & Guizani, M. (2020). A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. IEEE Internet of Things Journal, 8(7), 5476-5497.

目录

联邦学习（Federated Learning, FL）

❑ 数据孤岛与隐私安全担忧

- 在AI领域，数据是基础，然而数据通常以“数据孤岛”的形式存在。
- 传统的集中式学习中，数据采集和处理的过程中会被泄露。
- 隐私保护法规的完善：
  - 通用数据保护条例（GDPR）（2018）
  - 加州消费者隐私法案（CCPA）（2018）
  - 《数据安全法》（2021）
  - 《个人信息保护法》（2021）



Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216, 106775.

联邦学习（Federated Learning, FL）

❑ 数据孤岛与隐私安全担忧

- **通用数据保护条例**（General Data Protection Regulation, GDPR）

保护范围

只要是一个人所能产生出的任何数据，几乎都被重新定义为个人数据并受到保护。

- 个人身份 - 电话号码、地址、车牌等
- 生物特征 - 历数据、指纹、脸部辨识、视网膜扫描、相片等
- 电子纪录 - Cookie、IP 位置、移动设备 ID、社群网站活动纪录

原则

- 处理个人数据的业务流程必须在设计和默认情况下构建数据保护，这意味着个人数据必须使用假名化或匿名化进行存储，并且默认使用尽可能最高的隐私设置。
- 任何个人数据除非在法规规定的合法基础上完成，否则数据控制者或处理者必须从数据所有者那里获得明确的选择同意。
- 个人数据处理者必须清楚地披露任何数据收集，声明数据处理的合法基础和目的，保留数据的时间以及是否与任何第三方或欧盟以外的国家共享数据。

联邦学习（Federated Learning, FL）

❑ 数据孤岛与隐私安全担忧

- **中华人民共和国个人信息保护法**（Personal Information Protection Law of the People's Republic of China, PIPR）

保护范围

- 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。
- 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

法规

- **第二十九条**：处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。
- **第三十条**：个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。
- **第四十四条**：个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

联邦学习（Federated Learning, FL）

❑ 数据孤岛与隐私安全担忧

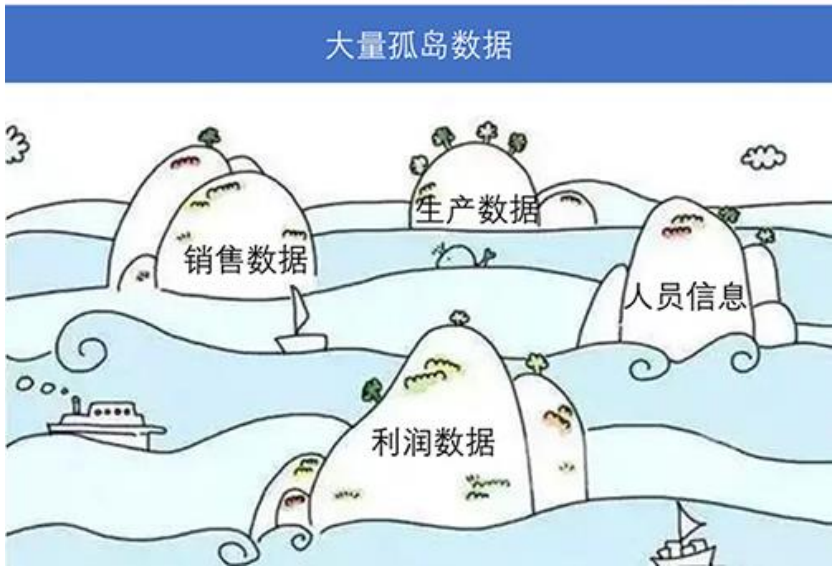
- **中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见（国务院公报2023年第1号）**

二、建立保障权益、合规使用的数据产权制度
（四）推进实施公共数据确权授权机制。

对各级党政机关、企事业单位依法履职或提供公共服务过程中产生的公共数据，加强汇聚共享和开放开发，强化统筹授权使用和管理，推进互联互通，打破“数据孤岛”。鼓励公共数据在保护个人隐私和确保公共安全的前提下，按照“原始数据不出域、数据可用不可见”的要求，以模型、核验等产品和服务等形式向社会提供，对不承载个人信息和不影响公共安全的公共数据，推动按用途加大供给使用范围。推动用于公共治理、公益事业的公共数据有条件无偿使用，探索用于产业发展、行业发展的公共数据有条件有偿使用。依法依规予以保密的公共数据不予开放，严格管控未依法依规公开的原始公共数据直接进入市场，保障公共数据供给使用的公共利益。

