文献引用格式：陈涛，郭睿，刘志强．面向大数据隐私保护的联邦学习算法航空应用模型研究 [J]. 信息安全与通信保密，2020(9):75-84.
CHEN Tao,GAO Rui,LIU Zhiqiang.Research on Aviation Application Model of Federated Learning Algorithm for Big Data Privacy Protection[J].Information Security and Communications Privacy,2020(9):75-84.

面向大数据隐私保护的联邦学习算法航空应用模型研究*

陈　涛[1]，郭　睿[1]，刘志强[2]
（1. 中国航空集团有限公司信息管理部，北京 101300；
2. 北京市公安局顺义分局警务支援大队，北京 101300）

摘　要：对目前人工智能算法在航空领域存在的数据孤岛问题和数据隐私保护问题进行了分析，并提出了面向数据隐私保护的联邦学习航空出行预测方法，在数据隐私保护的前提下，融合高铁出行数据、第三方应用 App 记录的居民消费数据进行联邦学习，大大提高了航空出行预测的准确性和可靠性，同时解决了多企业、多行业数据融合及机器学习带来的数据隐私保护问题。

关键词：数据孤岛；数据隐私保护；出行预测；联邦学习
中图分类号：TP309　　**文献标志码：**A　　**文章编号：**1009-8054(2020)09-0075-10

Research on Aviation Application Model of Federated Learning Algorithm for Big Data Privacy Protection

CHEN Tao[1], GAO Rui[1], LIU Zhiqiang[2]
（1.Information Management Department of China National Aviation Holding Company, Beijing 101300, China;
2.Police Support Branch of Beijing Public Security Bureau Shunyi District Bureau, Beijing 101300, China）

Abstract: Analyzing the problem of data islands and data privacy protection in the aviation field of artificial intelligence algorithms, and proposing a federal learning aviation travel prediction method for data privacy protection. On the premise of data privacy protection, it integrates high-speed rail data, the

* 收稿日期：2020-06-28；修回日期：2020-08-17　Received date:2020-06-28; Revised date:2020-08-17

resident consume data coming from third-party application App. The federal learning greatly improve the accuracy and reliability of aviation travel prediction, and at the same time it solves the data privacy protection problem brought by multi-enterprise and multi- industry data fusion machine learning.

Key words: data silos; data privacy protection; travel prediction; federal learning

0 引 言

近年来，航空领域大量应用了大数据和人工智能技术，如基于大数据机器学习的航空人为因素在航空事故调查中的影响研究、基于 MI-SVR 模型研究航空旅客出行指数预测的方法、基于长短时记忆网络（Long Short-Term Memory）的航班预售期内每日订座数预测研究等，采用大数据和人工智能算法解决航空领域内的故障预测、航空旅客出行指数预测、航班行程人数预测等问题。天气因素、人均收入和其他出行数据（高铁出行、长途汽车等）将对其预测的准确性产生极大影响。如何综合多行业数据进行精准预测是目前人工智能技术应用到航空领域亟需解决的问题。

人工智能（Artifical Intelligence，AI）技术是在多维度、全方位分析数据的基础上，根据特定的应用目标采集其中有用的特征进行训练、学习，最后实现应用智能化的目标。随着大数据、机器视觉检测、超级计算、可穿戴设备等技术的逐步普及应用，人工智能技术得到了快速发展并取得了显著的成果。如特斯拉推出的自动驾驶汽车、谷歌 AlphaGo 机器人等。

人工智能技术应用的基础就是数据的采集、处理、计算。因此需要很多应用系统支持对数据进行自动收集挖掘、整合分析，从而作出支持计算的行为决策，即人工智能技术严格依赖数据采集。然而在目前的发展过程中，数据采集和处理的过程中存在以下两个问题[1-2]：

（1）数据孤岛问题：目前，大多数企业存储的数据通常局限于本企业经营产生的业务数据，往往存在数据规模有限、数据质量良莠不齐的问题。另外，由于行业竞争、隐私保护等问题，造成了数据难以在不同的系统之间共享、整合的问题，导致整个互联网范围内的数据都是按照不同的应用彼此分离、单点存在的。由于人工智能技术往往基于多个领域，需要的数据覆盖范围广，不同应用之间无法共享数据，使得其要求的多领域的特点很难被满足，也即单个系统拥有的数据无法为人工智能技术的开展提供有力的支持。对于每个企业的应用系统而言，其花费了大量的成本部署数据采集、清洗、转换等应用，但是数据可能仅仅局限于自身系统使用，无法在整个互联网范围内高效地共享进而转换为更广泛的应用。这一方面无疑是对互联网数据资源的一种浪费，另一方面不同应用系

