计算机科学与技术学院

**毕业设计（论文）开题报告**

题 目：基于多方安全计算的联邦学习系统设计与实现

姓 名：汤明伟

学 号：1904010717

班 级：计算机19-7班

专 业：计算机科学与技术

指导教师：朱素霞

2022 年 12 月 30 日

**说 明**

1. 正文包括课题研究背景及意义、国内外在该方向的研究现状及分析（文献综述）、研究方案、论文进度计划、参考文献等部分。
2. 研究背景及意义和文献综述部分不少于3000字，报告总体为5000字左右。
3. 参考文献不少于10篇（其中英文文献至少3篇），要有近三年的文献，必须包含学术研究论文，不可全部为图书类文献，文献要在正文中引用。
4. 完成论文的截止日期为毕业学期的6月10日，可按此日期安排论文进度。
5. 正文为小四号字，中文用宋体，英文和数字用Times new roman。
6. 1.5倍行距。
7. 用A4纸双面打印。

# 目录

[目录 3](#_Toc20828)

[1 课题研究背景及意义 4](#_Toc18269)

[1.1 课题来源（问题提出） 4](#_Toc17433)

[1.2 选题目的及意义 4](#_Toc26072)

[2 国内外研究现状及分析（文献综述） 6](#_Toc23605)

[2.1 联邦学习国内外研究现状 6](#_Toc15361)

[2.2 未来联邦学习研究趋势分析 8](#_Toc4836)

[3.3总结 9](#_Toc11925)

[3 论文研究内容 9](#_Toc12513)

[3.1 研究目标、系统组成和功能、拟解决的关键问题 9](#_Toc18063)

[3.2 拟采取的研究方法、技术路线、实验方案（含工具、环境）及可行性分析 11](#_Toc6594)

[4 论文进度计划 12](#_Toc26025)

[参考文献 13](#_Toc27364)

# 1 课题研究背景及意义

## 1.1 课题来源（问题提出）

十四五规划中明确提出“发展数字经济，推进数字产业化和产业数字化，推动数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群”。党的十九届五中全会进一步提出推动数据资源开发利用，推进数据等要素市场化改革，这为加快培育发展数据要素市场指明了方向。在数字经济浪潮下，政府和企业需要在保障国家、公民数据安全、落实数据保护措施的基础上，推动各产业、各部门、各区域之间的数据共享流动，让大数据更好造福人民、促进经济发展。

但当前数据产业仍然面临众多挑战，其中最突出的是数据安全和隐私合规问题。近些年数据安全事件的新闻依旧层出不穷，背后是各类原因造成的数据泄漏，数据一旦泄漏极难回收，治理周期长、难度大。

另外，随着《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》相继实施，对数据安全保护要求、个人隐私数据合规使用提出了明确的监管要求。企业间数据孤岛效应明显，机构之间的数据无法互通，少数巨头公司垄断大量数据，小公司很难获得数据，形成大大小小的“数据孤岛”。对于很多企业，部门不会把数据与其他部门做简单的聚合，导致同一个公司内数据也往往以孤岛形式出现，从而限制企业的创新能力和运营效率。而传统的数据明文直接流通共享，已经行不通，数据要素的应用必须像金融、房地产一样需要被监管。为此，需要一种可管、可控、可用的数据流通新方式。

## 1.2 选题目的及意义

越来越多的需求让大家把目光放到了隐私计算上，让隐私计算成为数据要素市场化的关键技术。

隐私计算是一系列技术体系的合集，交叉融合了密码学、统计学、人工智能、计算机硬件等众多学科类别，它能够满足在不暴露原始数据的前提下，对数据进行加工、分析、处理、验证等，实现数据及其价值可管、可控和可计量的融合、共享、流通、计算。

其核心优势是分离数据所有权、控制权和使用权。隐私计算可把“数据可见的信息部分”和“无需看见就可计算的使用价值”分开，实现“数据可用不可见”、“数据不动价值动”，数据流通主体可以不再是明文数据本身，而是数据特定使用价值，甚至可通过计算合约把数据使用价值精确限制到具体的用途和使用次数，实现数据“使用可控可计量”。在基层平安法治数字治理中，隐私计算、区块链等新兴技术的融合应用在保护数据信息安全的同时，打破了信息“孤岛”和“藩篱”，整合了政府部门之间、政府和社会之间以及各社会主体之间的数据资源，有助于促进基层平安法治数据跨域进行安全计算、联合统计、联合建模，进而挖掘数据融合共享价值，对于实现政务数据可控使用、推动政务数据开放、提升政府数字治理能力具有重要意义。

