

基于联邦学习的航班延误预测模型

李国秦 维*

(中国民航大学计算机科学与技术学院 天津 300300)

摘要 针对现有的航班延误预测方法中未考虑多数据源与数据隐私问题,提出一种联邦学习框架,融合逻辑回归的方法,使训练数据可以保留在本地,无须上传共享,在保护数据隐私的前提下对航班延误情况进行预测。同时针对训练过程中会间接泄露信息的问题,采用同态加密技术对传输的参数进行加密操作。实验结果表明,用联邦建模的方法在不共享数据的情况下能达到与传统的方法相似的准确率,为优化民航业务提供了切实可行的方案。

关键词 航班延误 数据隐私 联邦学习 同态加密

中图分类号 TP399

文献标志码 A

DOI:10.3969/j.issn.1000-386x.2024.05.011

FLIGHT DELAY PREDICTION MODEL BASED ON FEDERATED LEARNING

Li Guo Qin Wei*

(College of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China)

Abstract In view of the fact that the existing flight delay prediction methods do not consider the problems of multiple data sources and data privacy, this paper proposes a federated learning framework, which integrates logistic regression methods, so that the training data can kept locally without uploading and sharing, and the flight delay can be predicted on the premise of protecting data privacy. At the same time, aimed at the problem of indirect information leakage in the training process, homomorphic encryption technology was adopted to encrypt the transmitted parameters. The experimental results show that the federated modeling method can achieve similar accuracy than the traditional method without sharing data, which provides a practical scheme for optimizing civil aviation business.

Keywords Flight delay Data privacy Federated learning Homomorphic encryption

0 引言

航班延误每年造成数百亿元的损失,延误发生时,航空网络的性能会受到影响,并且延误可能会传播到其他航班链,由于资源可用性的限制,这些航班链随后也会影响机场的性能。

针对航班延误问题,国内外学者进行了许多钻研。文献[1]开发了一种神经网络模型,该模型通过使用从机场各种传感器收集的数据和有关飞行的信息,利用神经网络来估计航班的起飞延误。文献[2]研究了使用航班数据和天气数据,采用并行算法验证了预测超过给定阈值的延误时具有较高的准确

性。文献[3]介绍了一种多级输入层人工神经网络结构,用来对航班延误进行预测。文献[4]分析了时间因素对多个不同机场航班延误的影响,并观察了延误率在一整天内的变化,使用方差分析和K均值聚类模型预测一天中特定时间段的延迟。文献[5]通过考虑时间和空间延迟状态作为解释变量,提出了预测飞行延迟的模型,将延迟分类按高于或低于某个阈值,采用随机森林算法预测延迟时间。文献[6]使用递归神经网络(RNN)来预测日常航班延误。文献[7]提出了一种结合天气数据的预测模型,实现了包括决策树、随机森林和k近邻在内的不同机器学习技术来预测天气引起的航班延迟。文献[8]将航班的滑出状态建模为马尔可夫决策过程,并使用强化学习的方法来预测航班

滑出时间造成的延迟。

根据对以上文献的研究可以发现,大部分航班延误问题的研究均采用机器学习的方法,这需要大量的数据来建立一个准确和稳健的模型。虽然当前的技术进步使大数据的存储、处理和计算更加高效,但组合来自不同来源的数据仍然是一个很大的挑战。竞争优势、隐私问题和法律法规以及围绕数据主权和管辖权的问题阻碍了许多组织公开共享其数据。在现有的预测航班延误方法中,不同机场的数据被收集到中央服务器进行处理。然而,由于机场的数据关系着他们的经济效益和战略制定,数据的潜在滥用可能导致严重的隐私侵犯。

为了应对这一挑战,提出基于联邦学习的框架,融合逻辑回归的方法,允许航空数据分布在多个站点进行训练。文献[9]对联邦学习的定义以及分类进行了系统的阐述,联邦学习分为横向联邦、纵向联邦以及联邦迁移学习,并分析了联邦学习通信过程中信息泄露问题。文献[10]提出了一个基于拍卖市场模型来激励数据所有者参与联邦学习,设计了一种基于深度强化学习和图神经网络的自动策略证明机制,实验证明该方法可以为各参与者带来最大的收益。文献[11]将联邦学习用于访问和分析医学数据,而无须共享个人信息,用于医学上的疾病预测及分析。本文针对航班延误预测问题中存在的共享数据问题,提出联邦学习框架,并对联邦学习通信中存在的共享数据潜在泄露问题,在联邦通信之前采用同态加密进行信息加密,让数据有双重保障。