统间的数据壁垒也导致大范围级别的数据应用，比如人工智能技术在各行各业的应用变得成本更加高昂、实施也更加困难。

（2）隐私保护问题：最近几年，随着各种网络新应用的不断涌现，应用对应的用户数据如何合理采集、安全传输、存储和处理变得愈来愈重要。一旦用户数据发生泄漏，都会引起社会的强烈谴责，甚至会对应用造成严重的信任危机。如2018年3月，英国一家名为剑桥分析的公司获取了数千万条脸书注册用户的个人信息。由于涉及的用户人数众多、数据种类广泛、数据内容繁多，此次数据泄露在世界范围内引起了抵制使用脸书的抗议活动。与此同时，针对用户数据隐私和安全管理的监管也在逐渐变得更为严格。国际上，2018年5月起欧盟开始正式出台《通用数据保护条例》（General Data Protection Regulation，GDPR）法案。国内在更早的2017年6月开始推行《网络安全法》，也在2019年5月开始实施《数据安全管理办法（征求意见稿）》。上述法案对应用系统采集、传输、使用数据整个过程的安全规范都有明确规定，如未经数据平台方的允许，任何第三方不得随意抓取、使用数据平台方的数据，以及未经用户同意不得随意将敏感类数据分享给第三方。一旦违反将会面临巨额罚款甚至需要承担法律责任。上述多项监管措施，使得在没有得到用户充分授权的情况下，单个应用采集数据及不同应用间数据整合面临重重阻力，这为人工智能领域传统的数据获取模式带来了新的巨大的挑战。

上述数据孤岛和隐私保护问题广泛存在，并且两者存在相互制衡的关系，制约了数据的广泛采集、共享和进一步的应用及人工智能技术的发展。如何在保护隐私安全、满足法律监管要求的前提下，设计一个全新的机器学习框架，达到整合多方数据、跨界共同建模，共同受益的目标，这是近年来数据安全领域和人工智能领域发展的一个重要课题。基于人工智能技术的航空出行数据预测需要在整合多方数据的基础上作出分析、决策，因此首先要解决上述的数据孤岛和隐私保护两个问题。

本文提出一种全新的基于联邦学习的航空出行预测算法，其设计目标是在满足数据安全的前提下，采用人工智能技术提高航空公司出行数据预测的正确率。

1 联邦学习背景

本联邦学习（Federated Learning）是为应对人工智能实际应用时面对的数据隐私保护问题而诞生的一种全新的人工智能学习框架[3]。其最早由Google公司在2016年提出，核心目标是使各个参与者在无需直接交换数据的前提下，实现数据在多个节点之间进行联合训练，达到建立共享的、全局有效的人工智能学习模型的目地。

基于联邦学习框架的人工智能模型的训练流程为[4]：

（1）在远程云上建立一个协调者，该协调者首先生成初始的全局数据模型 W_0；

（2）在第 i 轮训练过程中，每个参与者基于全局数据模型 W_i 和本地保存的数据 D_i 对本地人工智能模型进行训练；

（3）本地模型迭代更新后，根据某种加密通信机制，客户端将该模型参数 M_i 传输到协调者；

（4）协调者聚合每个参与者上传的数据并进行训练以构建全局模型 W_{i+1}；

（5）重复上述步骤，直到全局模型参数 W_i 收敛。

相对于传统的人工智能学习框架，联邦学习的典型特点是：训练过程无需共享数据，通过加密机制下的参数交换方式，在不会泄露用户隐私或违反监管条例的前提下，在云上建立一个虚拟的共有模型并对其进行训练更新。这些特点，充分整合了各个孤立数据源，汇聚多维度数据形成一个数据联邦，各个参与者都可从其中获益，真正实现了合作共赢。另外，多个参与者的数据始终保留在本地，无需上传共享，参与者之间也无法相互推测出对方拥有的特征，数据隐私也得到很好的保护[5]。

