深圳大学研究生课程期末论文评分表

课程名称：课程的名称

论文题目：请输入论文标题（通过 hspace 控制横线长度）

学　　号：0123456789　　姓　　名：名字

指标	评分标准	分值	得分
文献	文献资料是否恰当、详实；是否具有代表性；是否有述有评。	10	
选题	选题是否新颖；是否有理论意义或实用价值；是否与授课内容相符。	10	
规范	篇幅字数在规定要求范围内；文字表达是否准确、流畅；论述是否具有论辩性；图表计量单位是否规范；是否符合学术道德规范，论文独立完成，无抄袭现象。	30	
论证	研究方案是否具有可行性；是否能较好运用所学知识，观点明确；思路是否清晰；逻辑是否严密；结构是否严谨；论证是否充分。	30	
实用价值	调研成果是否具有实际应用价值；是否提出了可行的建议或解决方案；是否对相关领域有参考意义；是否体现创新思维。	20	
其他意见（选填）			
任课教师签名： 年_____ 月_____ 日		**总分：**	

1. 该表应在期末考试前由任课教师发给学生，告知学生论文评分标准；

2. 学生应在提交期末论文时，封面附上该表并补充填写好表格基本个人信息。

深圳大学研究生课程论文学术诚信承诺书

本人在此声明所提交的课程论文 _____（论文标题）是本人独立完成的，具有原创性，并且未抄袭、剽窃他人成果或侵犯他人的知识产权。本声明书详细阐述以下内容：

1. 本人郑重声明，课程论文的所有内容和观点均源自本人的研究和分析，未从其他来源直接复制或翻译。

2. 对于其他作者或研究人员的观点、数据、图片、图表等引用和参考，本人已按照学校规定的引用标准进行准确的引用和注明，并在文中明确标明了引用部分。

3. 本人保证，课程论文中使用的所有文献、资料和其他来源均已在参考文献部分列出，且准确无误地注明了相关信息，包括作者、出版年份、出版社或期刊名称等。

4. 本人明确知晓学术不端行为的严重性，包括但不限于抄袭、剽窃、造假、篡改数据等。本人承诺，在课程论文的整个研究和撰写过程中，坚守学术道德原则，维护学术诚信。

我郑重承诺以上内容的真实性，并愿意为我所提交的课程论文的原创性负全部责任。

论文作者签名：_____ 日期：_2025_ 年_06_ 月_12_ 日

深圳大学研究生课程论文

题目 论文的题目　　成绩 _____

专业 计算机技术　　课程名称 课程名称

代　　码 11234567

年级 20xx 级　　姓名 姓名

学号 0123456789　　时间 2025 年 06 月

任课教师 教师的名字

标题模板

课程名称：XXX

课程代码：XXXXXX

指导教师（授课老师）：XXX

学院：XXX

专业：XXX

姓名：XXX

学号：XXXXXXXX

完成日期：2025 年 6 月 13 日

提交日期：XXXX 年 XX 月 XX 日

摘要

在此处填写您的摘要内容

示例：本文围绕 XXX 展开分析，提出了 XXX 模型，并探讨了其优势与适用场景。

【关键词】请填写您的关键词，例如：区块链；联邦学习；数据共享；隐私保护；智能合约

Abstract

在此处填写您的英文摘要内容

示例：This paper systematically analyzes XXX and proposes XXX models. The advantages and challenges are discussed in detail.

【Keywords】请填写您的英文关键词，例如：Blockchain; Federated Learning; Data Sharing; Privacy Protection; Smart Contracts