在此背景下联邦学习（FL, federated learning）应运而生，其允许用户将包含个人隐私信息、组织机密信息、公司内部资料等数据留在本地进行模型训练，在云端聚合全局模型，但即便如此在交互过程中仍有隐私信息泄漏的风险，一旦数据泄露，将会使用户、组织或者公司遭受重大的损失。由于人们对隐私数据可能遭到泄漏感到担忧，相关法律法规[1]明确禁止收集和利用未授权的敏感数据。尽管在数据共享的同时满足用户敏感信息的隐私保护存在一定的困难，但由于最先进的机器学习模型需要大量的数据参与训练，不同组织或者公司对数据共享需求仍然很强烈。因此，如何让不同的数据持有者在联邦学习场景下保证用户隐私不被泄漏是构建一个高质量的机器学习模型所面临的巨大挑战。

为了保证模型训练中用户敏感数据的隐私性和训练过程的安全性，通常采用三种核心的隐私保护技术，即安全多方计算(SMC, secure multi-party computation)[2]、差分隐私(DP, differential privacy)[3]和同态加密(HE, homomorphic encryption)[4]。

其中联邦学习作为一种新兴的分布式计算范式，其使得用户原始数据在不输出本地设备的基础上可以找到一个更优化的模型，做到“数据不动模型动”，在保证用户数据隐私安全的前提下，打破数据孤岛，充分挖掘数据的潜在价值。联邦学习包括横向联邦学习、纵向联邦学习与混合联邦学习.

横向联邦学习也称为按样本划分的联邦学习（Sample-Partitioned Federated Learning或Example-Partitioned Federated Learning）[5]，可以应用于联邦学习的各个参与方的数据集有相同的特征空间和不同的样本空间的场景，类似于在表格视图中对数据进行水平划分的情况。事实上，“横向”一词来源于术语“横向划分（horizontal partition）”。“横向划分”广泛用于传统的以表格形式展示数据库记录内容的场景，例如表格中的记录按照行被横向划分为不同的组，且每行都包含完整的数据特征。举例来说，两个地区的城市商业银行可能在各自的地区拥有非常不同的客户群体，所以他们的客户交集非常小，他们的数据集有不同的样本ID。然而，他们的业务模型非常相似，因此他们的数据集的特征空间是相同的。这两家银行可以联合起来进行横向联邦学习以构建更好的风控模型。

纵向联邦学习：不同参与方的数据样本有较大的重叠，但样本特征的重叠度不高。例如，两家公司（银行和电子商务公司）向客户提供不同的服务，拥有客户不同方面的数据，但他们所服务的客户群体有较大的重叠。

横向联邦学习和纵向联邦学习要求所有的参与方具有相同的特征空间或样本空间，从而建立起一个有效的共享机器学习模型。然而，在更多的实际情况下，各个参与方所拥有的数据集可能存在高度的差异：

·参与方的数据集之间可能只有少量的重叠样本和特征。

·这些数据集的分布情况可能差别很大。

·这些数据集的规模可能差异巨大。

·某些参与方可能只有数据，没有或只有很少的标注数据。

为了解决这些问题，联邦学习可以结合迁移学习技术，使其可以应用于更广的业务范围，同时可以帮助只有少量数据（较少重叠的样本和特征）和弱监督（较少标记）的应用建立有效且精确的机器学习模型，并且遵守数据隐私和安全条例的规定[6]。我们将这种组合称为联邦迁移学习，它可以处理超出现有横向联邦学习和纵向联邦学习能力范围的问题。