联邦学习[6]的理念自提出以来，就受到了极大的关注，多家企业参与到研发联邦学习的框架中，如谷歌的 Tensorflow Federated（TFF）框架目前已较好的支持了横向联邦学习，并支持用户自定义模型训练算法。Open Mided 开源的 Pysyft 框架，提供了多种安全加密算法，为隐私保护提供更强有力的保证。国内的腾讯公司也推出了 FATE 框架，该框架率先在其内部的微众银行平台得到应用，在工业产品中验证了其高效性。

另外，基于联邦学习框架的成熟的人工智能产品近来也不断涌现。Google 在 Android 的 Google Gboard键盘中，采用了横向联邦学习技术，根据设备上的历史记录，在下一次迭代中改进输入法预测模型的性能。Gboard 主要会根据使用者已输入的单词推荐即将使用的下一个单词，以此来加快使用者的打字速度。据计算，Gboard 输入法联想词预测准确率增加 24%，联想词条点击率增加 10%。正如其宣传语所言，Gboard 实现了你的数据就在你手机本地，Google 输入法只是用它的目标。

Nvidia 与伦敦 King's College 合作，利用联盟学习方式，开发医疗影像的人工智慧系统。该系统只需从每个终端装置传送分析结果到中央模型就能训练。至于训练出的人工智慧系统，将运用在脑肿瘤分割分析。此过程不会泄漏病人任何隐私数据，对提升医疗结构用户体验有很大帮助。阿里巴巴利用联邦学习技术，推出蚂蚁金服共享学习平台，破解了电商数据共享和隐私保护难以平衡的难题，实现数据的多方协同和授权共享，应用在智能信贷、智能风控等专业领域中。

联邦学习不断发展的过程中，必然会有越来越多的领域从此项技术中获益。以航空出行领域应用为例，虽然人工智能技术应用越来越广泛，目前也有多家航空企业推出了基于人工智能技术的出行预测服务，但目前各个企业之间的内容安全服务和数据都是独立的，在数据不能互通的情况下，各家企业的数据资源非常有限。另外，并没有成功借鉴具有重要参考价值的铁路出行数据，以及部分用户消费 APP 数据。这些原因导致航空出行预测模型的效果不尽人意，要实现跨企业、行业甚至跨应用等多机构的整体安全协同治理也很困难。联邦学习可直击这些

航空企业的痛点，几近完美地解决存在的问题。

综合来看，联邦学习破解了数据隐私保护的难题，另外为人工智能技术的发展提供了全新的模型框架，对于数据安全和人工智能领域的不断发展和技术落地都有很重要的意义。

2 联邦学习原理

2.1 联邦学习数学模型

联邦学习的目标就是通过使用全新的训练模式使其训练效果超越传统的机器学习模型，在具体的数学数据模型[7-8]为：

定义 N 个用户：

$$\{F_1, \quad F_2, \quad \cdots, \quad F_N\} \tag{1}$$

每个参与者的私有数据为：

$$\{D_1, \quad D_2, \quad \cdots, \quad D_N\} \tag{2}$$

将每个用户的数据汇聚为整体数据集：

$$D = D_1 \bigcup D_2 \bigcup \cdots \bigcup D_N \tag{3}$$

针对数据集 D，使用传统机器学习方式获得的结果：

$$V_{sum} = [w^T \quad D] \tag{4}$$

使用联邦学习模型获得结果为：

$$V_{FED} = [w^T D_1] + [w^T D_2] + \cdots + [w^T D_N] \tag{5}$$

目标误差 δ 定义为：

$$\delta = [V_{FED} - V_{sum}] \tag{6}$$

2.2 联邦学习数学模型

联邦学习根据参与者的数据的特征分类为横向联邦学习（Horizontal Fedetated Learning，HFL）、纵向联邦学习（Vertical Fedetated Learning，VFL）和联邦迁移学习（Fedetated Transfer Learning，FTL）三类[9]。

2.2.1 横向联邦学习

横向联邦学习适用于特征（Features）重叠性高且用户（Samples）样本重叠少时的情境。在这种情况下，将数据集按照用户维度进行切分，并对不同用户的特征取交集进行计算。比如不同地区的航空公司，他们的业务相似（特征相似），但客户不同（样本不同）。横向联邦学习适用场景如图 1 所示：