联邦学习（Federated Learning, FL）

- 数据孤岛与隐私安全担忧



数据孤岛

隐私安全

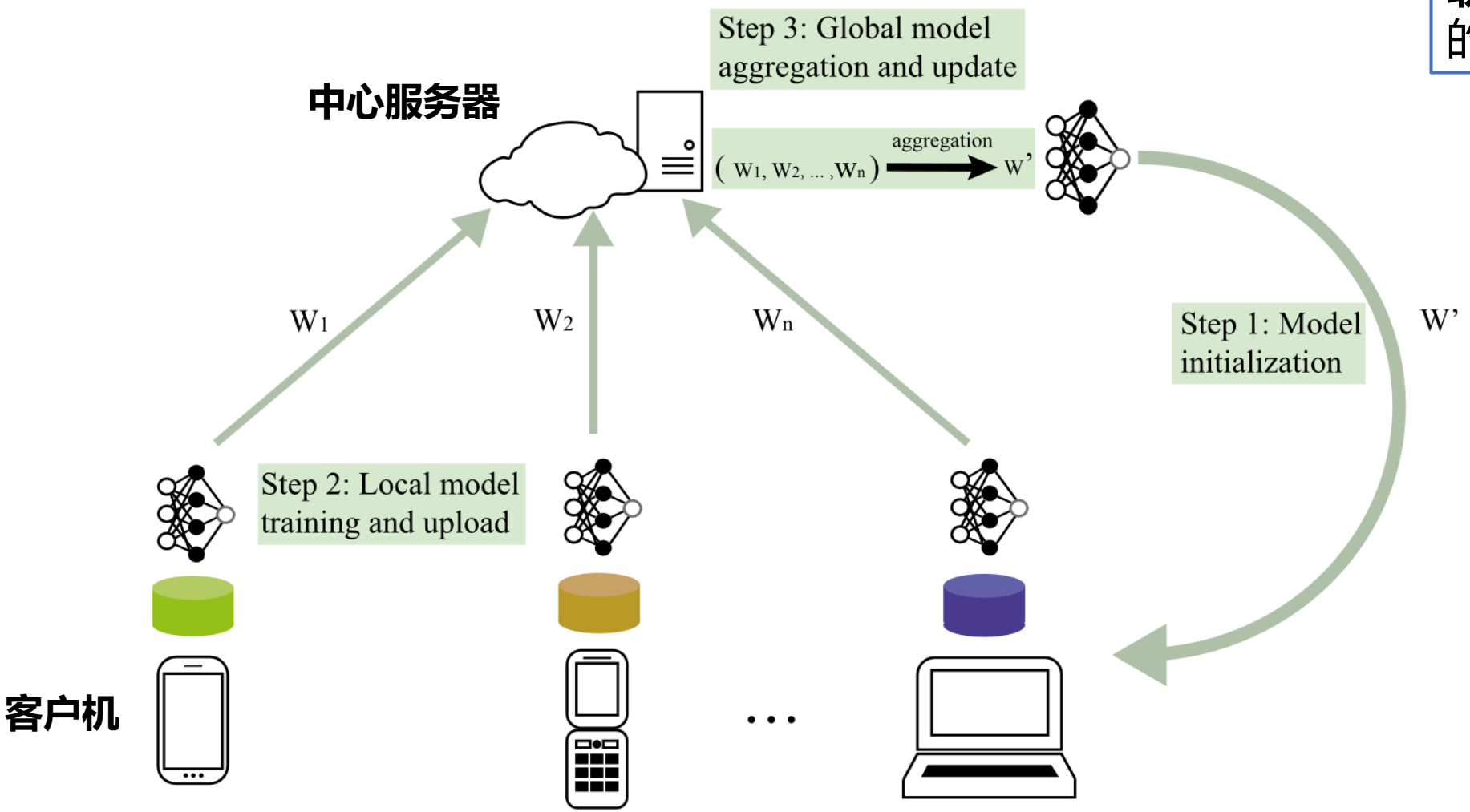
联邦学习：用户数据全程保留在本地不出域，保护了用户隐私！

图片来源：http://dustertech.com/news/529.html；视觉中国

联邦学习（Federated Learning, FL）

❑ 联邦学习基本流程

联邦学习：一种隐私保护的分布式机器学习范式。



Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216, 106775.

联邦学习（Federated Learning, FL）

❑ 联邦学习聚合算法baseline： FederatedSGD (FedSGD)

学习率：η；总客户机数量K；总样本量：n；每个客户端上的样本量n_k；选取的客户机比例C；

- 在每一通信轮(round) t：
  - **中心服务器**广播当前的全局模型w_t给每个被选取的客户机；
  - 每个被选取的**客户机**用自己的本地数据计算梯度：$g_k = \nabla F_k(w_t)$；
    - 方式1：每个被选取的**客户机**上传自己的梯度g_k；
      中心服务器聚合收到的梯度做梯度下降生成新的全局模型：
      - $w_{t+1} \leftarrow w_t - \eta \nabla F(w_t) = w_t - \eta \sum_{k=1}^{C \cdot K} \frac{n_k}{n} g_k$ 基于客户机本地样本数量的加权平均
    - 方式2：每个被选取的**客户机**梯度下降生成新的本地模型：$w_{t+1}^k \leftarrow w_t - \eta g_k$；
      中心服务器聚合收到的本地模型生成新的全局模型：
      - $w_{t+1} \leftarrow \sum_{k=1}^{C \cdot K} \frac{n_k}{n} w_{t+1}^k$ 基于客户机本地样本数量的加权平均

训练多轮⇒FedAvg

- 随机选取客户机参与训练≈传统深度学习中随机选取样本参与训练
- 每一轮只做一次梯度下降
- 每轮选取C比例的客户机参与训练：
  - $C = 1$：full-batch GD
  - $C < 1$：SGD

McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). PMLR.

联邦学习（Federated Learning, FL）

❑ 联邦学习聚合算法baseline：FederatedAveraging (FedAvg)

FedSGD：通信代价大 ⟹ 增加每个客户机上的计算量，减少通信轮数

学习率：η；总客户机数量K；总样本量：n；每个客户端上的样本量n_k；选取的客户机比例C；

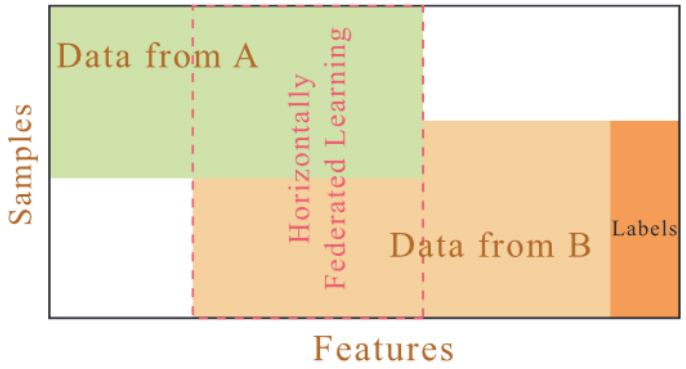
- 在每一通信轮(round) t：
  - **中心服务器**广播当前的全局模型w_t给每个被选取的客户机；
  - 每个被选取的**客户机**用自己的本地数据计算梯度：$g_k = \nabla F_k(w_t)$；
    - 每个被选取的**客户机**训练E个epochs：$w_{t+1}^k \leftarrow w_t - \eta g_k$；
    - **中心服务器**聚合收到的本地模型生成新的全局模型：
      - $w_{t+1} \leftarrow \sum_{k=1}^{C \cdot K} \frac{n_k}{n} w_{t+1}^k$ 基于客户机本地样本数量的加权平均

- 假设客户机训练的mini-batch size=B，则每轮迭代次数为$u_k = E\frac{n_k}{B}$

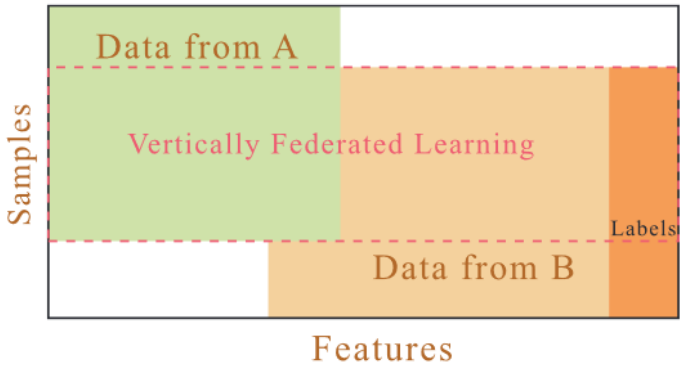
McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). PMLR.

