分离和联邦混合学习体系结构的性能和隐私分析

本文提出了一种新的混合联邦分裂学习体系结构，以结合效率和隐私方面的好处。
评估表明，联邦分裂学习可以减少每个运行联邦学习的客户端所需的计算能力，并使分裂学习并行化，同时在训练过程中保持对不平衡数据集的高预测精度。此外，与并行分割学习相比，FSL在特定的隐私方法中提供了更好的准确性和隐私权衡。

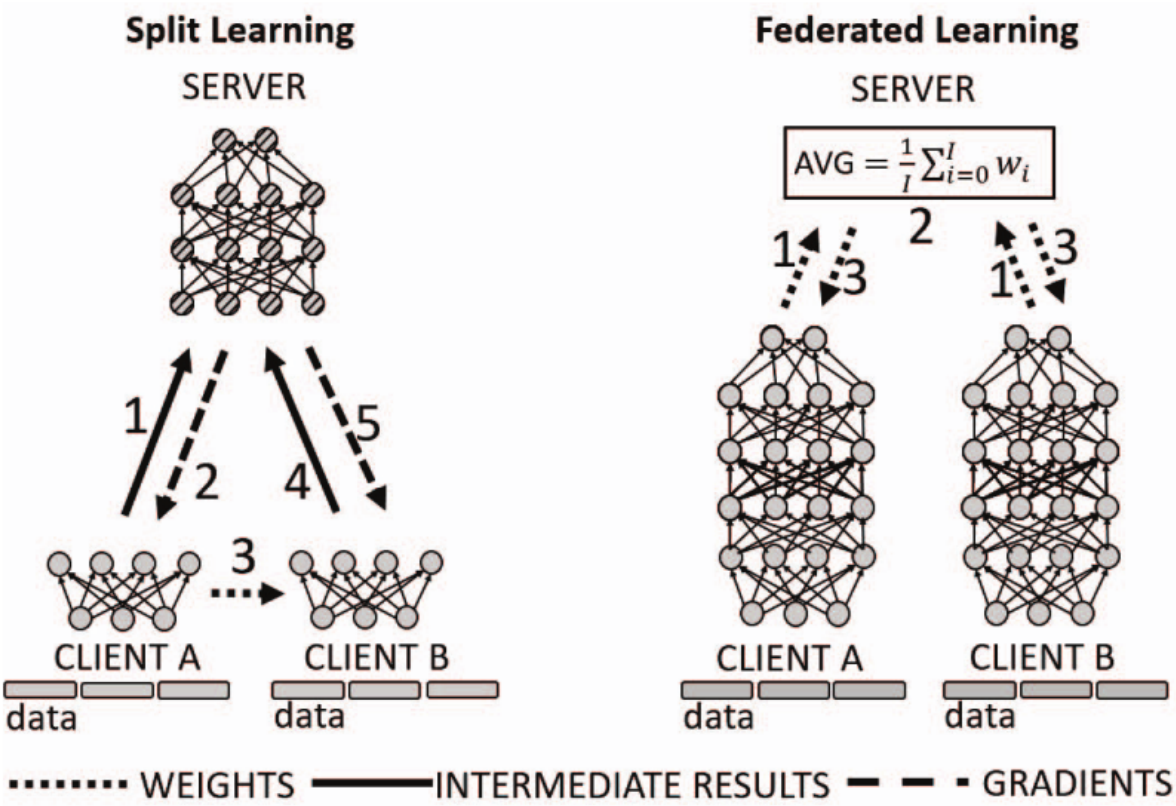
主要贡献:

(1)提出了一种新的分布式机器学习体系结构，称为联邦分裂学习，相对于目前的解决方案，它在效率和隐私方面具有优势。
(2)提出了一种通用的基于客户端的隐私方法作为对抗机器学习逆向工程攻击的对策。
(3)使用模拟和原型来评估混合学习架构。