图 1 横向联邦学习适用场景

横向联邦学习过程如图 2 所示，具体为：

（1）每个参与者（Database Bi）利用自己的资料训练模型，各自计算梯度，再将加密过的梯度修正量上传至中央服务器（Sever）；

（2）由中央服务器整合各参与者的梯度并且更新模型；

（3）中央服务器回传模型更新后的梯度给各个参与者；

（4）参与者更新各自的模型。

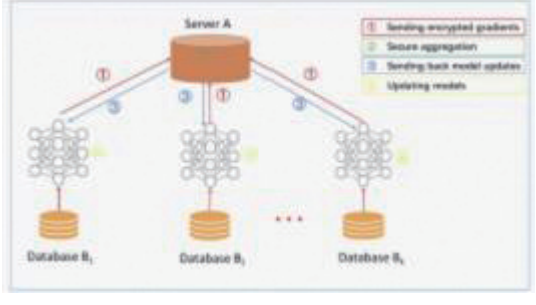

图 2 横向联邦学习过程

横向联邦学习是联邦学习架构中最典型的一种，目前由于其架构简单，实用性高，因此也被运用的最为广泛。

2.2.2 纵向联邦学习

纵向联邦学习适用于样本（Samples）重叠多且特征（Features）重叠少的情境。在这种情况下，将数据集按照特征维度进行切分，对相同用户的特征差集进行计算。比如同一地区的航空公司的客运和传媒，他们接触的客户都为该航班的旅客（样本相同），但业务不同（特征不同）。纵向联邦学习适用场景如图 3 所示：

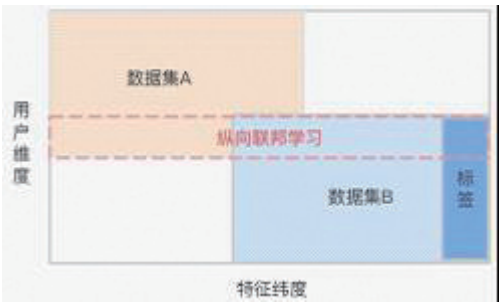

图 3 纵向联邦学习适用场景

纵向联邦学习过程如图 4 所示，具体为：

（1）协调者（Collaborator，C）将公钥发给参与者 A 和参与者 B；

（2）参与者 A 和 B 分别计算和自己相关的特征中间结果，并加密交互，用来求得各自梯度和损失值（Loss）；

（3）参与者 A 和 B 分别将计算后且加密的梯度修正量传送给协调者，同时 B 根据标签计算损失值并把结果汇整给协调者；

（4）协调者将解密后的梯度修正量分别回传给 A 和 B，更新双方的模型。

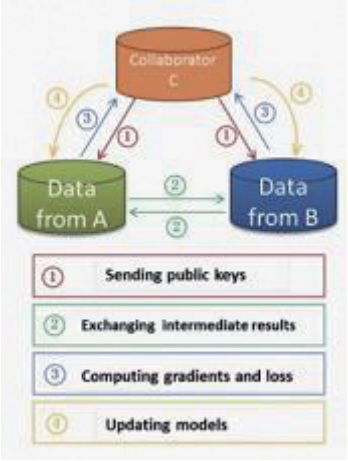

图 4 纵向联邦学习过程

纵向联邦学习虽然解决特征重叠少的问题，但是随着参与端增多，其对应的架构复杂度就会增加，相对更难以执行。

2.2.3 联邦迁移学习

联邦迁移学习适用于当多个参与者的数据的特征（Features）和样本（Samples）重叠都很少的情境。在这种状况下，就不会针对数据进行切割，而会引入迁移式学习（Transfer Learning）来克服资料与标签不足的状况。比如不同国家的航空公司和航空传媒公司，由于地理位置相差遥远，他们的用户群体交集很小。

另外，由于处理的业务不同，二者拥有的数据特征也大相径庭。联邦迁移学习适用场景如图 5 所示：

图 5 联邦迁移学习适应的场景

针对不同的场景，需要的迁移学习[10]算法不同，因此联邦迁移学习并没有统一的学习过程。

3 基于联邦学习的航空出行预测优化算法

3.1 模型原理

本文提出了面向数据隐私保护的联邦学习航空出行预测技术，在引入其他行业或公司数据（如居民收入数据、高铁出行数据和第三方APP应用数据）大大提高航空领域出行预测准确率的情况下，同时解决了交通出行领域多行业、跨行业数据共享的安全性问题。算法框架如图6所示：