# 2 国内外研究现状及分析（文献综述）

## 2.1 联邦学习国内外研究现状

文献[7]中率先提出了联邦学习的概念。其主要是用来解决多个终端数据进行中心化模型训练的问题，并将该训练思想应用于移动手机输入法改进场景[8]。手机终端设备通过下载初始化模型，利用本地数据训练，将模型参数加密上传至云端服务器，与其他用户数据融合，以此对共享模型进行改进，该过程不断重复直至达到预设精准度结束，最后用户下载全局模型到本地，完成一次训练。但是在此思想提出后的一段时间，联邦学习处于理论研究的状态，并没有太多的实际应用案例。尤其是 AI中传统数据处理模型通常是一方收集数据，另一方负责清理和融合，最后第三方将获取集成数据并建立模型供其他方使用。然而数据的多方流转，面临着严重的隐私泄漏问题。针对这些挑战，香港科技大学杨强联合微众银行提出了可能的解决方案:安全联合学习[2]。根据数据特征将联邦学习划分为横向联邦学习、纵向联邦学习和迁移学习。在此提供了联邦学习框架、系统结构和应用程序，以及关于该主题的全面调查。此外提出建议在组织之间建立基于联邦机制的数据网络，实现知识共享又不损害用户隐私。基于此模型，再次掀起了研究热潮。目前联邦学习研究主要是集中以下几个方面:

1. 通信开销。在联邦学习中，原始数据需要保存在客户端的本地，通过与中央服务器的频繁数据交互，完成模型的训练。通常情况下，联邦学习中会包含大量的终端设备，结合目前落地的实例，在实际的使用情况下更多的是类似移动终端设备，其网络通信的速度和质量不高，因此也成为了联邦学习模型训练的瓶颈。为了解决上述问题，Luping Wang 等人提出了CMFL模型[9]，为客户端提供了全局模型更新趋势的反馈信息。每个客户端检查它的更新是否符合该全局模型，是否与模型的改进足够相关，进而避免不相关更新上传至服务器，间接降低通信开销。Keith Bonawitz 等人[10]提出了面向大规模联合系统设计。在给定的 FL 轮数的报告阶段可选择启动四轮交互协议。但是存在单独的训练实体不可直接检查的问题，需要工具在测试和仿真中处理代理数据，而且模型之间不能直接交互运行，必须编译成 FL 计划，通过 FL 服务器部署;所有模型资源消耗和运行兼容性必须由基础设施自动验证。因此这种方法虽然限制了通信轮数，但是其局限性很大。
2. 隐私保护问题。基于联邦学习数据隐私保护，目前的技术除了针对具体机器学习模型实现隐私保护[18.20,72-4]外，还提出新的训练平台。例如，在横向联邦学习环境下[11]，文献[12]在联邦平均算法中添加了同态加密机制，但是密文传输加大了计算和通信开销，尤其在评估非线性函数使用多项式近似，对精度有很大的影响。朱强等[13人提出在 Mlaas 平台上安全训练机器学习模型，在此借助Paillier 加密算法，将本地数据加密上传，密文在神经网络模型下处理，但是由于数据离开参与方本身，虽然采用了加密训练模型，但是还是会出现间接的数据泄露问题。Ye等人[14]提出三元组梯度，其分析 TemGrad 隐私保护缺陷提出了解决方法EaSTFly[15]。在 EaSTFly 上结合秘密共享和同态加密来抵抗半诚实性攻击。但是该方案增加了客户端的计算量，需要客户端对梯度进行三元量化并进行批量编码最后上传结果。Yu 等人[16]提出在可信平台 TEE 环境下设计完整的联邦学习训练协议[17],参与方通过可信平台提交参数信息。但是目前可信计算的研究在实际的使用中还是存在一定的局限性。

(3) 安全威胁。目前机器学习在训练过程中面临着多种攻击威胁，对于模型反演攻击，Matt 等人[18]提出采用对返回值进行四舍五入处理，降低模型反演攻击的成功率。Chang 等人[19]提出在结果输出时，返回类别标签，在聚合多个测试样本的预测标签结果后，对结果混淆，进一步加强对模型的保护。对于投毒攻击，Matthew 等人[20]提出 TRIM 算法在不同的对抗模型上考虑了中毒的线性回归问题从现有的中毒攻击分类中提出了优化框架，分离中毒点并学习健壮的回归模型。Steinhardt[21]在文中提出现有的防御措施是无法预测最坏情况。针对此问题，文中提出构建一个大范围的攻击损失近似上界，首先进行离群点的去除，然后将经验风险最小化。但是在联邦学习环境中第三方或中央服务器是无法得到检测数据的,因此基于该种防御模型不适合联邦学习环境。