1 预备知识

1.1 问题陈述

通常来说,比预定时间晚15分钟以上起飞或到达的航班被视为延误航班。从根本上说,航班延误的发生是由于缺乏满足航空需求的空域容量供应。一些研究人员指出,空中交通管制不足和航空公司运营不规范也可能导致航班延误,而恶劣天气也是导致近一半系统延误的主要因素。航班延误由许多不同的因素造成,涉及多个不同的民航代理。这些因素导致的空中交通系统的任何中断都可能使涉及的众多机场和航空公司的航班出现更多后续延误。

1.2 联邦学习

联邦学习(Federated Learning, FL)是指多个客户端在一个中央服务器下协作式地训练模型的设置,该设置同时保证训练数据去中心化及分散性。通过使用

联邦学习,可以在不直接访问原始航空数据的情况下训练一个全局模型。具体来说,联邦学习的技术遵循服务器-客户端设置。在每一轮中,服务器从每个客户端收集更新的特征映射模型,用于模型聚合。每个客户端根据全局状态及其本地数据集执行本地计算,并向服务器发送更新。然后服务器将这些更新应用到其全局状态,训练过程一直持续到模型收敛。

联邦学习相比传统的集中学习有以下几个优点。首先,联邦学习对数据进行隔离,使数据不会对外泄露,从而满足用户的隐私保护和数据安全需求。其次,联邦学习可以保证模型质量无损,联邦模型综合了所有碎片化的独立模型,所以联邦模型的效果可以达到与碎片化的独立模型相似甚至更好的效果。除此之外,参与学习的个体在合作时地位平等,联邦学习允许参与者在传递模型参数的同时保持独立的训练。从以上可以得出结论,航空数据特别适合采用联邦学习进行处理。

定义共有 N 个机场的数据所有者 $\{F_1, F_2, \dots, F_N\}$,他们都希望通过结合各方数据 $\{D_1, D_2, \dots, D_N\}$ 来训练一个更好的航班延误预测优化模型。传统方法是将所有数据放在一起,并使用 $D = D_1 \cup D_2 \cup \dots \cup D_N$ 来训练模型 M_{sum} ,但由于各机场的数据涉及隐私,并不可以把自己的数据分享出来,所以问题迟迟得不到解决。而在联邦学习的过程中,数据所有者协同训练模型 M_{fed} ,任何数据拥有者都不会将其数据暴露给其他人。同时, M_{fed} 的准确性表示为 V_{fed} ,应该与 M_{sum} 的性能 V_{sum} 相接近。

每个用户有本地数据样本 $D_n = (x_i, y_i, 1 \leq i \leq n)$,其中 x_i 为输入, y_i 为其对应的输出。由每个用户的数据集训练的FL模型称为本地FL模型,服务器的FL模型将来自所有用户的本地模型聚合为全局FL模型。定义一个向量 w 作为模型参数,引入损失函数 $f(w, x_i, y_i)$,它捕捉了输入向量 x_i 和输出向量 y_i 上的FL性能。

在联邦学习中,目标是找到最小化全局目标函数的最佳参数:

$$w^* = \arg \min f(w) \text{ where } f(w) = \frac{1}{N} \sum_{i=1}^N F_i(w) \quad (1)$$

式中: N 表示参与学习者的数量; $F_i(w)$ 表示学习者 i 的本地目标函数。将使用式(1)计算的模型称为共有模型 w ,该模型是每个学习者的本地模型的加权平均值,每个学习者通过最小化其训练集上的本地损失函数来计算其本地目标。

1.3 同态加密

数据私有的协作联邦学习方法保持了数据的保密

性,并允许在不共享航班数据的情况下多个机场进行协同训练,但这其中仍然存在着隐私风险。研究表明,训练数据可以从模型权重中近似获得。

在训练过程中原始数据没有直接进行传输,但是被来回传输的模型参数会间接地造成数据泄露。按照链式求导法则,输入数据能够从梯度中反推出来。当训练数据中的输入数据被反推出来后,通过前向传播求出模型输出值,然后根据公式可以求出数据集中的目标输出数据,经过上述过程,数据集的信息便泄露出去。为了避免这个问题的发生,采用同态加密的方法对训练过程中的参数进行加密。