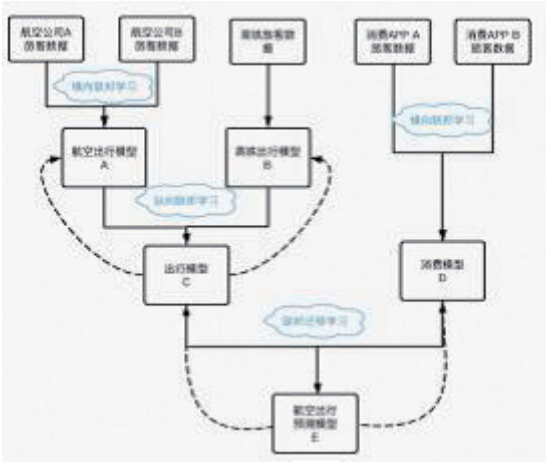

图6 联邦迁移学习应用领域

其主要步骤为：

（1）航空公司A和航空公司B之间采用横向联邦学习，提取共同的出行参数，如用户搜索记录、访问时间、航班预订记录、航空优惠信息等，最终经过训练形成航空出行模型A；

（2）航空公司和高铁集团之间采用纵向联邦学习，提取多维度特征参数指标和同用户训练样本，综合考察同一个用户的航空访问信息和高铁查询记录，与高铁模型B经过联合模型训练后形成出行模型C；

（3）航空公司和第三方应用App之间（如酒店预订、旅游类等消费App），由于参与者的数据的特征（Features）和样本（Samples）重叠都很少，因此采用联邦迁移学习算法进行联合调参。消费模型D与出行模型E，经过计算融合，最终形成航空出行预测模型E；

（4）在出行模型、消费模型以及最终的航空出行预测模型对应的参数收敛之前，需要反向更新各模型的参数，以达到不断迭代的目的。

上述基于联邦学习模型的航空预测模型中，还需要考虑模型参数在正向和反向传递过程中的安全性问题。综合考虑数据安全性及应用场景的特点，该模型采用非对称密钥的方式进行加密。非对称加密算法使用私钥进行信息加密[11-13]，公钥对加密信息解密。以航空出行模型A与高铁出行模型B进行横向联邦学习的过程举例，具体使用方式为：

（1）航空出行模型A与高铁出行模型B分别用其对应的私钥加密模型的各项参数，并各自将模型参数传送给出行模型C；

（2）出行模型C用事先约定好的公钥对收到的加密参数进行解密，并验证发送者的身份，如果验证通过，则模型C更新对应的输入参数。

3.2 实验结果对比与分析

3.2.1 联邦学习与分布式机器学习对比

当前，大规模机器学习模型在训练过程中存在对单个机器节点计算能力的要求超出其实

际存储和计算上限的问题[14]。针对这个问题，目前业界通用的解决办法是使用分布式机器学习系统。分布式机器学习系统通过采用数据并行、模型并行等方式，对数据训练集或者学习模型进行模块划分，利用分布式集群来实现完成大规模甚至超大规模机器学习目标。其中数据并行是分布式机器学习最常用的解决方法，数据并行指的是在分布式集群的每一个计算节点上保有相同的模型，然后将大量的数据分拆成不同的子集，各个计算节点负责一个数据子集的计算，在节点之间同步梯度、并更新模型参数[15]。该方法实现过程简单，但在数据划分时需要事先在全局范围内共享数据，存在 IO 开销大、数据隐私无法保证两个问题。

联邦学习与分布式机器学习有相似的地方，即都充分利用了分布式节点的计算、存储能力。但是联邦学习的具体学习过程中，最典型的特点是每个节点可在不共享资料的前提下，达到同样的训练模型的目标。这样带来的好处一方面减少了数据带来的网络、IO 开销，另一方面不泄漏用户隐私得到保护，满足日益严格的安全监管规范。联邦学习与分布式机器学习在数据处理、学习过程、额外优势方面的具体对比如表 1 所示：

