YOUR **COMPANY NAME**

**2024年全国大学生信息安全竞赛**

**概要介绍**

**作品名称：**  Fed Privacy Shield

**电子邮箱：** 2948953101@qq.com

**提交日期：** 2024年6月5号

**一、前言**

在数字化时代，数据成为了现代社会的核心资产，特别是在人工智能和大数据分析领域，用以提供个性化服务、优化业务流程和增强决策支持。然而，数据的广泛利用同时也引发了关于数据安全和隐私保护的严峻挑战，尤其是**处理敏感信息**时。

**数据泄露和隐私侵犯现象越来越频繁**。传统的数据处理模型通常涉及将大量数据集中存储至中心服务器，这增加了数据被非法获取的风险，并且面临法律和道德上的复杂挑战。此外，数据孤岛现象也阻碍了数据的跨领域有效利用，限制了其潜在价值的发挥。

联邦学习作为一种隐私保护技术，通过在本地处理数据并仅共享模型更新而非原始数据，有效降低了隐私泄露的风险，同时打破数据孤岛，提升数据利用效率。因此，**采用联邦学习技术开发数据处理系统**，对提高数据安全性和处理效率意义重大。

**二、创意描述**

本项目开发了一个基于联邦学习的数据处理平台，通过分布式学习机制保护用户数据隐私，并提升数据利用效率。该平台允许多个参与方在本地训练数据模型，仅共享模型参数，确保数据隐私安全。**适用于多个行业**，如医疗健康、金融服务和智能驾驶，提供安全可靠的数据分析和决策支持。

系统创新地提出了**Fast-PDMM Fed和Median-Cos**两种的聚合算法，显著提高了非独立同分布等数据环境下的模型训练效果，并优化了模型更新和聚合过程。同时，我们设计并实现了**自适应差分隐私算法和半可信端方案**，增强了数据在传输和聚合过程中的安全性，有效防御数据泄露和外部攻击。此外，我们采用**SSL/TLS加密传输、JWT鉴权机制和多层负载均衡技术**，进一步提高了数据传输的安全性和缓解了通信压力。

**三、功能简介**

系统分为用户端和管理端，均部署在Web平台上。

用户端功能包括**任务中心、对比实验、自定义服务和个人中心**，支持任务发布、进展查询、模型对比、场景创建和个人信息管理。管理端提供**集群监控、任务管理、用户管理和模型管理功能**，使管理员能够监控系统状态，部署应用程序，并维护用户活动与模型数据。

**四、特色综述**

本项目在Web端和云平台上整合了先进的聚合算法、加密技术和安全认证等技术，优化了模型更新效率并确保了数据隐私。实现了**训练任务均衡化、进程管理可视化、聚合方案多样化、隐私保护全面化、辅助功能贴心化**，最大程度地提升Fed Privacy Shield平台的训练效率、准确率、聚合合理性、安全性。

**五、开发工具与技术**

本项目后端采用Python和Go语言，使用Gin框架构建HTTP服务、gRPC框架构建微服务、Nginx实现负载均衡、MySQL和Redis存储数据、Nacos作为分布式配置中心、Consul进行服务的注册及发现、Jaeger进行全链路追踪、RabbitMQ进行异步通信和流量削峰、Docker进行容器化部署。编写Makefile加速服务的构建。前端采用 Vue.js 框架与 Arco design 组件库开发。

**六、应用对象**

系统主要服务于需要处理敏感数据的企业和研究机构，特别是在医疗、金融和政府部门。这些机构需要在遵守严格的数据隐私法规的同时，有效利用数据支持决策制定。

**七、应用环境**

系统适用于对数据隐私保护要求极高的场景。在个人医疗信息分析、金融风险评估和公共安全监控等领域，系统能够保证数据的隐私和安全，同时提供高效的数据分析工具，支持机构在保证合规性的前提下，充分利用数据资源。

**八、结语**

针对当前处理敏感数据时面临的隐私保护挑战，我们设计并开发了Fed Privacy Shield这一基于联邦学习的智能隐私计算平台。通过集成创新技术，本项目不仅解决了数据隐私和处理效率问题，而且提供了一种新的数据分析解决方案。我们期待这一系统在未来的实际应用中发挥更大的作用，推动隐私保护技术的发展和普及，从而助力各行各业的数据安全和决策优化。

目前，本项目已入选大学生创新创业训练计划，并获得了研发经费支持。我们有一篇与项目相关的研究论文在投，并正在申请相关的技术专利，以进一步巩固和扩展我们的研究成果。

**Fed Privacy Shield，智能守护数据隐私安全！**