(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111105240 B
(45)授权公告日 2022.12.20

(21)申请号 201911275791.8

(22)申请日 2019.12.12

(65)同一申请的已公布的文献号
申请公布号 CN 111105240 A

(43)申请公布日 2020.05.05

(73)专利权人 中国科学院深圳先进技术研究院
地址 518055 广东省深圳市南山区深圳大学城学苑大道1068号

(72)发明人 阳文斯 叶可江 须成忠

(74)专利代理机构 深圳市铭粤知识产权代理有限公司 44304
专利代理师 孙伟峰 阳志全

(51)Int.Cl.
G06Q 20/40(2012.01)
G06Q 40/02(2012.01)

(56)对比文件
US 2005091524 A1,2005.04.28
CN 109600255 A,2019.04.09
WO 2008122643 A2,2008.10.16
CN 110460600 A,2019.11.15
Wensi Yang ET..“FFD:A Federated Learning Based Method for Credit Card Fraud Detection”.《Lecture Notes in Computer Science》.2019,

审查员 董统传

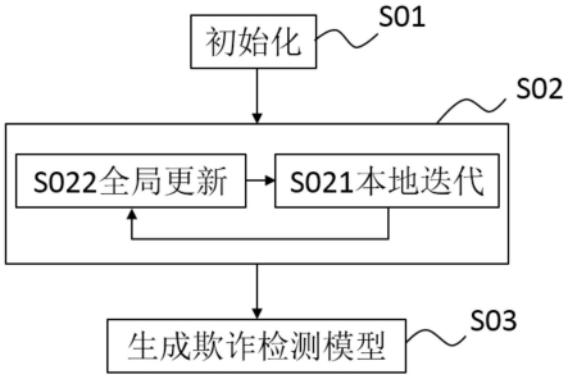
权利要求书2页 说明书8页 附图2页

(54)发明名称

资源敏感的联合金融欺诈检测模型训练方法及检测方法

(57)摘要

本发明公开了一种资源敏感的联合金融欺诈检测方法及检测模型训练方法,模型训练方法包括:S01、服务器端将欺诈检测模型的参数初始化为初始的全局参数;S02、模型训练,包括:S021、本地迭代:各客户端分别获取全局参数,用各自的样本数据集分别训练欺诈检测模型后,更新欺诈检测模型的参数作为本地参数传回服务器端;S022、全局更新:服务器端将本地参数整合成全局参数,并将全局参数发回各客户端进行步骤S021;S03、训练完成,生成采用最后的全局参数的欺诈检测模型。本发明使得各个银行或者金融机构在不共享自己私有数据集的前提下协同训练欺诈检测模型,解决了数据孤岛问题,而又不会侵犯客户隐私或泄露商业秘密,提升了金融欺诈检测效率和准确性。



CN 111105240 B

1.一种资源敏感的联合金融欺诈检测模型训练方法,其特征在于,包括:

S01、初始化:服务器端(A)将欺诈检测模型的参数初始化为初始的全局参数;

S02、模型训练,包括:

S021、本地迭代:各客户端(B_i)分别从服务器端(A)获取全局参数,用各自的样本数据集(D_i)分别训练欺诈检测模型后,更新欺诈检测模型的参数作为本地参数传回服务器端(A);

S022、全局更新:服务器端(A)整合收到的本地参数后生成全局参数,并将全局参数发送回各客户端(B_i)进行步骤S021的本地迭代;

S03、训练完成,生成采用最后的全局参数w*的欺诈检测模型;

其中,所述最后的全局参数w*满足:

$w^*=\arg\min F(w)$,且$F(w)=\frac{\sum_{i=1}^{N} D_i F_i(w)}{D}$, $F_i(w)=\frac{1}{|D_i|}\sum_{j\in D_i} f_j(w)$;

其中,F(w)为所有样本数据集上的全局损失函数,$F_i(w)$为第i个客户端上的样本数据集的本地损失函数,$f_j(w)$为第i个客户端上的第j个样本数据的本地损失,D_i为第i个客户端(B_i)上的样本数据集,$|D_i|$为样本数据集D_i的大小,i、j均为正整数,$D=\sum_{i=1}^{N} D_i$;

其中,步骤S01中,服务器端(A)将欺诈检测模型的两轮全局更新间的本地迭代的轮数τ初始化为τ_0,$\tau_0\geq 1$;

其中,步骤S021中,各客户端(B_i)在各自的样本数据集(D_i)下使用梯度下降法对欺诈检测模型进行本地迭代训练;