分裂学习：

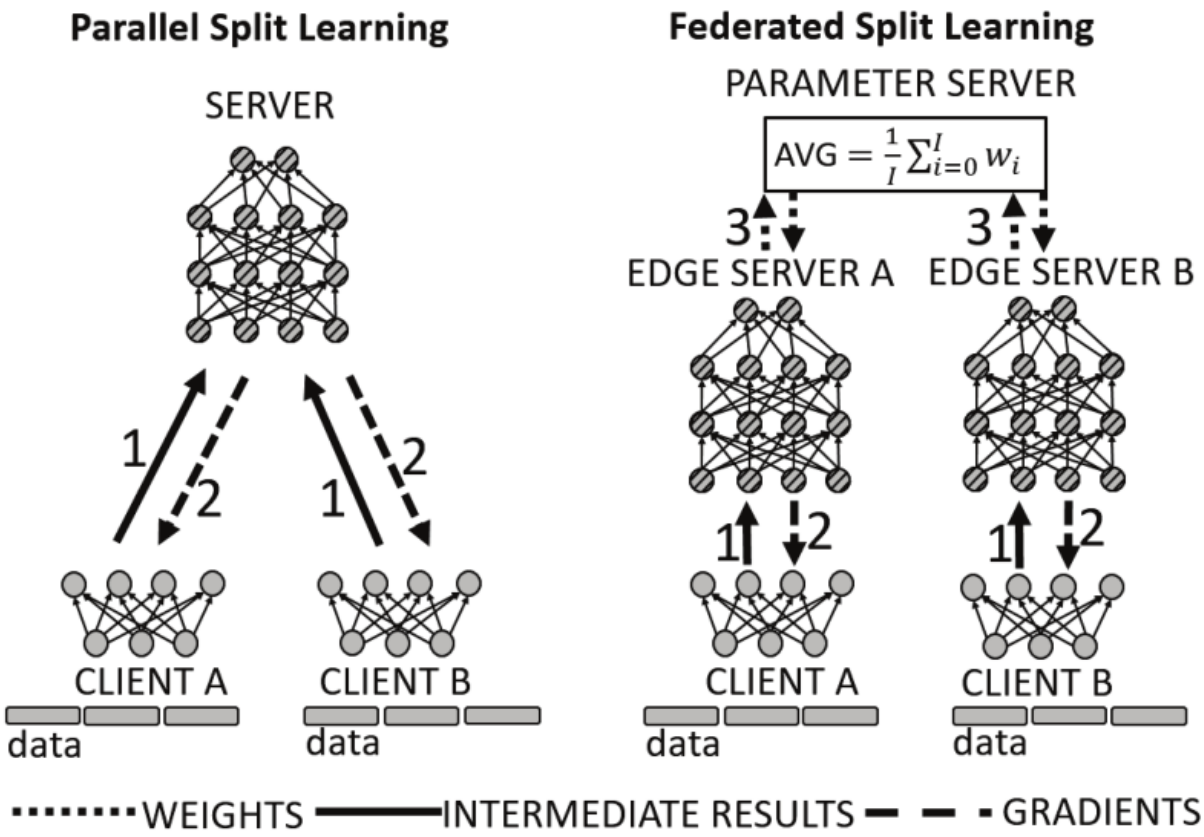
在分裂学习体系结构中，深度神经网络被划分为两个(或多个)部分。每个客户端运行深度神经网络模型的第一个分区(几层)，而第二个分区运行在单个服务器上。
在训练阶段，第一个客户端以所谓的向前传播的方式将中间数据发送到服务器;在梯度下降算法过程中，服务器在相应的向后传播中将梯度值发送回客户

主要缺点：
(1)训练过程是连续的，这会导致效率低下和计算资源的利用不足。
(2)如果每个Client中的数据集具有不平衡的特征(即非iid)，则该模型可能不会收敛到一个精确的模型。



联邦分离学习(FSL)

体系结构中包含三种类型的节点:客户机、边缘服务器和参数服务器。
FSL使用一个逻辑上集中的服务器。在FSL中，深度神经网络逻辑上被划分为两个分区。包含学习模型输入层的第一个分区被发送到客户机，而第二个分区在(边缘)服务器中运行。



联邦分离学习：

(1)对于每一对客户和边缘服务器进程，在客户端内部开始向前传播;客户端发送中间数据，即激活结果到相应的边缘服务器；边缘服务器继续向前传播阶段。

(2)边缘服务器获得输出后，计算损失函数的值，并开始向后传播。

(3)当梯度的计算到达中间数据时，梯度从边缘服务器发送到客户机。

(4)最后，隐私无关的FSL算法用这些梯度在客户机中终止向后传播。当所有对完成对其数据批次的处理后，边缘服务器中的权重在参数服务器中取平均值，然后发送回每个边缘服务器。

FSL架构，多对客户端和边缘服务器可以同时运行训练或推理过程。每个边缘服务器只需要与它的客户端一起工作，解耦对其他客户端的性能依赖关系。

基于DC的客户端隐私方法和基于DP的客户端隐私方法

计算两个不同的损失函数。第一个是隐私感知(如DC和差分隐私)，只在客户端中运行。第二个全局丢失函数在服务器上计算，并在训练过程中在客户机和服务器之间传播。在服务器中计算的交叉熵和在客户端中计算的距离相关性。通过增加两个丢失函数重新计算的频率，可以增加隐私性，增加中间结果与原始数据之间的距离(事实上是在训练过程中添加了噪声)。距离相关解决了一个优化问题，使原始训练数据和中间结果之间的差异最大化。

结论：

在本文中，我们设计了一种混合的联邦分离学习体系结构，它可以在限制缺陷的同时，充分发挥两者的优势。我们广泛地评估了我们提出的架构，并通过模拟进行了权衡分析，并在基于gpu的云上评估了原型。特别的是，我们评估了联邦分离学习的学习准确性、延迟、内存性能和隐私保证，并将其与最近提出的一种名为平行分离学习的混合架构进行了比较。

结果显示了我们的方案在延迟和内存利用率方面是如何更高效的。并得出结论，在我们的基于客户端的隐私方法下，距离相关损失函数实现了更好的隐私。