同态加密(Homomorphic Encryption, HE)是一种无须解密即可在加密数据上进行计算的方法,可以得到与在原始数据上计算相同的结果^[12]。在同态映射下,先运算后加密和先加密后运算的结果相同。采用同态加密的方法,可以保护隐私不受对数据进行操作的人的影响,处理者并不知道正在处理数据的具体信息。定义 $[\cdot]$ 表示加密,本文采用 Paillier 同态加密算法,算法的步骤如下:

(1) 密钥生成(KeyGen):随机选择两个大质数 p 、 q 满足 $\gcd(pq, (p-1)(q-1)) = 1$; 计算 $n = pq$ 和 $\lambda = \text{lcm}(p-1, q-1)$; 选择随机整数 $g (g \in \mathbb{Z}_{N^*}^*)$, $\mathbb{Z}_{N^*}^*$ 为密文空间,使得满足 n 整除 g 的阶; 定义 $L(x) = (x-1)/n$, 计算 $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$; 公钥为 (n, g) , 私钥为 λ 。

(2) 加密(Encryption):选择随机数 r , 且 $\gcd(r, n) = 1$, 输入公钥 (n, g) 和明文 m , 对明文加密得到密文 $c = g^m \times r^n \bmod n^2$ 。

(3) 解密(Decryption):输入私钥 (λ, μ) 和密文 c , 计算得明文 $m = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$ 。

(4) 同态属性: E 代表加密。

$$\begin{aligned} E(m_1) \times E(m_2) &= g^{m_1} r_1^n \times g^{m_2} r_2^n \pmod{n^2} = \\ &g^{m_1+m_2} (r_1 \times r_2)^n \pmod{n^2} = E(m_1 + m_2) \\ E(m_1)^{m_2} &= [g^{m_1} r_1^n \pmod{n^2}]^{m_2} = \\ &g^{m_1 \times m_2} r_1^{n \times m_2} \pmod{n^2} = E(m_1 \times m_2) \end{aligned} \quad (2)$$

$E(m_1)$ 与 $E(m_2)$ 相乘的结果等价于明文 $m_1 + m_2$ 在公钥 λ 和随机数 r_1 和 r_2 下加密的结果, $E(m_1)$ 的 m_2 次幂的结果等价于 m_1 与 m_2 相乘, 所以 Paillier 加密算法满足同态特性。

2 数据定义与预处理

2.1 数据定义

本文主要使用航班数据和气象数据两个数据集。

航班数据主要包括日期、始发机场和目的机场标识、航班号、飞机尾号、计划出发和到达时间、实际出发和到达时间、滑入和滑出时间、飞行距离等 20 个属性。气象数据是机场的天气状况,主要包括风向、风速、湿度、能见度、温度、气压、观测点位置、观测时间等 12 个属性。

2.2 数据预处理

数据清洗。由于数据集中存在一些空值和异常值,在进行数据清洗操作时,删除数据中有空值和异常值的航班和气象数据^[13],得到用于进行实验的干净数据集。

数据转换。数据集中存在一些非数字特征,将数据中的机场名称等离散数据进行 one-hot 编码。

数据标准化。由于不同的特征具有不同的比例,因此应用特征缩放将一些特征转换为具有相同比例的新特征。根据式(3)的标准化方法进行数据处理。

$$\hat{x}_i = \frac{x_i - E[x]}{\sqrt{\text{Var}[x]}} \quad (2)$$

式中: x_i 表示特征样本的原始值; $E[x]$ 表示期望值; $\text{Var}[x]$ 表示方差, \hat{x}_i 表示标准化后的特征值。

数据合并。由于航班数据和气象数据属于不同的数据源,航班和气象数据进行融合,得到最终的输入特征。数据融合之前需将航班数据和气象数据建立关联,确保机场所在位置与气象观测点和飞机起飞降落时间与天气观测时间可以一一对应起来。空间上以航班数据中的机场的位置和天气数据中的观测点地方确定同样的位置,时间上以航班的预计起飞或到达时间和气象观测时间作为关联参数^[13]。

2.3 数据分析

在航班预测问题中,需要过滤掉与航班延误无关的属性,增强对数据的基本结构和特征的理解,可以改进模型的训练,以确保能得到良好的预测结果。为了更好地理解结果数据,使用 Python 和统计软件程序对数据进行描述性统计分析,并将分析结果可视化。