## 2.2 未来联邦学习研究趋势分析

未来联邦学习研究趋势将更多与算法模型和安全隐私技术相关，目前联邦学习研究热点主要聚焦在机器学习方法、模型训练、隐私保护三方面。

未来几年研究趋势将更多涉及算法模型和安全隐私技术，如数据隐私、深度学习、差分隐私、边缘计算、物联网、云计算、移动设备、同态加密、优化问题、沟通效率等。

行业应用越来越成熟，应用研究方向呈现出更多与物联网、区块链[8]、车辆交互、5G/6G 等技术融合的态势。

通过新闻事件分析挖掘和搜索系统 NewsMiner 数据库，从已公开的新闻数据发现，联邦学习技术的行业应用最早出现在 2018 年，当时被应用在金融、IT 和通信领域，后来几年其应用探索逐渐扩展到智慧城市、教育、汽车等其他多个行业领域。

一．在金融业的应用

联邦学习在金融业应用目前处于框架设计、合作探索、在几个业务场景中初步试点的阶段。推进联邦学习在金融业应用落地的参与主体主要是科技公司（百度、腾讯、京东等）、互联网金融机构（微众银行、蚂蚁金服等）、少数传统商业银行（江苏银行、浦发银行、建设银行等）等。

二．在医疗业应用

联邦学习在医疗业应用目前处于研究探索、项目试点的阶段，参与主体不仅有科技公司，而且有较多的国内外权威科研机构、大学院所、医疗机构。国际性科技期刊 Nature《自然》曾发表关于联邦学习在医疗领域应用的文章，展示出联邦学习技术医疗应用的强大潜力。新冠疫情以来，通过使用联邦学习和来自各地区各医疗机构的数据来开发模型的研究意愿和实践更加强烈。

三．在电信业应用

联邦学习的最初提出就是为了解决移动设备数据训练问题，可以看作是其在电信业的最早应用。从公开的新闻数据看，联邦学习在电信业应用探索从 2018 年开始至今，应用场景从早期的通信资源分配已扩展到近期的客户体验和精准营销、6G 和卫星网络等。其中的参与主体主要是大型通信运营商、软硬件制造商等。

## 3.3总结

如今，联邦学习从技术维度上解决了人工智能发展过程中的安全问题。中国已经成为联邦学习技术的深度参与方，国内企业和科研机构积极参与联邦学习的技术研发和应用，以及标准制定。国际与国内联邦学习标准的相继出台有力促进了联邦学习生态的建立与发展。截至目前，联邦学习生态建设较成规模的有 FATE 开源社区与开放群岛开源社区。