表 1 联邦学习与分布式机器学习对比分析

	联邦学习	分布式机器学习
数据处理	节点自有	节点间共享
学习过程	节点决定是否更新	中心节点统一控制
额外优势	隐私保护 数据传输代价小	无

逻辑回归模型[16]（Logistic Regression Model）是目前广泛应用的一种机器学习算法，它通过将数据拟合到一个逻辑函数中，较大影响的因素分配高权重，完成对事件发生概率的预测。

本文对比实验使用基于逻辑回归模型的分布式机器学习算法对相同的数据进行分析预测，以对比不同算法的优劣。

3.2.2 实验结果分析

本文主要应用 Spark 分析平台对出行数据进行分析预测，具体的实验环境如表 2 所示：

表 2 实验环境说明

指标	指标指数
集群机器个数	6
单机内存	32G
系统版本	Ubuntu 16.04
Spark 版本	2.4.2
编程接口	PySpark

采用本文所提出的算法与传统基于逻辑回归模型的分布式机器学习算法对多个数量级的旅客信息出行分析，并以此为基础，分别对未来一周、一个月和三个月内的出行人数进行预测，算法预测的准确率分别如图 7、图 8 和图 9 所示，其中横坐标轴代表分析的数据人数总量，纵坐标代表使用两种算法分别计算出的预测正确率。

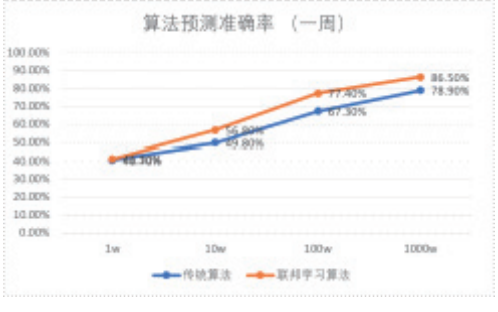

图 7 模型预测准确率一周对比情况

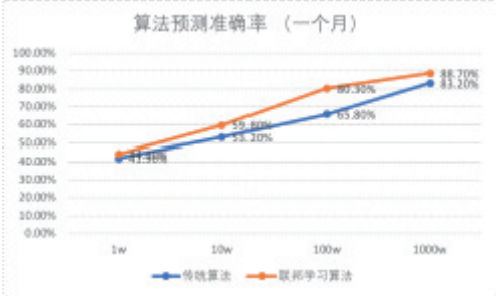

图 8 模型预测准确率一个月对比情况

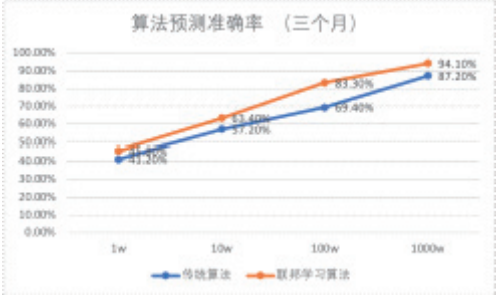

图 9 模型预测准确率三个月对比情况

从上图算法准确率对比图中可以看出：

（1）在相同预测时间范围、相同数据规模的情况下，基于联邦学习预测算法的预测正确率均高于传统的基于逻辑回归模型的分布式机器学习算法，准确率最大差异可达 14.5%（预测周期为一个月，人群数据规模为 100 万时），体现出了基于联邦学习预测算法的优越性。

（2）在预测未来相同时间范围内的出行数据时，随着人群数据从 1 万到 1000 万过程中，两种算法的计算准确率也随之提高，即满足训练数据越多，预测结果越准确的规律。

（3）在不同时间范围的预测数据中，预测的周期越长，准确率越高。如图 9 所示，两种算法对未来 3 个月内的出行数据预测准确率均高于其对应的一周预测准确率。即两种算法对较长期的预测结果均具有更好的作用，这是因为用户往往出于提前购票优惠的心理提前进行消费，导致部分用户消费记录具有前瞻性，因此较长期的预测效果表现更好。