其中,步骤S022包括:计算各样本数据集D_i的本地损失函数梯度$\nabla F_i(w)$与全局损失函数梯度$\nabla F(w)$之差的收敛的上界δ,$\delta=\frac{\sum_i D_i \delta_i}{D}$, $||\nabla F_i(w)-\nabla F(w)||\leq \delta_i$,然后根据上界δ得出新的到下一轮全局更新前的本地迭代的轮数τ,并将其发送回各客户端(B_i)。

2.根据权利要求1所述的资源敏感的联合金融欺诈检测模型训练方法,其特征在于,

各客户端(B_i)的一轮本地迭代的过程包括:从样本数据集(D_i)中选取一个样本数据,计算出该样本数据对应的本地损失函数的梯度$\nabla f_j(w)$,用梯度下降法更新欺诈检测模型的参数,重复上述过程直至遍历样本数据集(D_i)中的样本数据,即完成一轮本地迭代。

3.根据权利要求1所述的资源敏感的联合金融欺诈检测模型训练方法,其特征在于,

所述步骤S022中的生成全局参数过程还包括:

服务器计算剩余资源量是否可供下一次本地迭代和全局更新,当剩余资源量不足下一次本地迭代和全局更新时,减小新的本地迭代的轮数τ至可能的最大值,并停止训练。

4.根据权利要求1所述的资源敏感的联合金融欺诈检测模型训练方法,其特征在于,所述得出新的到下一轮全局更新前的本地迭代的轮数τ的过程包括:

各客户端(B_i)利用各自的样本数据集(D_i)计算第一中间参数ρ_i、第二中间参数β_i以及样本数据集(D_i)的本次本地迭代中的最后一轮本地迭代(t_0)的本地损失函数梯度$\nabla F_i(w_i(t_0))$,其中,$\rho_i\leftarrow\frac{||F_i(w_i(t))-F_i(w(t))||}{||w_i(t)-w(t)||}$, $\beta_i\leftarrow\frac{||\nabla F_i(w_i(t))-\nabla F_i(w(t))||}{||w_i(t)-w(t)||}$,$w_i(t)$代表第i个客户端上的第t轮迭代的欺诈检测模型的参数,w(t)代表全局参数;

服务器根据第一中间参数ρ_i、第二中间参数β_i、样本数据集(D_i)的本次本地迭代中的最后一轮本地迭代(t_0)的本地损失函数梯度$\nabla F_i\left(w_i(t_0)\right)$分别得到第一全局中间参数ρ、第二全局中间参数β、所有样本数据集的本次本地迭代中的最后一轮本地迭代(t_0)的全局损失函数梯度$\nabla F\left(w(t_0)\right)$,其中,$\rho \leftarrow \frac{\sum_{i=1}^{N} D_i\rho_i}{D}$, $\beta \leftarrow \frac{\sum_{i=1}^{N} D_i\beta_i}{D}$, $\nabla F(w(t_0)) \leftarrow \frac{\sum_{i=1}^{N} D_i\nabla F_i(w(t_0))}{D}$;

结合公式$\tau^* = \arg\max_{\tau} G(\tau)$, $G(\tau) = \frac{\tau}{\tau+b/c}\left(\eta\left(1-\frac{\beta\eta}{2}\right)-\frac{\varphi h(\tau)}{\tau}\right)$,得到新的本地迭代的轮数τ,其中,η为梯度下降的步长,φ为常数,$h(\tau) = \frac{\delta}{\beta}\left(\left(\eta\beta+1\right)^{\tau}-1\right)-\eta\delta\tau$。

5.一种资源敏感的联合金融欺诈检测方法,其特征在于,采用权利要求1～4任一所述的资源敏感的联合金融欺诈检测模型训练方法训练欺诈检测模型后,将欺诈检测模型用来预测待检测数据。

资源敏感的联合金融欺诈检测模型训练方法及检测方法

技术领域

[0001] 本发明涉及金融安全技术领域，尤其涉及一种资源敏感的联合金融欺诈检测模型训练方法及检测方法。

背景技术

[0002] 近年来，随着电子商务和移动互联网的发展，极大地增加了各个银行的信用卡交易数量，由于信用卡的使用越来越多，诈骗者也试图寻找更多的机会来进行信用卡欺诈，同时各个银行和金融机构也不得不面对越来越多的信用卡欺诈行为。信用卡欺诈是一种犯罪行为，它给银行和金融机构以及持卡人带来了巨大的经济损失。