未来，随着人工智能技术和应用的不断升级，联邦学习的技术研发和落地应用还将进一步扩大和深入。联邦学习未来市场与商业化的实际落地将出现更多的异构场景下的应用。

# 3 论文研究内容

3.1 研究目标、系统组成和功能、拟解决的关键问题

1.研究目标

使用多方安全计算算法：秘密共享、同态加密技术应用到横向联邦学习模型里，实现被选择的客户端上传本地模型进行模型聚合最后达成数据模型结果的共享。

2.系统组成和功能

系统的大致组成如图1所示：

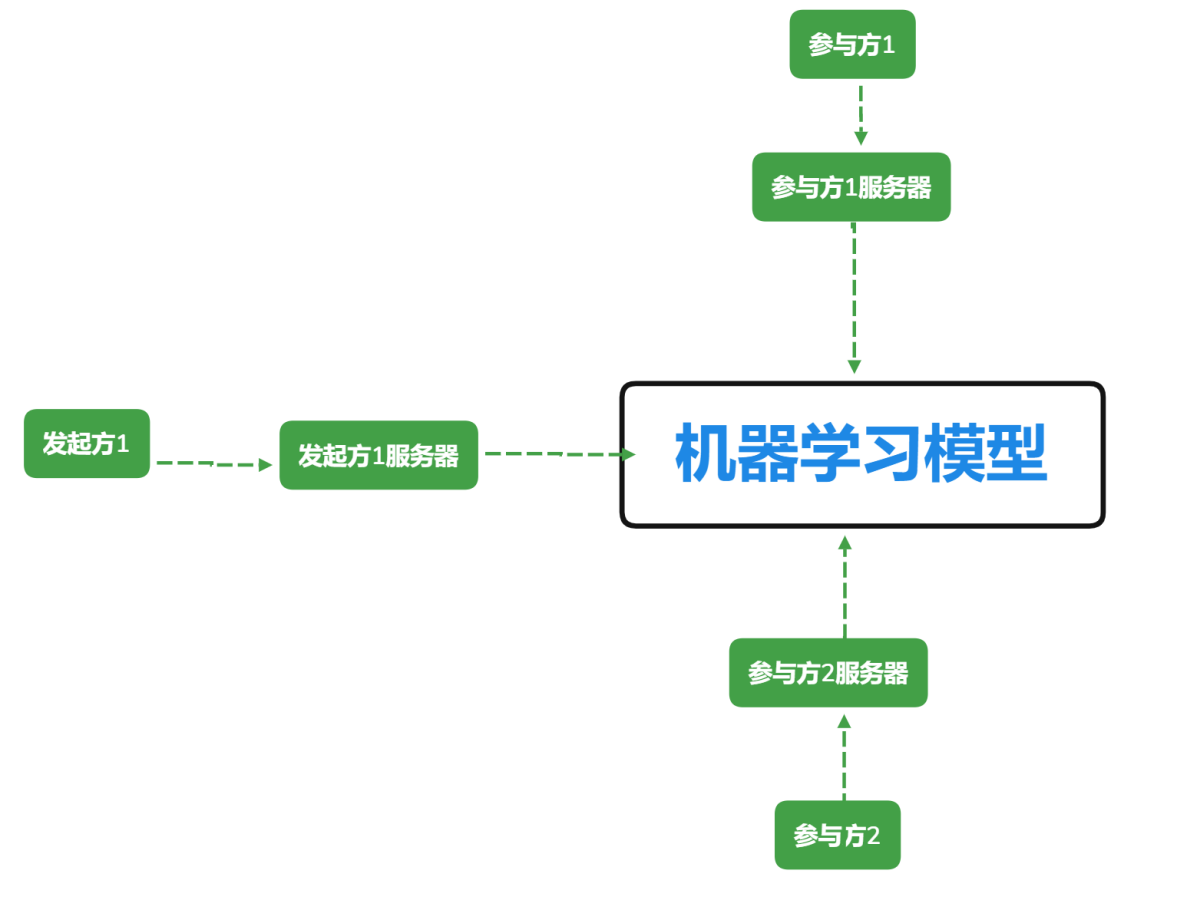


图1 系统组成结构图

客户-服务器架构也被称为主-从（master-worker）架构或者轮辐式（hub-and-spoke）架构。在这种系统中，具有同样数据结构的 K 个参与方（也叫作客户或用户）在服务器（也叫作参数服务器或者聚合服务器）的帮助下，协作地训练一个机器学习模型。横向联邦学习系统的训练过程通常由如下四步组成：

步骤1：各参与方在本地计算模型梯度，并使用同态加密、差分隐私或秘密共享等加密技术，对梯度信息进行掩饰，并将掩饰后的结果（简称为加密梯度） 发送给聚合服务器。

步骤2：服务器进行安全聚合（secure aggregation）操作，如使用基于同态加密的加权平均。

步骤3：服务器将聚合后的结果发送给各参与方。

步骤4：各参与方对收到的梯度进行解密，并使用解密后的梯度结果更新各自的模型参数。

3.拟解决的关键问题

（1）考虑数据安全性和模型准确性等问题，例如使用加密和差分隐私技术对数据进行保护，并使用模型聚合算法来避免模型震荡和过拟合。

（2）web系统的启动，解决认证阶段。

（3）软件系统进行机器学习模型和训练。

（4）软件可视化页面的设计。

（5）以使用matplot将生成的图表保存为图片或PDF等格式，以便与其他人分享或用于报告。

3.2 拟采取的研究方法、技术路线、实验方案（含工具、环境）及可行性分析

1.拟采取的研究方法和技术路线

首先横向联邦学习的服务端的主要功能是将被选择的客户端上传的本地模型进行模型聚合。并将web系统启动部分和基于多方安全计算的算法验证demo链接起来，挑选最合适的算法。然后进行数据集的测试和优化，尽可能多的覆盖到各种情况并提高识别准确率。之后设计整体软件系统，进入联邦机器学习部分的代码系统。最后实现可视化界面，方便管理员进行异常情况查看和处理。