目录

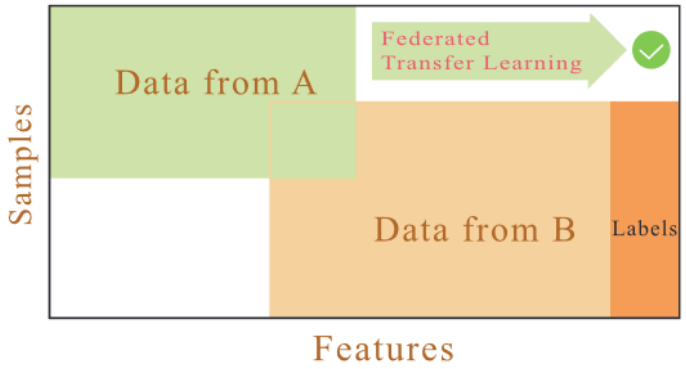
联邦学习分类：基于数据划分方式



横向联邦学习



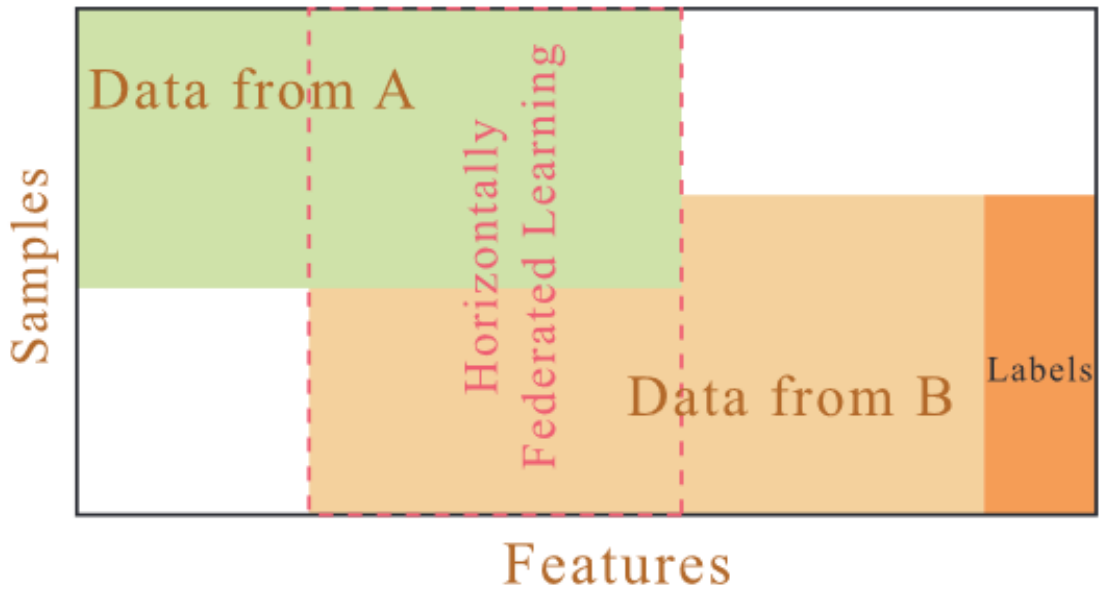
纵向联邦学习



联邦迁移学习

联邦学习分类：基于数据划分方式

❑ 横向联邦学习（Horizontal Federated Learning，HFL）



- 特征维度重叠很多，但是用户样本维度重叠很少。
- 拿出特征维度重叠但是用户不完全重叠的部分来训练。

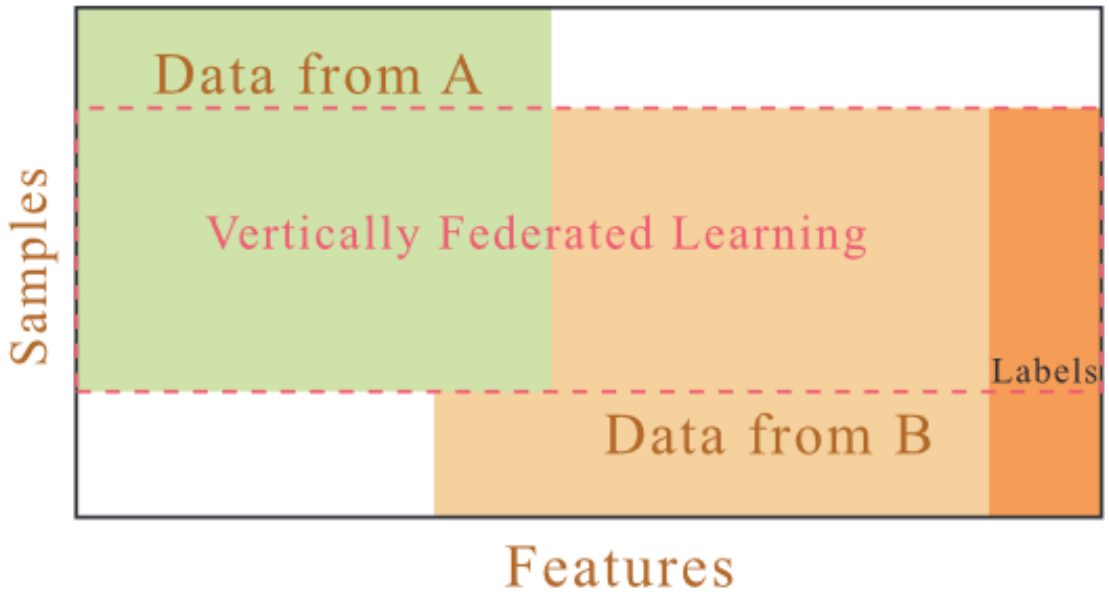
应用：多家医院跨区域协作训练模型

- HFL适用于业务相同但是用户群体不一样的场景。

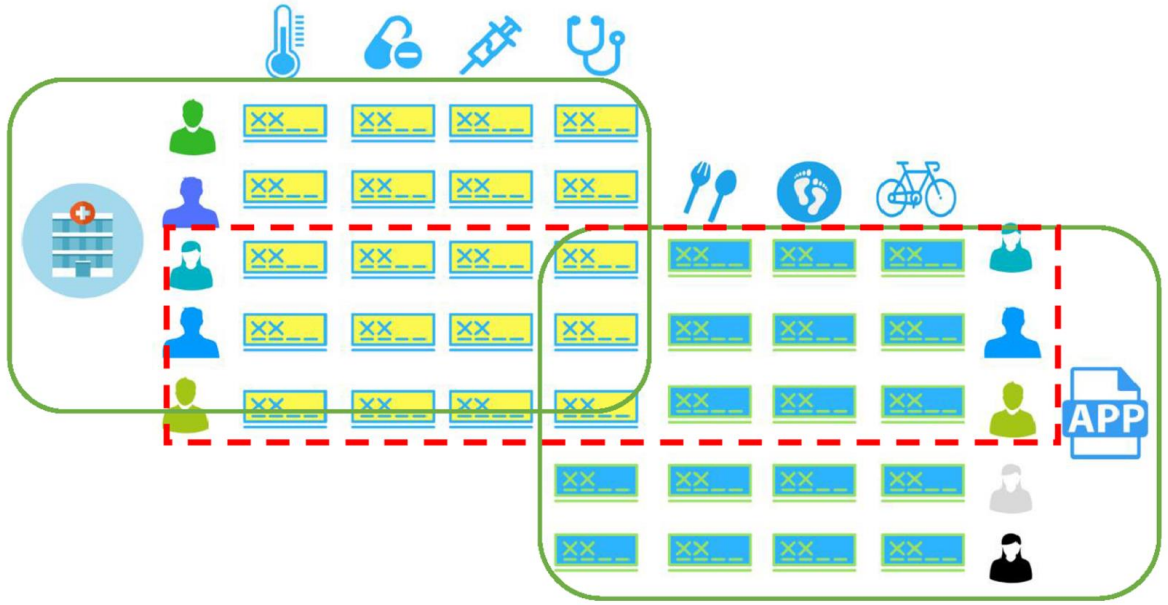
- *Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216, 106775.*
