附件 4：

编号：_____

中国地质大学（武汉）

大学生自主创新启航项目申报书

项目名称：基于有向无环图的可遗忘联邦学习

负 责 人：储添翼

所在院系：计算机学院 （签章）

联系电话：15377623625

指导老师：宋军 杨帆

申请日期：2022 年 2 月 16 日

共青团中国地质大学（武汉）委员会

2022 年制

一、 简 表

<table>
<tr><td rowspan="5">研究项目</td><td>项目名称
（限 26 汉字）</td><td colspan="4">基于有向无环图的可遗忘联邦学习</td></tr>
<tr><td>学科名称</td><td colspan="2">科技发明制作类</td><td>研究类别</td><td>应用</td></tr>
<tr><td>申请金额</td><td>2 万元</td><td>起止年月</td><td colspan="2">2022 年 2 月至 2024 年 2 月</td></tr>
<tr><td>本项目获得其他资助情况</td><td colspan="4">无</td></tr>
<tr><td rowspan="3">负责人</td><td>姓名</td><td>储添翼</td><td>专业</td><td colspan="2">地质学（国家理科基地班）</td></tr>
<tr><td>性别</td><td>男</td><td>学号</td><td colspan="2">20191002188</td></tr>
<tr><td>QQ</td><td>3265687871</td><td>联系方式</td><td colspan="2">15377623625</td></tr>
<tr><td>摘要</td><td colspan="5">本项目旨在构建一种基于有向无环图（DAG）的去中心化联邦学习系统，以实现隐式模型个性化以及隐私数据自主化。
传统的联邦学习允许一组分布式客户端在私有数据上训练通用的机器学习模型，模型更新交换由中央实体或以分散的方式管理。然而，所有客户端的强大通用性使得这些方法不适用于非独立同分布数据，使得模型在去中心化与个性化之间不能平衡统一；并且客户端在更新交换模型后的数据难以撤销和删除，从而带来更多的隐私泄露问题。
通过本系统，客户端不需要训练单一的全局模型，而是专注于本地数据训练个性化模型，因此比集中或基于区块链的联邦学习更好地覆盖非独立同分布数据，从而在去中心化与个性化之间取得平衡。并穿插使用了 Machine Unlearning 技术，通过构建深度神经网络，使得客户端在提出数据遗忘请求时能够在达到删除隐私数据目的的同时大幅减少计算开销。
通过在 FMNIST、CIFAR-100 以及 Poets 数据集中进行大量实验，我们的工作已获得较理想的实验结果，达到了同类研究的先进水平。</td></tr>
<tr><td colspan="2">**关 键 词**（用分号分开，最多 5 个）</td><td colspan="4">联邦学习；共识机制；DAG；个性化；机器遗忘学习</td></tr>
</table>

二、指导老师及团队合作者信息

指导老师	**姓名**	宋军	**所在学院**	计算机学院
	职称	教授	**联系方式**	15071059090
	邮箱	songjuncug@hotmail.com		
指导老师	**姓名**	杨帆	**所在学院**	计算机学院
	职称	副教授	**联系方式**	13886091949
	邮箱	fanyang@cug.edu.cn		

	姓名	**学院**	**年级**	**专业**	**联系方式**
合作者	张慕翔	计算机学院	大三	大数据	13733066634
	刘正鹏	计算机学院	大三	信息安全	15327243600
	叶继伟	计算机学院	大三	计算机科学	18162696950

三、立项依据与研究内容

立项依据

(1)背景和意义

随着隐私信息受重视程度不断提高，联邦学习作为一种多方参与并且保障信息安全和保护数据隐私的机器学习方法被提出。本项目对联邦学习进行研究和改进，提高了联邦学习的个性化程度，在保护用户隐私的前提下更好地服务用户。

(2)挑战

1、非独立同分布数据问题：现有的机器学习任务默认训练数据遵循独立同分布。但在真实世界中数据大多遵循非独立同分布（Non-IID）。使用 Non-IID 数据训练会出现意想不到的负面效果，比如模型准确度低、模型无法收敛等。

2、通信开销问题：实际应用中，客户端往往在可用的通信带宽和允许的能源使用方面受到限制。

3、数据泄露问题：由于训练出的模型与训练数据一定具有相关性，且可以通过一定的方法从模型中反推出训练数据，联邦学习中，节点能够不断的看到每一轮迭代的参数，从而造成隐私泄露问题的加剧。