2.实验方案（含工具、环境）

零知识证明和秘密分享进行网站的登录和认证阶段验证用户，计划采用以下方案或者更复杂的版本：

用户输入用户名和密码，然后使用密码学哈希函数对密码进行哈希处理，并使用秘密分享算法将哈希值拆分为两个或多个部分，这些部分可以在多个服务器（模拟的）之间进行共享。

对于每个处理端，使用哈希值的一部分作为密钥，使用密码学签名算法生成一对公钥和私钥。然后将公钥发布在服务器上，并将私钥保存在本地。

当用户尝试登录时，服务器将要求用户进行零知识证明，证明他们知道与其帐户关联的密码。用户使用其密码对的哈希值的部分来计算证明，证明他们知道密码。证明可以使用零知识证明协议进行验证，以确保密码不会在证明过程中泄露。如果验证成功，则将密码的哈希值部分与其他处理端共享的哈希值部分合并，以重构哈希值并验证其与存储在服务器上的哈希值相匹配。如果哈希值匹配，则用户被授权登录。

这个方案使用了秘密分享算法将密码哈希值拆分为多个部分，以确保在没有足够的部分的情况下无法重构哈希值。同时，使用零知识证明可以确保用户不需要将其密码直接传递给服务器。这可以提高安全性，因为服务器无法将密码存储在明文中或使用不安全的方式传输密码

联邦学习系统的核心是通过分布式训练多个客户端的模型，并将它们的更新聚合成一个全局模型，从而实现在不泄露用户数据的情况下进行模型训练。

使用Tensorflow、PyTorch和Numpy等深度学习框架可以实现联邦学习系统。

其中，Tensorflow和PyTorch提供了分布式训练的功能，可以将模型和数据分配到多个计算节点上进行训练，然后将结果聚合到全局模型中。

Numpy则可以通过将模型参数和梯度等信息进行序列化和传输，实现模型更新的分布式计算。

在实现联邦学习系统时，需要考虑数据安全性和模型准确性等问题，例如使用加密和差分隐私技术对数据进行保护，并使用模型聚合算法来避免模型震荡和过拟合等问题

使用pandas和matplot可视化数据初步分为以下步骤：

加载数据：首先，可以将数据缓存为pickle或json格式，以便快速加载和使用。使用pandas可以方便地读取这些数据文件，并将它们转换成DataFrame对象。

数据预处理：通过DataFrame对象，可以进行数据的清洗、转换、过滤等操作，以便更好地展现数据的特征和趋势。

数据可视化：使用matplot可以将预处理后的数据可视化，例如制作直方图、散点图、折线图等图表，并使用标签、标题、颜色等方式使其更加美观和易于理解。

保存图表：最后，可以使用matplot将生成的图表保存为图片或PDF等格式，以便与其他人分享或用于报告等场合。

综上，使用pandas和matplot的数据缓存方案可以使数据的处理和可视化更加方便和高效，并且通过将数据保存在pickle或json格式中，还可以大大减少数据加载和预处理的时间，提高数据处理的效率。

3.可行性分析

目前横向联邦学习以云计算为中心，有一到多个服务器，面对的是众多终端设备，需要一个全局的模型优化，并在这个过程当中保证数据不出本地、数据不出库、模型得到保护等；而异构联邦学习则强调当数据分布不一样的情况下，结合机器学习来实现“数据不动模型动，数据可用不可见。

而且在安全性分析方面，除了传统的正确性分析和基本的安全属性分析外，还使用加密和差分隐私技术对数据进行保护并且将数据保存在pickle或json格式中，还可以大大减少数据加载和预处理的时间，提高数据处理的效率。综上基于多方安全计算的联邦学习系统的设计与实现可行性较高。

# 4 论文进度计划

论文各环节的进度安排如表1所示。

|  |
| --- |
|  |

表1 进度计划表

|  |  |
| --- | --- |
| 时间安排 | 实施进度 |
| 2022.10.17~2022.11.30 | 了解毕业设计内容，查阅资料，熟悉开发语言，筛选目标检测算法。 |
| 2022.12.1~2022.12.31 | 搭配开发环境，学习并尝试使用目标检测算法。 |
| 2023.2.27~2023.3.20 | 测试目标检测算法在隐私计算联邦学习框架并选择最合适的算法进行多方安全认证的mock实验。 |
| 2023.3.21~2023.4.10 | 数据集的测试和优化，尽可能多的覆盖到各种情况并提高识别准确率。 |
| 2023.4.11~2023.4.30 | 设计整体软件系统，实现可视化界面管理。 |
| 2023.5.1~2023.5.20 | 修改bug。 |
| 2023.5.21~2023.6.10 | 撰写论文，准备答辩。 |

# 参考文献

[1] TEAM I G P. EU General data protection regulation (GDPR) - an implementation and compliance guide, fourth edition[M]. Cambridgeshire: IT Governance Publishing, 2020.