[0003] 现有的信用卡欺诈检测技术主要分为以下两种：

[0004] 1、基于规则的欺诈识别，该方法是通过规则建立防范机制是比较传统的一类信用卡欺诈检测技术。其通过分析大量欺诈样本，将欺诈行为特点记录下来应用规则引擎及统计分析技术形成“规则”，然后进行多维度多规则的组合，每条规则被赋予一定的权重，命中相关规则的行为会得到累积的分值。即对单次信用卡交易行为的欺诈度进行综合量化，从而来预测欺诈的概率确定诈骗风险评级。

[0005] 2、基于机器学习的模型，指的是采用数据挖掘方法，基于历史数据而建立的分类模型，利用海量数据通过机器训练模型来对信用卡交易进行判断，通过分析消费行为来进行模式识别。通过已有的训练样本(即已知数据以及其对应的输出)去训练得到一个最优模型，具有对未知数据进行推测和分类的能力，比如在已知“好”和“坏”标签的前提下，尝试从历史数据中，分析出欺诈交易的典型特征和消费行为模式，从而遇到相似的行为时可以分辨是否是欺诈交易。

[0006] 然而，上述两种方法都具有一定的缺点。

[0007] 例如，前一种基于规则的欺诈识别的反欺诈规则引擎中，这些甄别欺诈行为的规则依赖于从大量历史案例中总结出来的“专家知识”，也称之为“规则”。随着数据量的增大，数据类型的增多，传统的基于规则匹配的离散式欺诈分析预警系统已经无法准确识别欺诈。

[0008] 由于单靠人工分析是很难检测到信用卡交易事务数据集中的欺诈模式的，所以开发出一种系统来自动实施欺诈检测对于银行和金融机构而言，是必不可少的。

[0009] 然而，基于传统的机器学习的方法中，由于持卡人在不同客户群上的消费模式各不相同，因此需要使用考虑每个客户群动态的数据集来训练性能最佳的模型，但一部分传统的机器学习模型都是运用本地数据集建立独立的内部欺诈检测模型，对用户群的消费模式并不能完全了解，所以独立的内部模型的效果时常不佳。

[0010] 鉴于银行和金融类公司间的竞争性质，他们不愿彼此或在数据中心中共享其专有数据，传统的用于欺诈检测的机器学习模型通常仅使用每家银行或金融机构单独收集的内部数据进行训练。由于这一原因，导致了信用卡欺诈检测过程中出现了严重的数据孤岛问题，导致信用卡欺诈检测效率和检测准确率都不理想。

发明内容

[0011] 鉴于现有技术存在的不足，本发明提供了一种资源敏感的联合金融欺诈检测模型训练方法及检测方法，使得银行、各金融机构等之间的大规模协作成为可能，使得各个银行、金融机构在不共享自己私有数据集的前提下协同训练欺诈检测模型，提高训练效率和准确性。

[0012] 为了实现上述的目的，本发明采用了如下的技术方案：

[0013] 一种资源敏感的联合金融欺诈检测模型训练方法，包括：

[0014] S01、初始化：服务器端将欺诈检测模型的参数初始化为初始的全局参数；

[0015] S02、模型训练，包括：

[0016] S021、本地迭代：各客户端分别从服务器端获取全局参数，用各自的样本数据集分别训练欺诈检测模型后，更新欺诈检测模型的参数作为本地参数传回服务器端；

[0017] S022、全局更新：服务器端整合收到的本地参数后生成全局参数，并将全局参数发送回各客户端进行步骤S021的本地迭代；

[0018] S03、训练完成，生成采用最后的全局参数的欺诈检测模型。

[0019] 作为其中一种实施方式，所述最后的全局参数w^*满足：

[0020] $w^*=\mathrm{argmin}F(w)$，且$F(w)=\frac{\sum_{i=1}^{N}D_iF_i(w)}{D}$，$F_i(w)=\frac{1}{|D_i|}\sum_{j\in D_i}f_j(w)$；

[0021] 其中，$F(w)$为所有样本数据集上的全局损失函数，$F_i(w)$为第i个客户端上的样本数据集的本地损失函数，$f_j(w)$为第i个客户端上的第j个样本数据的本地损失，D_i为第i个客户端上的样本数据集，$|D_i|$为样本数据集D_i的大小，i、j均为正整数。