- *Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. Computers & Industrial Engineering, 149, 106854.*

联邦学习分类：基于数据划分方式

❑ 纵向联邦学习（Vertical Federated Learning，VFL）



- 特征维度重叠很少，但是用户样本维度重叠很多。
- 拿出用户维度重叠但是特征不完全重叠的部分来训练。



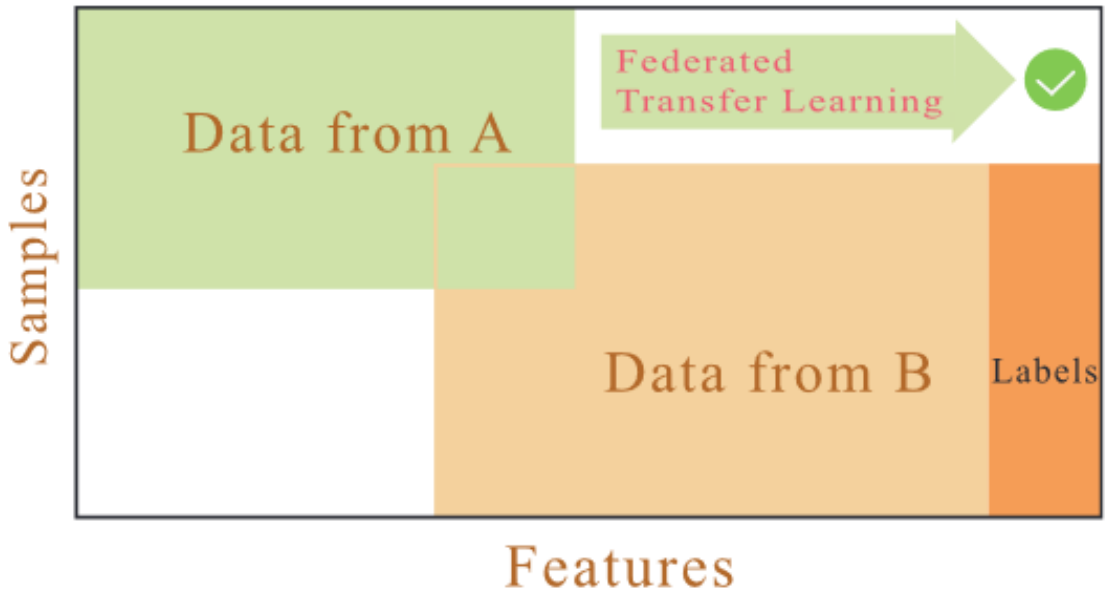
应用：同区域医院与手机应用公司协作训练模型

- VFL适用于用户群体相同但是业务不一样的场景。

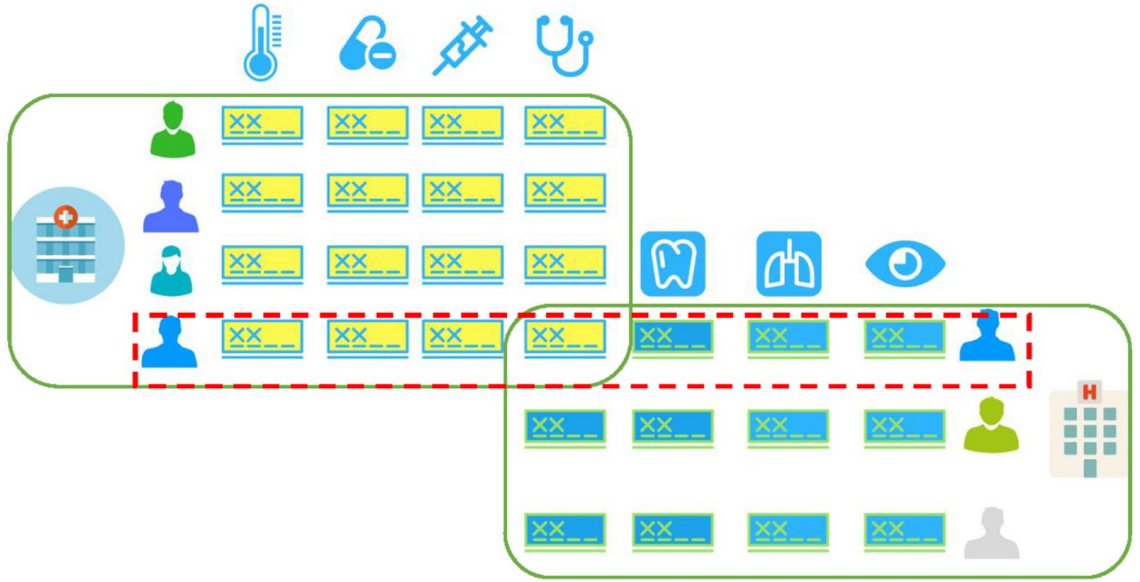
- *Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216, 106775.*
- *Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. Computers & Industrial Engineering, 149, 106854.*