[2] EVANS D, KOLESNIKOV V, ROSULEK M. A pragmatic introduction to secure multi-party computation[J]. Foundations and Trends in Privacy and Security, 2018, 2(2/3): 70-246.

[3] DWORK C, ROTH A. The algorithmic foundations of differential privacy[J]. Foundations and Trends in Theoretical Computer Science, 2013, 9(3/4): 211-407.

[4] ACAR A, AKSU H, ULUAGAC A S, et al. A survey on homomorphic encryption schemes[J]. ACM Computing Surveys, 2019, 51

[5]KAIROUZ P,MCMAHAN H B,AVENT B,et al.Advances and Open Problems in Federated Learning[A/OL].arXiv.org(2019-12-10).https://arxiv.org/abs/1912.04977

[6] Konecny Y J.Mcmahan H B，Yu F Xet al. Federated learning:Strategies for improvingcommunication efficiency[J/OL].Computer Science.2018:1-10.

[7] Konecny J, Mcmaham H B, Ramage D,et al. Federated optimization: Distributed machinlearning for on-device intelligenceJ/OL1. 2016.(2016-10-081. http://arxiv.org/abs/ 1610.02527

[8]Yang O, Liu Y, Chen T, et al. Federated machine learning: Concept and applications[Jl. ACMTransactions on Intelligent Systems and Technology(TIST), 2019,10(2): 1-19.

1. Wang L, Wang W,Bo L I CMFL: Mitigating Communication Overhead for FederatedLearning(C],//2019 IEEE 39th International Conference on Distributed Computing SystemsICDCS).IEEE.2019:954-964
2. Bonawitz K. Eichner H, Grieskamp W, et al Towards Federated Learning at Scale: SystemDesign/C].// Proceedings ofthe second SysML Conference. 2019:1-15.
3. Phone L T,Aono Y, Hayashi T, et al. Privacy-preserving deep learning via additivelyhomomorphic encryptionJ]. IEEE Transactions on Information Forensics and Security, 2018.13(5): 1333-1345.
4. Mcmahan H B, Moore E, Ramage D, et al. Federated learning of deep networks using modelaveraging[J/OL].2016[2016-02-171.https://arxiv.org/abs/1602.05629.
5. 朱强，机器学习中的对抗样本防御和隐私保护D1西安电子科技大学,2019.
6. Kim M,Song Y, Wang S. et al. Secure Logistic Regression Based on Homomorphic Encryptiond Evaluation/.JMIR medical informatics.2018.6(2): e9.
7. Dong Y, Chen X,Shen L.et al. EaSTFLy: Efficient and security ternary federated learninglJ].Computers & Security.In Press.202094:101824.
8. Phan N, Wu X, Dou D.Preserving differential privacy in convolutional deep belief networksJ]Machine Learning.2017.106(9):1681-1704
9. Chen Y, Luo F, Li T, et al. A training-integrity privacy-preserving federated learning schemewith trusted execution environmentfIl Information Sciences,2020,522: 69-79.
10. Matt F, Somesh J, Thomas R. Model inversion attacks that exploit confidence information andbasic countermeasurelCl, //n Proc. of the 22nd ACM SIGSAC Conference on Computer andCommunications Security. 2015:1322-1333.on attacks against mobile-based contir
11. Alrubaie M Chane JMReconstructisystems in the cloud(J. IEEE Transactions on Information Forensics and Security, 2016, 11(12): 2648-2663.
12. Jagielski M,Oprea A, Biggio B, et al. Manipulating Machine Learning: Poisoning Attacks ancCountermeasures for Regression Learning[Jl. IEEE Symposium on Security and Privacv.201819-35.
13. Steinhardt, Jacob, Koh W, et al. Certified Defenses for Data Poisoning Attacks(C1. // Proc of th31st Annual Conf on Neural Information Processing Svstems (NeurIPS), Cambridge. MA: MITPress,2017: 3517-3529.