图 1 显示了离港航班延误时间分布图,横轴为延误时间,纵轴为频率,其中,大约 90% 的延误时间落在 0~50 分钟之内,延误时间的中位数为 11 分钟,一次航班最严重的延误持续了 1 988 分钟,长时间的延误所占比例较少。图 2 显示了数据集中航班飞行距离的分布,横轴为飞行距离,纵轴为频率。可以看出,飞行距离主要集中在 1 000 英里以内,平均飞行距离在 803.4 英里左右,最长的一次飞行行为 4 983 英里。图 3 为飞行距离与延误时间之间关系的散点图,可以发现飞行距离越长,产生的延误越少,延误的概率更低一

些。大部分延误主要发生在 3 000 英里的飞行距离以内。

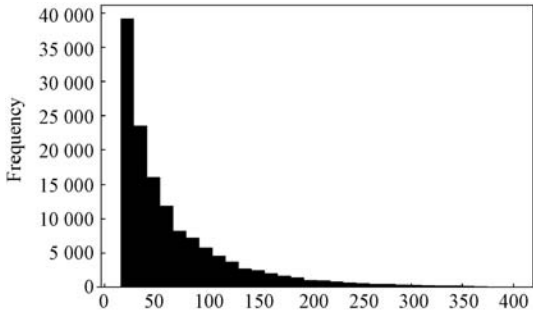


图 1 延误时间分布

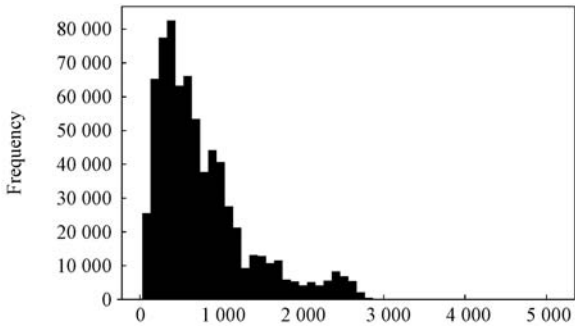


图 2 飞行距离分布

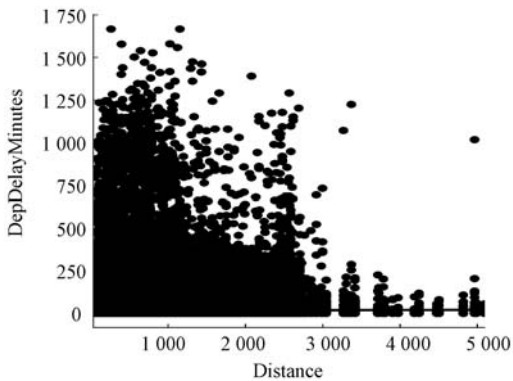


图 3 飞行距离-延误时间分布散点

图 4 以热图的形式显示了一个相关矩阵,以便确定与航班延误问题相关的最重要的特征,数值越大代表二者的相关性越强。重点是出发和到达延迟与其余特征之间的联系。可以看出出发延迟和到达延迟之间具有强相关性。

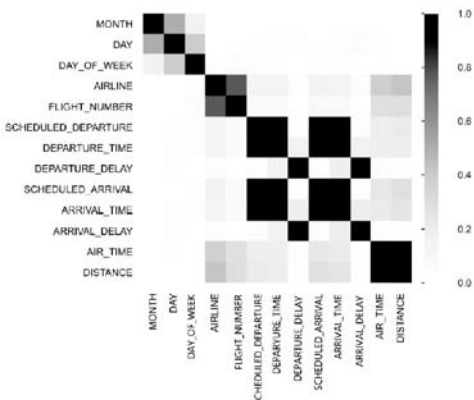


图 4 属性相关性热

3 模型设计

在本文中,采用监督分类算法逻辑回归以及横向联邦学习框架,将航班延误的情况表示为标签 1,航班正常的情况表示为标签 0。

逻辑回归在大多数情况下没有封闭形式的解。因此,需要使用非线性优化方法来寻找回归参数的最大似然估计。牛顿-拉夫森迭代法和随机梯度下降(SGD)是最常用的训练优化方法。因为牛顿-拉夫森迭代方法涉及矩阵求逆,并且大多数同态加密方案不支持除法或矩阵求逆,所以很难用同态加密方案来评估该方法。另一方面,梯度下降不需要除法运算,是同态加密逻辑回归的更好选择。因而选择随机梯度下降法来作为逻辑回归的优化方法。