联邦学习分类：基于数据划分方式

❑ 联邦迁移学习（Federated Transfer Learning，FTL）



- 特征与用户样本维度重叠均很少，不分割数据。
- 采用迁移学习去克服数据与标签的不足。



应用：一家医院的一些疾病诊断和治疗信息可以通过FTL传输到另一家医院，以帮助其他疾病的诊断

- VFL适用于用户群体与业务都鲜有重合的场景。

- *Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216, 106775.*
- *Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. Computers & Industrial Engineering, 149, 106854.*

目录

联邦学习中的一些隐私保护技术

- 安全多方计算（Secure Multi-party Computation，MPC）
- 同态加密（Homomorphic Encryption，HE）
- 差分隐私（Differential Privacy，DP）

联邦学习中的一些隐私保护技术

❑ 安全多方计算（Secure Multi-party Computation，MPC）

- 安全多方计算（MPC）允许多方在自己的私有输入上协作计算一个函数，但是除了函数的输出以外不能泄露任何信息，即每一方只能得到其函数输出值而不能得到其他方的输入输出。

具体而言，MPC允许n方协作计算函数f：

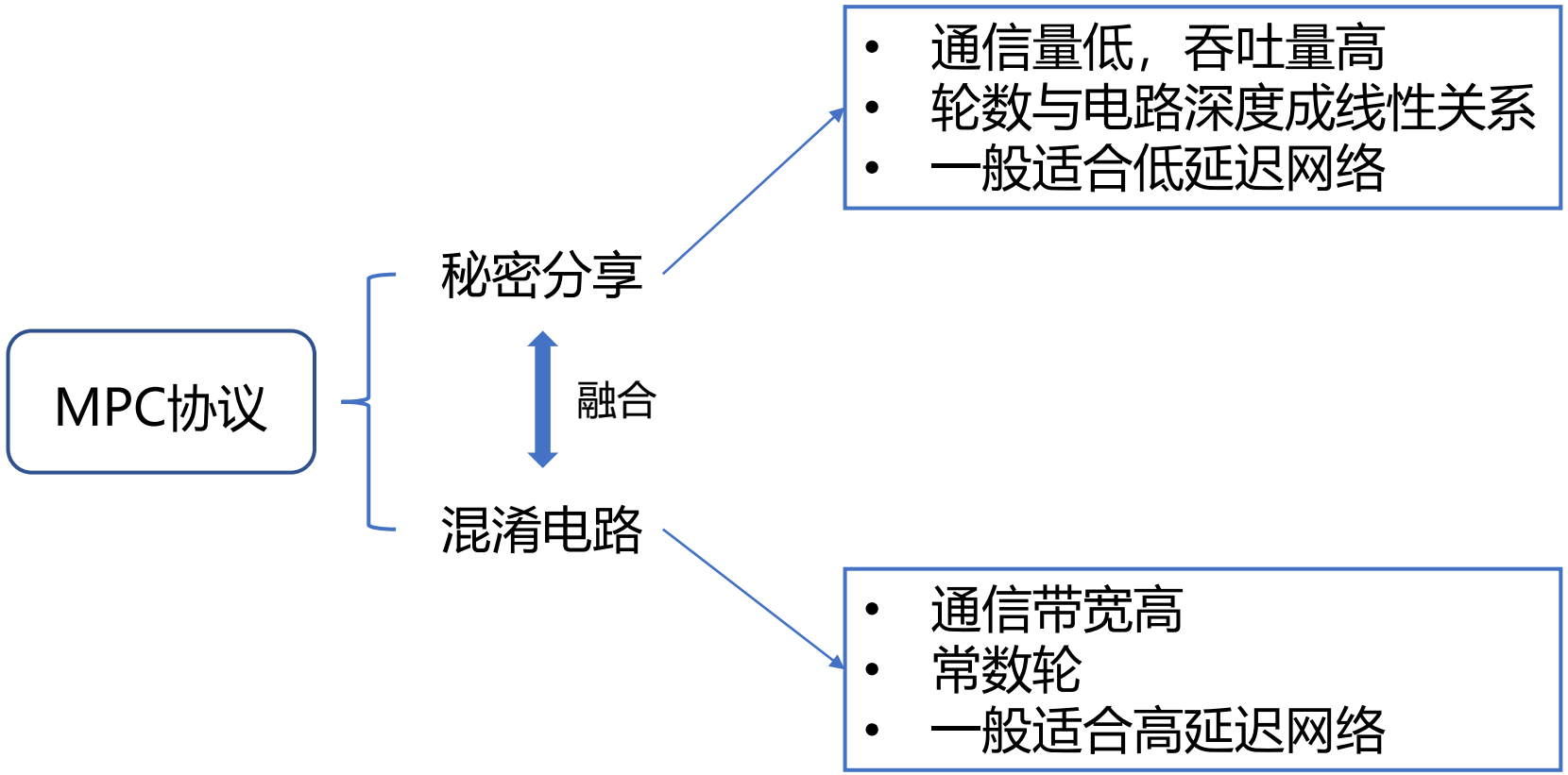
$$(y_1, \ldots, y_n) \leftarrow f(x_1, \ldots, x_n)$$

其中每一方P_i持有一个输入x_i，得到其输出y_i，并且不能得到(x_i, y_i, f)之外的其他任何信息。

- *Feng, D., & Yang, K. (2022). Concretely efficient secure multi-party computation protocols: survey and more. Security and Safety, 1, 2021001.*
- *Boneh, D., & Shoup, V. (2023). A graduate course in applied cryptography. Version 0.6.*

联邦学习中的一些隐私保护技术

❑ 安全多方计算协议的基本设计方法



Feng, D., & Yang, K. (2022). Concretely efficient secure multi-party computation protocols: survey and more. Security and Safety, 1, 2021001.