目录

1 引言

1.1 背景介绍

在此处填写背景介绍内容

示例：在大数据和人工智能快速发展的背景下，数据孤岛和隐私保护之间的矛盾日益凸显[1]。联邦学习的提出为这一困境提供了新的思路……

1.2 报告的目的与重要性

在此处填写报告的目的与重要性内容

2　章节标题示例：技术概述

2.1　技术定义与特性

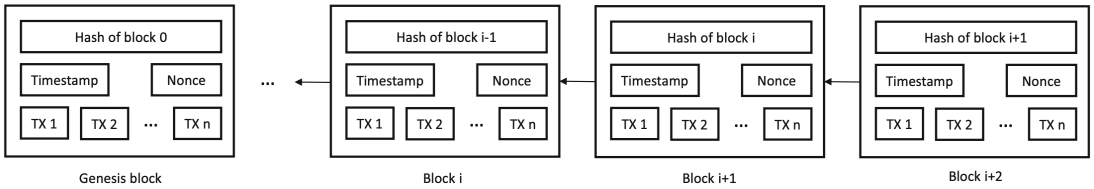

图 1: 示意图示例：此处填写图片说明文字

2.2　工作原理

- 特性一：请填写特性描述。
- 特性二：请填写特性描述。
- 特性三：请填写特性描述。

3　联邦学习

3.1　联邦学习基本概念

联邦学习（Federated Learning, FL）是一种分布式机器学习框架，在保障数据隐私的前提下，实现多方协同训练机器学习模型[2]。与传统集中式训练不同，联邦学习不要求上传原始数据到中央服务器，而是各参与方（客户端）在本地使用自身数据训练模型，仅上传模型更新（如参数梯度）至中央服务器进行聚合，从而形成全局模型，如图 2所示。

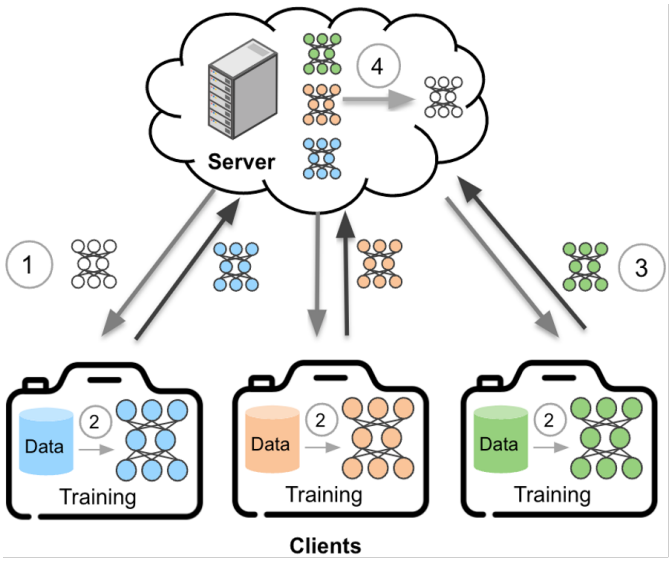

图 2: 联邦学习工作流程总览图

该概念最早由 Google 于 2016 年提出[1]，其核心优势在于数据始终保留本地，避免了隐私泄露风险与法律合规问题，同时通过整合多方知识提升模型泛化性能。联邦学习已在医疗、金融、移动终端等数据敏感场景获得广泛应用[3-4]。