对于一个预测航班延误的联邦模型,包括一个聚合中央服务器和 N 个参与客户端。

聚合服务器:在每一轮学习中,聚合服务器聚合上传的密文,然后将结果分发给每个参与者。

参与客户端:参与客户端是一组具有相似规模和特点且持有航班数据的大型枢纽机场。参与者的目标是通过联邦学习合作训练高质量航班延误预测模型。在每一轮联邦学习中,每个参与者在本地训练模型,加密他们自己的参数,并上传到聚合服务器。此外,他们从聚合服务器接收聚合的密文,解密后更新模型。

假设每个机场 i 拥有大小为 H_n 的数据集。在联邦模型中,具有 d 个特征的输入样本向量是 $\mathbf{x}_i \in \mathbf{R}^d$,输入样本 \mathbf{x}_i 的标记输出值是 $y_i \in \mathbf{R}$,将它们组合成一组输入输出对 $\{\mathbf{x}_i, y_i\}_{i=1}^{H_n}$ 。对于航班延误预测任务,需要学习一个最佳模型,通过输入训练样本向量 \mathbf{x}_i 并确定模型参数向量 $\mathbf{w} \in \mathbf{R}^d$ 来推断 y_i 值,第 i 个机场相对于其模型参数 \mathbf{w} 的局部损失函数为 $F_i(\mathbf{w})$,即:

$$F_i(\mathbf{w}) = -\frac{1}{n} \sum_{i=1}^n [y_i \ln \hat{y}_i + (1 - y_i) \ln(1 - \hat{y}_i)] \quad (4)$$

机场 i 完成一轮训练后,将参数上传到中心服务器。在中心服务器上,将全局预测模型问题定义如下:

$$\mathbf{w}^* = \operatorname{argmin}_{\mathbf{w}} f(\mathbf{w}) \text{ where } f(\mathbf{w}) = \frac{1}{N} \sum_{i=1}^N F_i(\mathbf{w}) \quad (5)$$

式中: N 表示参与学习者的数量, $F_i(\mathbf{w})$ 表示机场 i 的本地目标函数,最终训练目标是 minimized 全局损失函数 $f(\mathbf{w})$ 。

如图 5 所示,整个过程主要分为五个阶段:密钥生

成阶段、初始化阶段、模型训练阶段、聚合阶段和更新阶段。

(1) 密钥生成。各机场生成密钥,其中各机场被认为是诚实的。

(2) 服务器初始化模型参数 w^0 并发送给各个机场 $\{1, 2, \dots, N\}$ 。

(3) 机场从同一个全局模型开始,该模型要么是随机初始化的(初始训练),要么是根据代理数据训练的。在局部模型训练期间,基于给定的学习率 η 、时期 E 和批处理大小 B ,在每个站点计算相对于其当前模型参数 w^k 的本地梯度 $(\nabla F_i(w))$,所有的机场学习者使用相同的超参数值(学习率、批量大小等)在相同的逻辑回归模型上进行训练,使用相同的本地 SGD 优化器,并将计算后的结果 w_i^k 加密传给服务器。

(4) 服务器收到来自各机场传来的计算结果 $\{w_0^k, w_1^k, \dots, w_N^k\}$,因为本文使用的加密方法是同态加密,该方法具有不解密即可进行运算的特性,所以即使参数进行了加密,仍然可以正常进行聚合。基于同态加密的特性,服务器可以在不解密的前提下聚合来自局部模型的参数 $\sum_{i=1}^N W_i^k$,并对参数进行更新 $w^{k+1} \leftarrow \frac{1}{N} \sum_{i=1}^N w_i^k$,得到一个全局模型 w^{k+1} 。随后将更新后的参数 w^{k+1} 传给各机场客户端。

(5) 机场从服务器收到新的参数后,进行解密并更新自己的参数。

w 为模型参数, K 为迭代步数, w 上标表示不同的迭代步数,下标表示不同的数据所有者,含有下标的参数表示局部模型参数,否则其为全局模型参数。

重复迭代步骤(3) - 步骤(5)过程,直到预测正确的样本数量与总体样本数量的比值大于设置的值时,全局损失函数收敛,则停止训练。训练全局模型的过程只依赖于本地模型的更新,而不是站点上的原始数据。