(3)研究现状及发展趋势

目前，针对使用非独立同分布数据进行联邦学习的研究尚处于起步阶段[1]。已经提出的一种解决方法是提出新的联邦聚合算法，提高模型收敛的速度，但是存在精度下降的情况，并且实验使用的数据集较简单[2]。针对通信开销问题，目前的研究方向主要是将现有的一些压缩通信方案从集中式业务流程简化设置转换为完全去中心化的设置[3] [4]，或者设计去中心化优化算法。针对联邦学习中的数据泄露问题，寻求更有效的对抗攻击的方法。

(4)本项目解决方法

本项目是在 DAG 的联邦学习的基础上，采用机器遗忘学习的技术，提高用户对于自己的数据的自治程度，解决针对非独立同分布数据的模型训练的收敛速度问题以及用户个性化问题。

【参考文献】

[1] Y. Chen, Y. Ning, M. Slawski and H. Rangwala, "Asynchronous Online Federated Learning for Edge Devices with Non-IID Data," 2020 IEEE International Conference on Big Data (Big Data), 2020

[2] J. Xiao, C. Du, Z. Duan and W. Guo, "A Novel Server-side Aggregation Strategy for Federated Learning in Non-IID situations," 2021 20th International Symposium on Parallel and Distributed Computing (ISPDC), 2021

[3] Mihaela Ion, Ben Kreuter, Ahmet Erhan Nergiz, Sarvar Patel, Mariana Raykova, Shobhit Saxena, Karn Seth, David Shanahan, and Moti Yung. On deploying secure computing commercially: Private intersection-sum protocols and their business applications. IACR Cryptology ePrint Archive, 2019:723, 2019.

[4] J. Xu, W. Du, Y. Jin, W. He and R. Cheng, "Ternary Compression for Communication-Efficient Federated Learning,"IEEE, 2020

研究内容、研究目标,以及拟解决的关键科学问题

(1)项目研究内容

针对拟解决的两个关键科学问题，本项目主要研究了基于 DAG 的共识机制、Ray 与 SISA 高效框架以及优化随机漫步等技术，旨在构建一种基于 DAG 的隐式模型个性化、隐私数据自主化的去中心化联邦学习系统。

1、基于 DAG 的共识机制

为了高效灵活得达到共识目标，提高系统吞吐量，我们准备采用基于 DAG 的改进方案来实现共识机制。通过 DAG 有向无环图结合 Popov 的方法，以使其适应具有隐式专门化的去中心化学习用例，可以使整个系统具有更好的可伸缩性以及在模型通信中更高的灵活性。

2、Ray 与 SISA 高效框架

为了提高模型在本地个性化训练的效能，我们准备适当得使用 Ray 高性能分布式执行框架与 DAG 进行结合来更高效得并行处理数据。为了减小遗忘请求的计算开销，我们引入了 SISA 框架。当需要进行遗忘请求时，只需重新训练受影响的部分，从而减少不必要的重训练时间。

3、优化随机游走

为分隔保护各小型集群，我们准备使用 Louvain 算法来获得集群聚类。通过调整相应参数来控制 DAG 的有偏向的随机游走，以便在大多数情况下，客户端只批准来自同一集群的其他客户端的交易，从而提高批准纯度。随着时间的推移，聚类之间的模型差异应该会变得更加明显，误分类分数也会不断降低。

(2)项目研究目标

本项目旨在构建一种基于 DAG 的隐式模型个性化、隐私数据自主化的去中心化联邦学习系统。针对传统联邦学习面临的问题和挑战，本系统将提供一种高效可扩展的分布式解决方案，以达到在实际情况中更适用于非独立同分布数据、统一平衡个性化模型到本地数据、自由响应用户的隐私数据撤销请求等目标。

(3)拟解决的关键科学问题

1、共识机制问题

由于去中心化系统需要不断接受大量广泛的资源和设备，因此需要高效的共识机制来进行审核批准，从而达到更高的吞吐量。但是传统的分散共识方案更多的是基于区块链，而线性区块链存在可扩展限制，且会导致网络拥塞问题。

2、中毒及攻击问题

尽管客户端以匿名的方式参与模型更新，但通过聚类后的小型集群增加了反匿名攻击的可能性。此外，如果知道集群中某个客户端的特征，就可能推断出同一集群的其他客户端的私有数据分布特征。而且一旦一个集群中毒，可能导致集群内的共识被恶意节点接管或者恶意客户端的批准间接影响到其他集群。

拟采取的研究方案及可行性分析

(1)拟采取的研究方案与技术路线

1、联邦学习的核心目标就是为所有参与者共同训练出一个单一的模型，但是对于非独立同分布的数据来说，这种单一的模型并不理想。

2、联邦学习中的一个关键问题就是通信开销，也就是快速收敛的主要障碍，于是，我们的研究采用了基于 DAG 的通信进行分布式的联邦学习，更新后的模型权重在此 DAG 中作为节点发布，而边表示当前模型对先前模型的批准。