联邦学习中的一些隐私保护技术

❑ 安全多方计算：秘密分享（Secret Sharing）

- 秘密分享的基本思想是将一个秘密分割成多份并分发给多个参与方，使得所有或一定数量的参与方（如达到门限值t个参与方）才能重新还原出该秘密。

具体而言，一个秘密分享方案包含一个拥有秘密s的秘密分发方和n个参与方。一个秘密分享方案主要包含如下两个算法：

- 秘密分发算法：秘密分发方将秘密s分割成n份，并将这n份份额分别分发给n个参与方。
- 秘密重构算法：符合条件的参与方集合一起用自己的份额恢复出原始秘密s。

- 该技术可保证即使攻击者获取部分参与者秘密，也无法还原出原始秘密。
- 该技术因允许只需一定数量的参与方即可还原出秘密，可用于避免单点故障问题。

联邦学习中的一些隐私保护技术

❑ 安全多方计算：秘密分享（Secret Sharing）

- **Shamir秘密分享**：又叫(t,n)门限秘密分享。假设一个秘密分发方与n个参与方$U=\{U_1,U_2,\dots,U_n\}$需要执行Shamir秘密分享方案，需要至少t个参与方一起才能恢复秘密。

基本思想：对于任意一个t-1次多项式函数，只需要获得其曲线上的t个不同的点就可以通过多项式插值（如拉格朗日插值法）确定该多项式。

- 初始化：生成一个有限域Z_p，$p>s, p>n$。
- 秘密分发算法：秘密分发方随机生成$t-1$个整数$a_i \in Z_p, 1\le i\le t-1$，生成一个$t-1$次多项式$f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+a_0\ (mod\ p)$，其中$f(0)=a_0=s$；随机选取$n$个互不相同的整数$x_i \in Z_p, 1\le i\le n$；分别将$x_i$代入多项式计算得到n个秘密份额$s_1=f(x_1), s_2=f(x_1),\dots,s_n=f(x_n)$，并将这$n$个份额分别分发给$n$个参与方。
- 秘密重构算法：　参与方的t个用自己的秘密份额借助拉格朗日插值公式恢复秘密：$s=(-1)^{t-1}\sum_i^k f(x_i)\prod_{j=1,j\neq i}^{t}\frac{x_j}{x_i-x_j}\ (mod\ p)$。

Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.

联邦学习中的一些隐私保护技术

❑ 同态加密（Homomorphic Encryption，HE）

- 一种加密形式，它允许对密文进行特定形式的代数运算得到仍然是加密的结果，将其解密所得到的结果与对明文进行同样的运算结果一样。

$$E(X\Delta Y) = E(X)\Delta Y(Y)$$

同态：近世代数中的概念，从一个代数结构到同类代数结构的映射，它保持所有相关的结构不变。

- 设$\langle G,*\rangle$和$\langle H,\circ\rangle$是两个代数结构，$f: G \to H$是一个映射，如果对于$\forall a, b \in G$，都有$f(a * b) = f(a) \circ f(b)$，则称$f$是从$G$到$H$的一个同态或同态映射。

李顺东, 窦家维, & 王道顺. (2015). 同态加密算法及其在云安全中的应用. 计算机研究与发展, 52(6), 1378-1388.

联邦学习中的一些隐私保护技术

❑ 同态加密的分类

$$E(X\Delta Y) = E(X)\Delta Y(Y)$$

	可操作次数	适用于的操作Δ
部分同态加密（Partially Homomorphic Encryption，PHE）	无限次	仅适用于加法（加法同态加密）或乘法（乘法同态加密）操作
全同态加密（Fully Homomorphic Encryption，FHE）	无限次	对加法、乘法运算均成立
些许同态加密（Somewhat Homomorphic Encryption，SHE）	有限次	

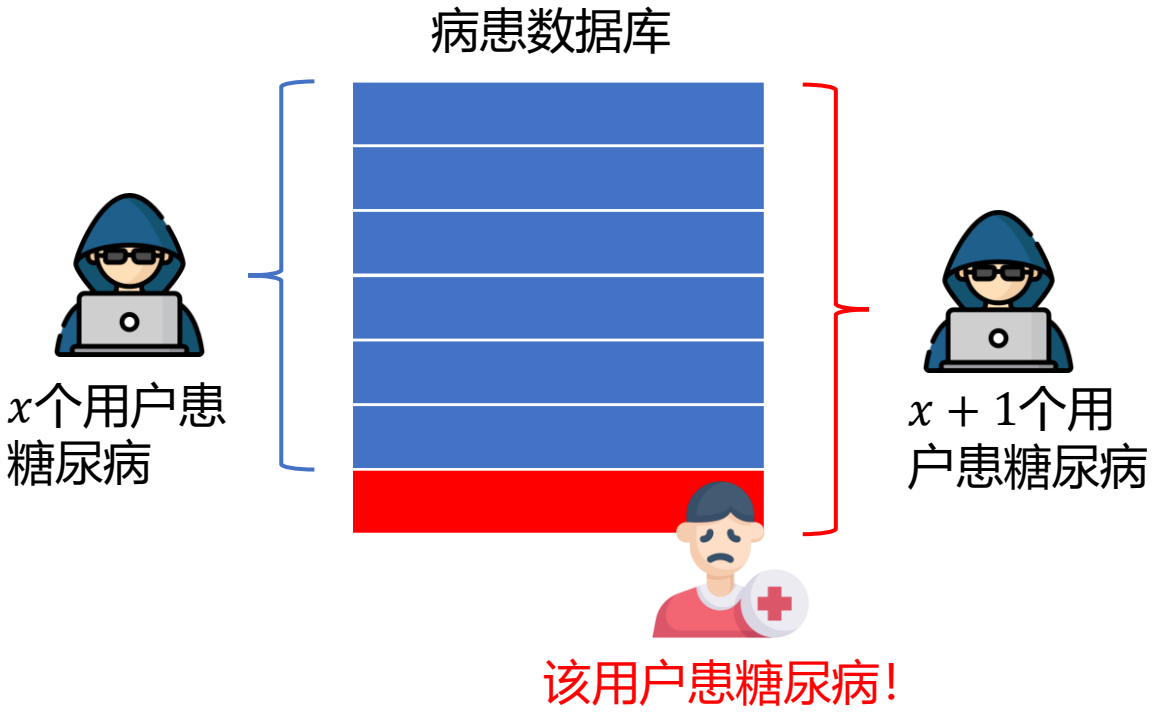
李顺东, 窦家维, & 王道顺. (2015). 同态加密算法及其在云安全中的应用. 计算机研究与发展, 52(6), 1378-1388.