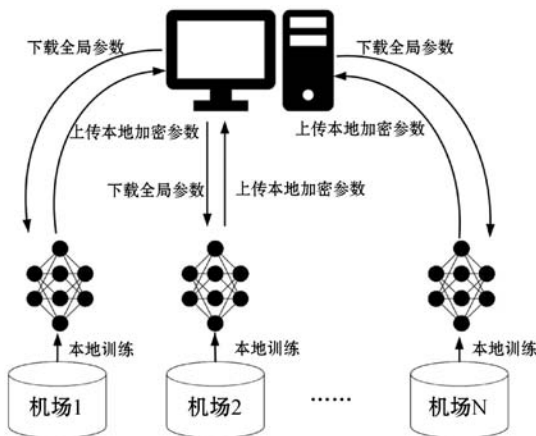


图5 联邦学习航班延误预测模型

4 实验及结果分析

4.1 实验设置

本文采用的数据集为国内三个机场的航班数据以及各机场观测点的气象数据,使用2018年1月—2019年12月两年的数据,实验环境设置三台机器模拟三个不同的机场参与者,使用RAM为8GB,操作系统为CentOS 7,CPU为i7-8565U的三台相同规格的机器模拟客户端,采用一个操作系统为CentOS 7的服务器作为模型聚合器。

要对所提出的模型进行无偏评估,将用于建模的数据分成两部分,即训练集和测试集。训练集用来对模型参数进行拟合,测试集用于提供最终模型的无偏评估。训练集和测试集以7:3的比例进行划分。根据上面提出的机场状态和气象数据的特征,包括总共32个的集合特征作为预测建模的输入,机场每小时航班的延误情况作为是基于原始数据计算的标签。

对于每个本地客户端进行训练时,最大网速配置为10 MB/s,用于模型上传和下载,权重衰减系数为0.0001,学习率为0.1,批处理大小设置为256,迭代总次数为2000次。

为了说明联邦学习和一般机器学习方法在数据模型形成过程中的区别,同时使用了传统的集中式方法进行模型训练。在传统的集中式机器学习训练对照实验中,两个数据集的数据直接混合进行训练。

4.2 评估指标

使用混淆矩阵记录预测结果,以评估模型的预测性能。真反例(T_N)代表的是实际上是准时航班,预测结果也是准时航班;假正例(F_P)代表实际上没有延误,但是预测结果为延误航班;假反例(F_N)代表实际上是延误航班,但预测不会延误;真正例(T_P)代表实际上是延误的,预测结果也是延误的。在模型比较中,主要使用准确度(Accuracy)、精确度(Precision)、召回率(Recall)和F1 score进行衡量。

准确性是最常用和最直观的性能指标,它是在所有样本数中做出正确预测的样本比例,反映了整体分类结果的准确性,计算公式如下:

$$A_{\text{accuracy}} = \frac{T_P + T_N}{T_P + F_N + F_P + T_N} \quad (6)$$

精确率是正确预测为延误的航班数量占全部预测为延误航班的比例,计算公式如下:

$$P_{\text{recision}} = \frac{T_P}{T_P + F_P} \quad (7)$$

召回率是正确预测为延误航班的数量占全部实际为延误航班数量的比例。相应的计算公式如下:

$$R_{recall} = \frac{T_p}{T_p + F_N} \quad (8)$$

为了更直观、更简洁地反映模型的性能,提出了 F1 值的评价指标,对 Precision 和 Recall 进行比较全面的评估。F1 值是算术平均值除以几何平均值。当 F1 较大时,TP 相对增加,FP 相对减少,即准确率和召回率都相对增加。相应的计算公式如下:

$$F1_{score} = 2 \times \frac{P_{recision} \times R_{recall}}{P_{recision} + R_{recall}} \quad (9)$$

图 6 - 图 7 分别为联邦学习和集中学习预测结果的混淆矩阵,大部分样本可以被正确分类。表 1 显示了训练所得模型的性能指标。集中学习的准确率为 0.943,联邦学习的准确率为 0.915,由于中间传输过程和加密操作不可避免地对结果造成一定的精度损失,虽然联邦学习没有达到集中学习相同甚至更高的精度,但是联邦学习建模的方法在保证各方隐私的同时可以得到与传统方法相差不大的结果,误差在可接受的范围内,联邦学习方法让数据可以安全共享,因此可以证明该框架具有实用价值。

表 1 实验结果

模型	准确率	精确率	召回率	F1 score
联邦学习	0.915	0.889	0.713	0.791
集中学习	0.943	0.940	0.798	0.863