3、此外，我们还将引入 Machine Unlearning 的概念，以基于 DAG 的联邦学习为基础，用户或系统能够让训练好的模型遗忘掉特定数据训练参数，从而保护模型中隐含数据。

4、机器遗忘学习的主要方法是将训练集分为 shards，针对 shards 分为 slices，对每个 slice 训练后记录模型参数，每个数据点被划分到不同的 shards 和 slices 中，发出遗忘请求后，排除掉对应数据点，然后 retrain 对应的 shard 和 slices，以空间开销换取训练的时间开销。

5、我们使用三个具有不同特征的数据集来反映我们的方法在不同场景中的效果。①FMNIST-Clustered 数据集。②Poets：是 Shakespeare 数据集的扩展。③CIFAR-100：包括不同动物、物体或风景的 32x32 像素 RGB 图像。

(2)方案的可行性分析

本方案是在阅读大量相关文献的基础上，进行深入的分析总结后提出的联邦学习解决方案，即在完全去中心化的联邦学习中结合了个性化和遗忘学习的方法。在基于 DAG 的分布式联邦学习中，应对诸如投毒攻击等，现有的系统难以将恶意节点的完全排除，同时用户也无法要求系统遗忘掉他（她）的偏好，于是我们采用了机器遗忘学习的方法；基于 DAG 通信的灵活性还能为机器遗忘学习的实现创造很大的便利，减小计算开销的同时也能够有效减小模型性能降低的程度。

本项目的特色与创新之处

（1）在通信方式上，针对联邦学习中通信开销过大的问题，采用基于 DAG 的模型更新通信，与此同时，与区块链类似，通过 DAG 在分布式系统中创建共识，且基于 DAG 的分布式账本允许添加多个并发块，达到提高系统吞吐量的目的，以应对大型联邦学习场景下高并发的问题。

（2）共识机制方面，由于联邦学习中数据非独立同分布（Non-IID）的特点，我们采用节点提交操作权重作为模型更新的方式以防止其他节点发布其训练结果，因为最终模型没有改进。鉴于攻击者只能以有限的速率发布恶意更新，他们必须在攻击效应和其节点在有偏向的随机游走中被其他用户选择的概率之间做出妥协，从而有效的限制了其影响，以提高系统的鲁棒性。

（3）安全方面，为了保护用户的隐私，诸如欧盟的 GDPR，美国的 California Consumer Privacy Act，还有加拿大的 PIPEDA 等法案都要求用户拥有删除自身数据的权利。我们创新性的将遗忘学习引入联邦学习中，使得用户能够向系统提交数据遗忘的请求，实现遗忘之后的模型和不用这个数据点训练的模型有一样的状态效果。与此同时，系统也可以凭借遗忘学习“遗忘”恶意节点所产生的负面影响，提高系统的鲁棒性。

年度研究计划及预期研究结果

年度研究计划：2022.2-2024.2

2022.2-2022.6

（1）查找并仔细阅读大量与研究课题相关文献，学习涉及到的理论知识和关键技术，研究如何系统得构建联邦学习框架。

（2）研究机器遗忘学习和基于 DAG 的联邦学习，研究如何制定高鲁棒性，高效的联邦学习方案和如何检测和处理中毒模型，并搜集相关数据集用于模型训练。

2022.7-2023.3

（1）按照架构要求对待用数据集进行预处理操作。

（2）研究 python 项目开发环境配置，并下载相关库函数。

（3）利用机器学习搭建用于分布式机器学习的网络，对模型进行初步调试。

2023.4-2023.9

（1）进一步调试模型，采用合理的训练策略和评估方法，全面测试所构联邦学习系统的性能。

（2）基于前期的研究，将系统功能进行集成。

2023.10-2024.2

（1）对前期设计的系统进行测试实验，验证系统功能并不断完善系统性能。

（2）进行项目总结，评价和验收。

预期研究结果：

对非独立同分布数据的学习方法能够提高联邦学习的广泛性和普适性，使用 DAG 可以过滤掉降低训练结果的模型，并对每个模型特征化，机器遗忘学习使模型聚合拥有回溯的能力，并且指定模型是否参与聚合具有不可区分性，可以抵御恶意模型的投毒攻击，具有较强的鲁棒性。预期在信安大赛以及挑战杯中取得优异的成绩，且申请相应专利。