联邦学习中的一些隐私保护技术

❑ 差分隐私（Differential Privacy，DP）

差分隐私是Dwork在2006年首次提出的一种隐私定义，函数的输出结果对数据集中任何特定记录都不敏感。

假设这样一种差分攻击场景：



差分隐私：使得攻击者的知识不因新样本的出现而发生改变。

添加噪声：使查询结果变成一个随机变量，使加入新样本前后的数据库查询结果的分布相近，如此以来攻击者分不清查询结果来自于哪一个数据库，便无法获取新知识。

$$\mathcal{M}(D) = f(D) + r$$

噪声

查询函数

保障了个体级别的隐私

联邦学习中的一些隐私保护技术

❑ 差分隐私形式化定义

- **邻接数据集**：仅有一条记录不同的两个数据集D，D'。
- **随机化算法$\mathcal{M}$**：对于特定输入，该算法的输出不是固定值，而是服从某一分布。
- **隐私预算ϵ**：控制算法的隐私保护程度，ϵ越小，隐私保护效果越好。

$\mathcal{M}(D) = f(D) + r$

- **隐私损失**：对于任意的输出结果S：

$$\text{privacyloss} = \left| \ln \frac{\Pr[\mathcal{M}(\mathrm{D}) \in \mathrm{S}]}{\Pr[\mathcal{M}(\mathrm{D}') \in \mathrm{S}]} \right|$$

KL散度

其描述了算法$\mathcal{M}$在邻接数据集上输出同一个值的概率差别大小。

◆ **ϵ −差分隐私**：$\text{privacyloss} = \left| \ln \frac{\Pr[\mathcal{M}(\mathrm{D}) \in \mathrm{S}]}{\Pr[\mathcal{M}(\mathrm{D}') \in \mathrm{S}]} \right| \leq \epsilon \Rightarrow \Pr[\mathcal{M}(D) \in S] \leq \Pr[\mathcal{M}(D') \in S] \times \mathrm{e}^{\epsilon}$

严格

◆ **(ϵ, δ) −差分隐私**：$\Pr[\mathcal{M}(D) \in S] \leq \Pr[\mathcal{M}(D') \in S] \times \mathrm{e}^{\epsilon} + \delta$

松弛

失败概率

联邦学习中的一些隐私保护技术

❑ 差分隐私：敏感度（Sensitivity）

为满足差分隐私，需要添加多少噪声量？—— 取决于查询函数的敏感度。

- 函数f的敏感度：当输入由数据集D变化为邻接数据集D'后，f的输出变化程度。

◆ 全局敏感度（Global Sensitivity）：$GS(f) = \max_{D,D'} |f(D) - f(D')|$；该敏感度的定义与查询的数据集无关，即对于任意数据集都成立。　　太严格了！

◆ 局部敏感度（Local Sensitivity）：$LS(f, D) = \max_{D'} |f(D) - f(D')|$；将两个数据集中的一个作为待查询的实际数据集，仅考虑此数据集的所有邻接数据集。

- l_1敏感度：$|f(D) - f(D')| \leftarrow l_1 - norm$
- l_2敏感度：$|f(D) - f(D')| \leftarrow l_2 - norm$

$$l_p - norm: \quad D(X, Y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{\frac{1}{p}}$$

联邦学习中的一些隐私保护技术

❑ 差分隐私中常用的随机化算法（机制）

$$\mathcal{M}(D) = f(D) + r$$

- 拉普拉斯机制（Laplace mechanism）：

$$r = Lap(\frac{S}{\epsilon})$$

- 高斯机制（Gaussian mechanism）：

$$r = Gaus(b)$$

- 以0为中心，以b为尺度的拉普拉斯分布为：$Lap(x|b) = \frac{1}{2b}e^{-\frac{|x|}{b}}$，该分布方差为$2b^2$
- 满足$(\epsilon, 0)$ −差分隐私
- s为l_1敏感度

- 以0为中心，以 b 为尺度的高斯分布为：$\mathrm{Gaus}(x|b) = \frac{1}{\sqrt{2\pi}b}e^{-\frac{x^2}{2b^2}}$，该分布方差为$b^2$
- 当$b^2 > 2\ln(1.25/\delta)$且$\delta \geq bs/\epsilon$时，满足$(\epsilon, 0)$ −差分隐私
- s为l_2敏感度

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 9(3–4), 211-407.

联邦学习中的一些隐私保护技术

❑ 差分隐私中常用的随机化算法（机制）

拉普拉斯机制与高斯机制针对的都是数值型的回复，只需直接在回复的数值结果上增加噪声即可。如果我们想返回一个准确结果（即不能直接在结果上增加噪声），同时还要保证回复过程满足差分隐私，该怎么办呢？

—— 指数机制

- 指数机制（Exponential mechanism）：
  - 选择一个备选回复集合R
  - 指定一个全局敏感度为s的评分函数f
  - 指数机制输出$r \in R$，各个回复的输出概率与下述表达式成正比：

$$\exp\left(\frac{\epsilon f(D,r)}{2s}\right)$$

例如，假设我们要为一个大型会议敲定一个日期。我们想选择一个与尽可能少的参会者有时间冲突的日期来举办会议。在这个场景下，在举办日期上增加噪声可能会使日期从星期五变成星期六，使冲突参会者的数量显著增加。应用指数机制就可以完美解决此类问题：既不需要在日期上增加噪声，又可以实现差分隐私。

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 9(3–4), 211-407.