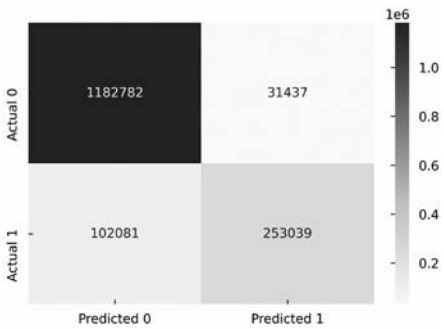


图 6 联邦学习结果混淆矩阵

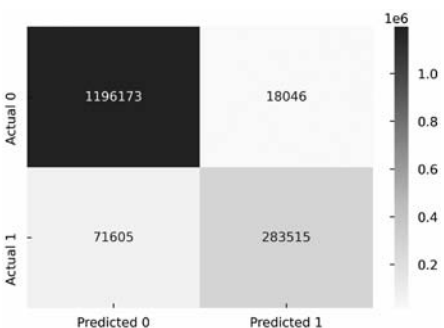


图 7 集中学习结果混淆矩阵

ROC 曲线能够尽量降低不平衡数据集带来的干扰,更加客观地衡量模型本身的性能,所以同时采用

ROC 曲线来评估模型性能。ROC 是 TP 与 FP 的关系图。AUC(Area Under Curve)被定义为曲线下的面积,它常常用作评估标准,因为有时候不同曲线之间的差别可能不够明显,单纯观察曲线并不能清晰地说明哪个分类器的效果更好,AUC 作为计算出来的曲线涵盖的面积值,能更清楚地比较分类器的效果,AUC 值越大,相对应的分类器效果越好。

图 8 为两种方法的 ROC 曲线以及其 AUC 值的比较。可以看出,联邦学习的 AUC 值为 0.930,而集中学习的 AUC 值为 0.933,两者面积只相差 0.003,联邦学习可以达到与集中学习相似的性能。

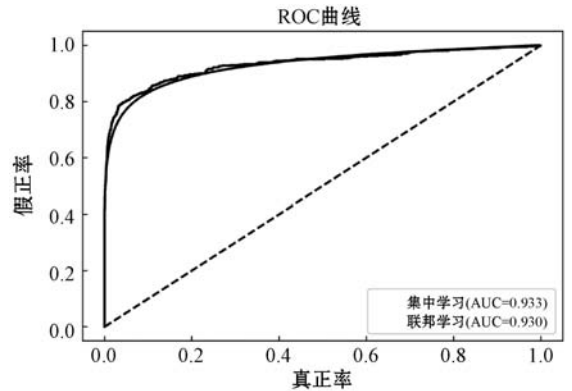


图 8 ROC 曲线

综合各项指标和性能曲线结果,可以发现联邦学习能够较好地实现航班分类预测性能,得到与传统方法相似的性能。同时,联邦学习框架也体现出了相比于传统分类器在隐私保护和学习能力上的优势。

5 结 语

在这篇论文中,致力于开发一个能够预测航班未来延误情况的联邦学习模型,使用来自多个大型枢纽机场数据源,以联邦学习的方式为不同的信任场景训练不同的机器学习模型。通过遵守数据保护框架,能够保证整体隐私不受来自系统的任何模式输出的影响,也不受任何中间结果的影响,同态加密还保证未经任何数据保护的任任何消息交换不会被窃取,因此不会泄露任何信息,这为参与者以及模型本身提供了端到端的隐私保证。有了这些保证,系统生产的模型可以安全地部署到生产中。本文这项工作主要集中在逻辑回归模型,接下来会考虑将所提出的方案扩展到其他分类模型中和应用场景中,在提高模型精度方面也有继续探索的空间。