4 总结与展望

近年来，数据的孤岛分布以及对数据隐私监管力度的加强正在逐渐成为人工智能的下一个挑战，联邦学习的产生为人工智能打破数据屏障和进一步发展提供了新的思路。它实现了在保护本地数据的前提下让多个数据拥有方联合建立共有的模型，从而实现了以保护隐私和数据安全为前提的互利共赢。本文提出了一种基于联邦学习的航空出行预测优化模型，该模型在不泄露用户隐私数据的前提下，可基于广大旅客历史出行数据、消费数据对未来航空出行趋势进行预测。将该模型与传统分布式机器学习模型进行对比实验，结果验证了本文提出模型的有效性。将本文提出的模型应用到航空公司实际场景中，在满足严格的数据监管的前提下，可帮助航空公司有效决策未来出行的航班数、航班种类，便于公司据此做出相应的决策来提高营收。

另一方面，对于联邦学习而言，未来需要重点发展的方向主要有：

联邦学习开源生态加快发展，鼓励多方参与到该领域的学习与研究中来。成熟的开源产品可帮助加快联邦学习的商业化应用落地。

建立统一的联邦学习数据标准。目前联邦学习模型中不同的实体间数据在组织格式上差异巨大，进行模型计算前需要大量的数据清洗及转换工作。未来可建立统一的联邦学习数据标准，用相对统一的数据格式组织可以更快的

建立起相应的学习模型，降低模型在实际场景应用时的执行难度。

参考文献：

[1] 王文杰，胡柏青，刘驰．开源大数据治理与安全软件综述 [J]. 信息网络安全 ,2017,17(5):28-36.

[2] Yang Q,Liu Y,Chen T,et al.Federated Machine Learning: Concept and Applications[J].Acm Transactions on Intelligent Systems,2019,10(2):1-19.

[3] Brisimi T S ,Chen R ,Mela T,et al.Federated learning of predictive models from federated Electronic Health Records[J].International journal of medical informatics,2018,112(1):59-67.

[4] Barcelos C F,Gluz J C ,Vicari R M .An Agent-Based Federated Learning Object Search Service[J]. Interdisciplinary Journal of E Skills & Lifelong Learning,2011(7):1-7.

[5] Malle B,Giuliani N,Kieseberg P,et al.The More the Merrier - Federated Learning from Local Sphere Recommendations[C]//International Cross-domain Conference for Machine Learning & Knowledge Extraction,2017.

[6] 王蓉，马春光，武朋．基于联邦学习和卷积神经网络的入侵检测方法 [J]. 信息网络安全 ,2020,20(4):47-54.

[7] Liu W,Chen L,Chen Y,et al.Accelerating Federated Learning via Momentum Gradient Descent[J]. IEEE Transactions on Parallel and Distributed Systems,2020,31(8):1754-1766.

[8] Pan S J,Yang Q.A survey on transfer learning[J]. IEEE Transactions on knowledge and data engineering,2010,22(10):1345-1359.

[9] Sheth A P,Larson J A.Federated database systems for managing distributed, heterogeneous, and autonomous databases[J].Acm Computing Surveys,1990,22(3):183-236.

[10] 王伟，沈旭东．基于实例的迁移时间序列异常检测算法研究 [J]. 信息网络安全 ,2019,19(3):11-18.

[11] 向永谦，宋智琪，王天宇．一种基于双明文的数据对称加密算法 [J]. 信息网络安全 ,2018,18(7):69-78.

[12] 宋利民，宋晓锐．一种基于混合加密的数据安全传输方案的设计与实现 [J]. 信息网络安全 ,2017,17(12):6-10.

[13] 王生玉，汪金苗，董清风，等．基于属性加密技术研究综述 [J]. 信息网络安全 ,2019,19(9):76-80.

[14] 谢永恒，冯宇波，董清风，等．基于深度学习的数据接入方法研究 [J]. 信息网络安全 ,2019,19(9):36-40.

[15] Li M,Andersen D G,Smola A,et al.Communication efficient distributed machine learning with the parameter server[J].Advances in neural information processing systems,2014(1):19-27.

[16] Zhang Z,Trevino V,Hoseini S S,et al.Variable selection in Logistic regression model with genetic algorithm[J]. Annals of Translational Medicine,2018,6(3):45-45.

作者简介：

陈　涛（1979—），男，学士，高级工程师，主要研究方向为企业安全架构规划设计、网络安全审计与合规建设；

郭　睿（1983—），男，学士，高级工程师，主要研究方向为企业安全架构规划设计、应用安全、云计算安全；

刘志强（1983—），男，学士，二级警督，主要研究方向为信息安全技术管控和重要信息系统安全等级保护。