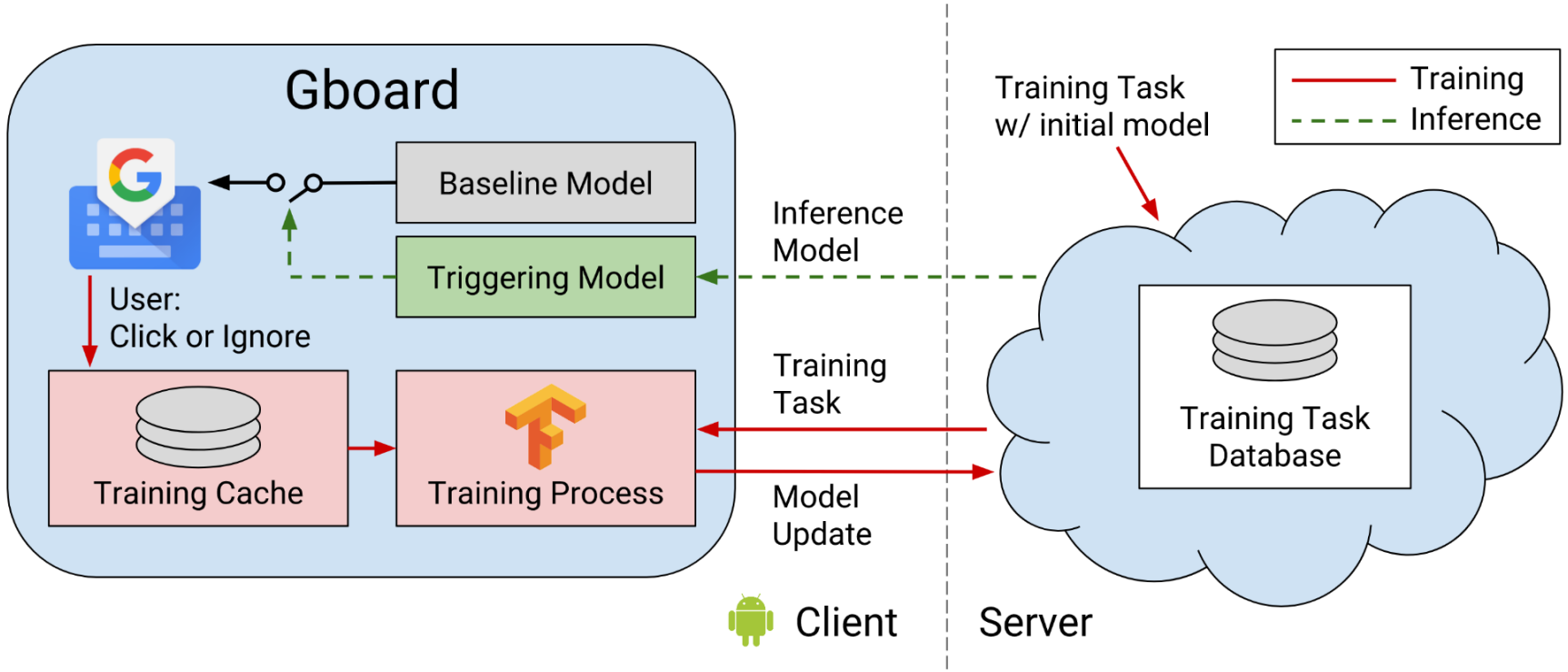
目录

联邦学习应用

❑ Google Gboard改善输入预测质量

训练一个模型预测查询建议是否是有用的，以此过滤掉不相关的查询。

- Baseline Model：on-device训练，生成备选集。
- Triggering Model：联邦学习训练（用户数据），从备选集中筛选出最终结果。



Yang, T., Andrew, G., Eichner, H., Sun, H., Li, W., Kong, N., ... & Beaufays, F. (2018). Applied federated learning: Improving google keyboard query suggestions. arXiv preprint arXiv:1812.02903.

联邦学习应用

❑ 医疗应用

疾病预测：每个医疗机构可能都有大量患者数据，但这可能远远不足以训练他们自己的预测模型。需要有一个多数据源医疗数据共享平台，在能够保证数据源隐私安全的情况下又能够实现数据价值的共享。

- **全基因组关联分析**：人类的很多疾病跟基因突变有关。全基因关联分析（GWAS）是指从人类全基因组范围内找出存在的序列变异，已广泛地应用于临床的早期疾病筛查、用药指导及辅助诊断等领域。
  - 隐私安全：基于几十个基因位点（SNPs）数据就可以基本确定一个个体的身份。
  - 大量样本：非常依赖大量基因数据的积累。

iPRIVATES框架

- **跨国川崎病联合研究**：罕见疾病是医学研究中经常遇到的问题，但同一国家往往存在样本少，在不同医院分散等实际困难，极大的阻碍了相关研究，诊断治疗工作。

PRINCESS：全球首例跨国（英国、美国、新加坡）罕见病多中心遗传数据隐私保护分析

- **影像学深度分析引擎**：医学影像学数据由于数据孤岛问题、传统数据脱敏的局限性带来的隐私问题、数据监管问题等，无法实现数据安全有效被利用。
- **电子病历（EMR）结构化**：在基于EMR的下游应用研究中，往往需要进一步对EMR进行结构化，比如从诊断中结构化出疾病名称、发病部位和并发症等。构建信息抽取模型需要大量的标注数据。在医疗领域，受限于信息安全和隐私保护等法律法规的合格性要求，电子病历是不能离院的。

来源：中国信息通信研究院《联邦学习场景应用研究报告》2022.

联邦学习应用

❑ 金融应用

- **信贷风控**：金融行业需要各个行业维度的数据去覆盖各类业务产品与风控需求，从而能够使业务人员及时准确地洞察不同来源与业务场景的风险行为变化。
  - 隐私计算技术可以在保护用户信息不泄露的前提下将来自更多元，多维度的数据纳入联合风控模型中，从而实现更精细的洞察，构建更精准的风控模型。
  - 各类金融机构也可基于隐私计算技术，利用多维度数据建立联合金融风险模型，共享黑名单与风控应用等。在数据没有离开各自本地的情况下，扩充多方特征或样本，使模型效果不断提高。

- **零售营销**：金融机构可利用历史营销样本通过纵向联邦学习的方式与支付机构、运营商、 互联网机构、政务部门等外部数据源进行联合建模来优化营销效果。
  - 如在某银行在面向新客进行的进件营销上的场景中，由于银行在进件业务流程中的数据维度一般较为单一，不能较好的综合判断进件客户的价值潜力。行业服务商通过联邦学习的方式，安全合规的联合外部数据源，在保证数据不出库的情况下，补充了征信类、通信类、终端类、行为偏好类数据特征进行纵向联邦建模，较大的提升了APP端进件营销的响应率。

- **反洗钱监督**：通过横向联邦学习，各个金融机构无需建立物理模型即可共享通用模型，可以有效解决该领域样本少、数据质量低的问题。 特别针对中小金融机构而言，在不共享用户数据的前提下，通过联合大型金融机构或联合多家金融机构，可以共同建立横向联邦反洗钱模型，提高侦测能力。

来源：中国信息通信研究院《联邦学习场景应用研究报告》2022.

联邦学习应用

❑ 其他应用

- **政务开放**：2020 年 12 月 30 日，中央全面深化改革委员会第十七次会议审议通过《关于建立健全政务数据共享协调机制加快推进数据有序共享的意见》，强调要全面构建政务数据共享安全制度体系、管理体系、 技术防护体系，打破部门信息壁垒，推动数据共享对接更加精准顺畅。
  - 在政务数据开放共享的过程中，由于缺乏可信的数据资产权利确认方案，导致政府部门不愿意共享数据。因缺乏有效的隐私安全保护技术，数据共享后无法限制数据用途，导致数据滥用和隐私泄露等问题，政府部门共享数据意愿较低。联邦学习相关产品可以与大数据开发组件集成，打破政府部门数据孤岛，实现跨部门、与社会数据等安全共享。
- **个性化推荐广告**：如果想要实现更加个性化的策略，广告主通常需要上传一方数据到媒体平台的工具上进行洞察和分析，但出于行业特性或数据安全的考虑往往只能止步。

来源：中国信息通信研究院 《联邦学习场景应用研究报告》2022.

谢谢！

邬长倜

2023.4.12