参 考 文 献

[1] Demir E, Demir V B. Predicting flight delays with artificial

- neural networks: Case study of an airport[C]//Signal Processing & Communications Applications Conference, 2017: 1–4.
- [2] Belcastro L, Marozzo F, Talia D, et al. Using scalable data mining for predicting flight delays[J]. *ACM Transactions on Intelligent Systems and Technology*, 2016, 8(1): 1–20.
- [3] Khanmohammadi S, Tutun S, Kucuk Y. A new multilevel input layer artificial neural network for predicting flight delays at JFK airport[J]. *Procedia Computer Science*, 2016, 95: 237–244.
- [4] Qin Q L, Yu H. A statistical analysis on the periodicity of flight delay rate of the airports in the US[J]. *Advances in Transportation Studies*, 2014, 3: 93–104.
- [5] Rebollo J, Balakrishnan H. Characterization and prediction of air traffic delays[J]. *Transportation Research Part C: Emerging Technologies*, 2014, 44: 231–241.
- [6] Kim Y J, Choi S, Briceno S, et al. A deep learning approach to flight delay prediction[C]//35th Digital Avionics Systems Conference, 2016: 1–6.
- [7] Choi S, Kim Y J, Briceno S, et al. Prediction of weather-induced airline delays based on machine learning algorithms [C]//35th Digital Avionics Systems Conference, 2016: 54–60.
- [8] Balakrishna P, Ganesan R, Sherry L. Accuracy of reinforcement learning algorithms for predicting aircraft taxi-out times: A case-study of Tampa bay departures[J]. *Transportation Research Part C: Emerging Technologies*, 2010, 18(6): 950–962.
- [9] Yang Q, Liu Y, Chen T J, et al. Federated machine learning: Concept and applications[J]. *ACM Transactions on Intelligent Systems and Technology*, 2019, 10(2): 1–19.
- [10] Jiao Y T, Wang P, Niyato D, et al. Toward an automated auction framework for wireless federated learning services market[J]. *IEEE Transactions on Mobile Computing*, 2020, 20(10): 3034–3048.
- [11] Silva S T, Gutman B A, Romero E, et al. Federated learning in distributed medical databases: Meta-analysis of large-scale subcortical brain data [C]//16th IEEE International Symposium on Biomedical Imaging, 2019: 270–279.
- [12] 段淑敏, 殷守林, 张燕丽, 等. 新的同态加密方法——基于 Paillier 和 RSA 密码体制的代理重加密[J]. *微型机与应用*, 2016, 35(7): 6–8, 18.
- [13] 吴仁彪, 李佳怡, 屈景怡. 融合气象数据的并行化航班延误预测模型[J]. *信号处理*, 2018, 34(5): 505–512.
- [14] Zhu H Y, Jin Y C. Multi-objective evolutionary federated learning[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2018, 31(4): 1310–1322.
- [15] Baluch M, Bergstra T, El-Hajj M. Complex analysis of united states flight data using a data mining approach[C]//7th Annual Computing and Communication Workshop and Conference, 2017: 1–6.
- [16] Lu Z L, Wang J D, Zheng G S. A New method to alarm large scale of flights delay based on machine learning[C]//International Symposium on Knowledge Acquisition & Modeling, 2008: 589–592.
- [17] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[C]//International Conference on the Theory and Applications of Cryptographic Techniques, 1999: 223–238.
- [18] 秦莹. 面向数据安全的形式化验证可满足问题研究[D]. 湖南: 国防科学技术大学, 2016.
- [19] Esmaeilzadeh E, Mokhtarimousavi S. Machine learning approach for flight departure delay prediction and analysis[J]. *Transportation Research Record Journal of the Transportation Research Board*, 2020, 2674(4): 3611.
- [20] Anderson A, Kumar A, Christopher A. Analysis of flight delays in aviation system using different classification algorithms and feature selection methods[J]. *The Aeronautical Journal*, 2019, 123(1267): 1–22.
- [21] Borsky S, Unterberger C. Bad weather and flight delays: The impact of sudden and slow onset weather events[J]. *Economics of Transportation*, 2019, 18: 10–26.
- [22] Hossain M S, Hossain M S, Islam M S, et al. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach[J]. *IEEE Access*, 2020, 8: 205071–205087.
- [23] Brisimi T S, Chen R D, Mela T, et al. Federated learning of predictive models from federated electronic health records [J]. *International Journal of Medical Informatics*, 2018, 112: 59–67.
- [24] Guo X J, Liu Z L, Li J, et al. VeriFL: Communication-efficient and fast verifiable aggregation for federated learning [J]. *IEEE Transactions on Information Forensics and Security*, 2020, 16: 1736–1751.
- [25] Guan X M, Ma L. Departure capacity prediction for hub airport in thunderstorm based on data mining method[C]//29th Chinese Control and Decision Conference, 2017: 6004–6009.
- [26] Pyrgiotis N, Malone K M, Odoni A. Modelling delay propagation within an airport network[J]. *Transportation Research Part C: Emerging Technologies*, 2013, 27: 60–75.
- [27] 陈兵, 成翔, 张佳乐, 等. 联邦学习安全与隐私保护综述 [J]. *南京航空航天大学学报*, 2020, 52(5): 675–684.
- [28] Huang L, Shea A L, Liu D B, et al. Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records [J]. *Journal of Biomedical Informatics*, 2019, 99: 103291.