3.2　联邦学习的工作流程

联邦学习的典型流程如图 3所示，主要包括以下步骤：

(i) **全局模型初始化与下发**：服务器初始化全局模型并下发至客户端。

(ii) **客户端本地训练**：客户端在本地数据上进行模型训练，更新模型参数。

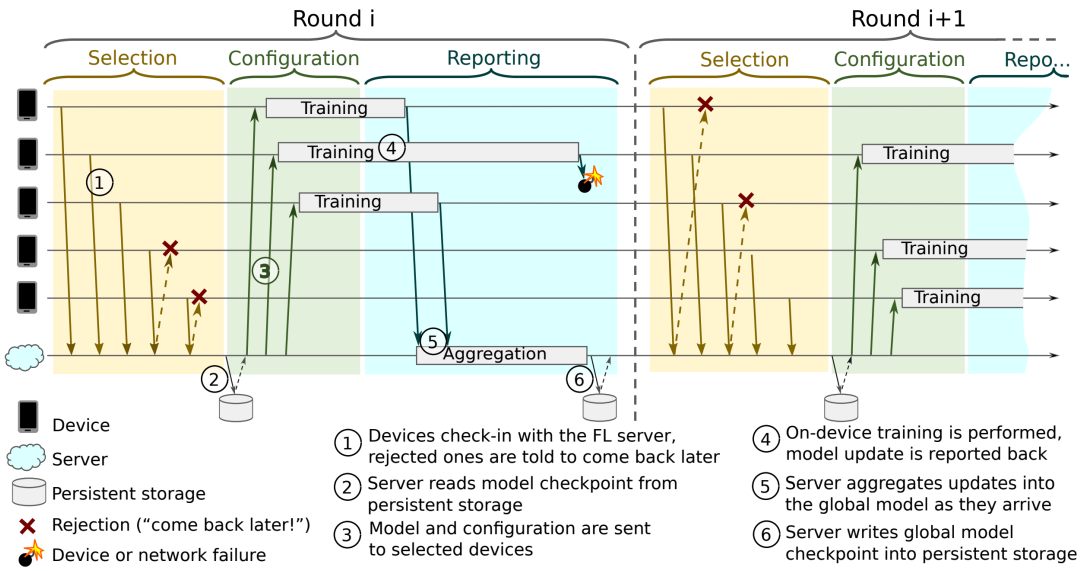

图 3: 典型联邦学习协议轮次流程示意图[5]

(iii) **本地模型更新上传**：客户端将加密后的模型更新（如梯度）上传至服务器。

(iv) **全局模型聚合**：服务器采用如 FederatedAveraging 等算法聚合客户端更新，形成新的全局模型。

(v) **循环迭代直至收敛**：重复上述过程，直至模型收敛或达到设定轮次。

(vi) **模型评估与部署**：服务器对全局模型进行评估，若满足性能要求则部署至客户端。

在整个过程中，原始数据从不离开本地，跨节点仅传递模型更新，可结合差分隐私、安全多方计算等技术进一步增强安全性与信任度。

3.3 联邦学习的主要挑战

尽管联邦学习在隐私保护方面具备优势，其分布式架构也带来了以下关键挑战[6-7]：

- **信任与安全挑战**：依赖中心服务器存在单点故障与中毒攻击等安全隐患，需引入稳健聚合、差分隐私等机制提升安全性。
- **缺乏激励机制**：缺乏合理激励可能导致参与方积极性不足或出现搭便车行为，影响整体训练质量。

- **统计异构性**：各客户端数据分布差异显著（Non-IID 问题），加剧模型收敛困难，影响全局模型泛化性。
- **系统异构性**：设备性能与网络环境差异大，易产生“慢节点”问题，需设计容错与调度机制适应异构环境。
- **通信负担**：多轮模型交换带来高通信开销与潜在窃听风险，需借助加密与通信压缩技术优化效率与安全。
- **法规约束**：需遵循各国数据隐私法规（如 GDPR）限制，设计合规的跨境协作方案[8]。

综上，联邦学习在打破数据孤岛方面展现潜力，但仍需解决信任、激励与异构性等技术难题。为应对这些挑战，区块链的去中心化与可编程机制为联邦学习提供了重要补充。下一节将系统探讨区块链赋能下的数据共享机制设计。

参考文献

[1] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial intelligence and statistics. PMLR, 2017: 1273-1282.

[2] YANG Q, LIU Y, CHEN T, et al. Federated machine learning: Concept and applications[J]. ACM Transactions on Intelligent Systems and Technology (TIST), 2019, 10(2): 1-19.

[3] ZHANG J, LIU Y, HUA Y, et al. Fedtgp: Trainable global prototypes with adaptive-margin-enhanced contrastive learning for data and model heterogeneity in federated learning[C]//Proceedings of the AAAI conference on artificial intelligence: Vol. 38. 2024: 16768-16776.

[4] HARD A, RAO K, MATHEWS R, et al. Federated learning for mobile keyboard prediction[A]. 2018.

[5] BONAWITZ K, EICHNER H, GRIESKAMP W, et al. Towards federated learning at scale: System design[J]. Proceedings of machine learning and systems, 2019, 1: 374-388.

[6] ZHU J, CAO J, SAXENA D, et al. Blockchain-empowered federated learning: Challenges, solutions, and future directions[J]. ACM Computing Surveys, 2023, 55(11): 1-31.

[7] LI T, SAHU A K, TALWALKAR A, et al. Federated learning: Challenges, methods, and future directions[J]. IEEE signal processing magazine, 2020, 37(3): 50-60.

[8] LI H, YU L, HE W. The impact of gdpr on global technology development[J]. Journal of Global Information Technology Management, 2019, 22(1): 1-6.