四、研究基础与工作条件

工作基础

(1)研究工作积累

1、团队成员积极向上，成绩优异，具有良好的创新意识和团结精神。团队成员基础良好，精通 C++/python/Java 等编程语言，同时具有优秀的个人素质。团队的实践能力强，曾合作在微众银行举办的 Fisco-Bcos 编程大赛中斩获十强的席位。

2、团队成员自学能力强，善于从多方渠道获取相关知识。各成员分别查找联邦学习、Non-IID 等方面的相关文献并取得一定成果，团队在相关方面有所了解并有所思考。

3、团队成员查阅大量联邦学习相关的论文，对联邦学习存在的问题以及最新的解决方法有了一定的认识和了解。团队成员也同研究联邦学习的学者和相关团队进行交流，合法申请数据集和交流模型训练中遇到的问题。

(2)研究工作成绩

1、当前本项目对 DAG、联邦学习和机器遗忘等开展了研究。使用 DAG 构建联邦学习框架，提高模型的个性化，解决了非独立同分布数据的训练问题，加快了模型的收敛速度，同时模型的精度不会降低。

2、在本项目中拟采用 Machine Unlearning 技术，使得客户端在提出数据遗忘请求时能够在达到删除隐私数据目的的同时大幅减小计算开销，解决了联邦学习中由于梯度更新导致的数据泄露的问题。

工作条件
(1)已具备的实验条件： 1、团队成员均拥有笔记本，可以达到中小型的模型训练和测试的要求。 2、指导老师具有丰富的指导经验，曾带领多个队伍获得全国级大赛的各种奖项（如：全国信息安全大赛一等奖四项）。 3、团队成员学习的知识有助于项目的研究，同时团队成员常在实验室，交流学习更加方便，有利于项目的深入开展。 4、团队负责人有较强的组织管理能力以及统筹规划能力，对工作认真负责；团队成员积极上进，互相勉励，互相督促，在保证专业学习质量的情况下进行学习研究，具有较好的学科基础以及较强的学习能力和自我管理能力。 **(2)尚缺少的实验条件：** 1、由于笔记本性能欠佳以及数据集规模过大，在模型训练时会出现运行花费时间长或者无法运行的情况，对项目开展带来了一定的阻碍。 2、团队需要租用可用于运行大型分布式机器学习程序的服务器。 3、团队缺少用于进行实验所需的部分硬件设备。 **(3)拟解决的途径：** 1、根据团队成员的课表合理安排工作时间以及定期进行小组讨论，汇报工作进度，进行工作规划。 2、向学校申请配置专用的办公电脑、服务器。 3、在处理大型数据集时，合理安排四台笔记本电脑分工进行预处理，利用有限的资源不断推进工作。

五、经费预算

项目总经费	20,000 元	
申请基金经费	10,000 元	
学院匹配经费	10,000 元	
支 出 科 目	金 额（元）	计 算 根 据 及 理 由

合　计	20,000	
1. 设备费	9,000	需要租借阿里云 GPU 服务器、购买显卡等硬件设备
2. 材料费	2,000	打印相关材料以及相关书籍资料的购买
3. 测试化验加工费	1,000	项目后期需要进行大规模的测试
4. 差旅费（≤20%）	4,000	项目研发及测试阶段需要进行现场测试时，产生的交通费、住宿费等
5. 会议费（≤10%）	500	研究期内需要参加一些相关会议以及相关的报名费用
6. 专家咨询费（≤10%）	500	项目研发阶段小组成员需要向相关的专家咨询，促进项目往更好更深的方向发展
7. 出版／文献／信息传播／知识产权事务费	3,000	研发以及测试阶段需要购买相应付费软件以及文献资料

说明：

1. 设备费。不得购置大型仪器设备。

2. 材料费。是指在项目研究过程中发生的各种原材料、辅助材料的消耗费用。

3. 测试化验加工费。是指在项目研究过程中发生的检验、测试、化验及加工等费用。

4. 差旅费。是指在项目研究过程中开展科学实验(试验)、科学考察、业务调研、学术交流等所发生的外埠差旅费及(含出差补助)、市内交通费。

5. 会议费。是指在项目研究过程中为组织学术研讨、咨询以及协调等活动而发生的会议费用。

6. 专家咨询费。是指在项目研究过程中支付给临时聘请的咨询专家进行学术指导所发生的费用。

7. 出版／文献／信息传播／知识产权事务费。是指在项目研究过程中发生的论文论著出版、文献资料检索与购置、专用软件购置、专利申请与保护的费用。

六、项目审批

指导老师意见	指导老师签字： 年　　月　　日
学院推荐意见	分管院领导签字： （签章） 年　　月　　日
学校意见	（签章） 年　　月　　日

注：本申请书一式两份。