[0022] 作为其中一种实施方式，步骤S01中，服务器端将欺诈检测模型的两轮全局更新间的本地迭代的轮数τ初始化为τ_0，$\tau_0\geq 1$；

[0023] 步骤S021中，各客户端在各自的样本数据集D_i下使用梯度下降法对欺诈检测模型进行本地迭代训练；

[0024] 步骤S022包括：计算各样本数据集D_i的本地损失函数梯度$\nabla F_i(w)$与全局损失函数梯度$\nabla F(w)$之差的收敛的上界δ，$\delta=\frac{\sum_i D_i\delta_i}{D}$，$||\nabla F_i(w)-\nabla F(w)||\leq\delta_i$，然后根据上界δ得出新的到下一轮全局更新前的本地迭代的轮数τ，并将其发送回各客户端。

[0025] 作为其中一种实施方式，各客户端的一轮本地迭代的过程包括：从样本数据集D_i中选取一个样本数据，计算出该样本数据对应的本地损失函数的梯度$\nabla f_j(w)$，用梯度下降法更新欺诈检测模型的参数，重复上述过程直至遍历样本数据集D_i中的样本数据，即完成一轮本地迭代。

[0026] 作为其中一种实施方式，所述步骤S022中的生成全局参数过程还包括：

[0027] 服务器计算剩余资源量是否可供下一次本地迭代和全局更新，当剩余资源量不足下一次本地迭代和全局更新时，减小新的本地迭代的轮数τ至可能的最大值，并停止训练。

[0028] 作为其中一种实施方式，所述得出新的到下一轮全局更新前的本地迭代的轮数τ的过程包括：

[0029] 各客户端利用各自的样本数据集D_i计算第一中间参数ρ_i、第二中间参数β_i以及样

本数据集D_i的本次本地迭代中的最后一轮本地迭代t_0的本地损失函数梯度$\nabla F_i\left(w_i(t_0)\right)$，其中，$\rho_i \leftarrow \frac{||F_i(w_i(t))-F_i(w(t)||}{||w_i(t)-w(t)||}$，$\beta_i \leftarrow \frac{||\nabla F_i(w_i(t))-\nabla F_i(w(t)||}{||w_i(t)-w(t)||}$，$w_i(t)$代表第i个客户端上的第t轮迭代的欺诈检测模型的参数，w(t)代表全局参数；

[0030] 服务器根据第一中间参数ρ_i、第二中间参数β_i、样本数据集D_i的本次本地迭代中的最后一轮本地迭代t_0的本地损失函数梯度$\nabla F_i\left(w_i(t_0)\right)$分别得到第一全局中间参数ρ、第二全局中间参数β、所有样本数据集的本次本地迭代中的最后一轮本地迭代t_0的全局损失函数梯度$\nabla F\left(w(t_0)\right)$，其中，$\rho \leftarrow \frac{\sum_{i=1}^{N} D_i\rho_i}{D}$，$\beta \leftarrow \frac{\sum_{i=1}^{N} D_i\beta_i}{D}$，$\nabla F(w(t_0)) \leftarrow \frac{\sum_{i=1}^{N} D_i\nabla F_i(w(t_0))}{D}$；

[0031] 结合公式$\tau^* = \underset{\tau}{\arg max}\, G(\tau)$，$G(\tau) = \frac{\tau}{\tau+b/c}\left(\eta\left(1-\frac{\beta\eta}{2}\right)-\frac{\varphi h(\tau)}{\tau}\right)$，得到新的本地迭代的轮数τ，其中，η为梯度下降的步长，φ为常数，$h(\tau) = \frac{\delta}{\beta}\left(\left(\eta\beta+1\right)^{\tau}-1\right)-\eta\delta\tau$。

[0032] 本发明的另一目的在于提供一种资源敏感的联合金融欺诈检测方法，采用一种上述的资源敏感的联合金融欺诈检测模型训练方法训练欺诈检测模型后，将欺诈检测模型用来预测待检测数据。

[0033] 本发明通过构建一种能进行资源优化的联合的机器学习框架，使得各个银行或者金融机构在不共享自己私有数据集的前提下协同训练欺诈检测模型，使得银行或者各金融机构间的大规模协作成为可能，解决了数据孤岛问题，而又不会侵犯客户隐私或泄露商业秘密，提升了金融欺诈检测效率和准确性。同时，还可以对整个系统的资源(如计算资源和通信资源)消耗情况进行统计分析，自适应地协调整个欺诈检测系统的资源和性能，使得整个系统在有限的带宽、能量、时间等资源预算下获得最佳的学习性能。

附图说明

[0034] 图1为本发明实施例的联合金融欺诈检测系统的结构示意图；

[0035] 图2为本发明实施例的联合金融欺诈检测模型训练方法的流程图。

[0036] 图3为本发明实施例的联合金融欺诈检测方法的流程图。

具体实施方式

[0037] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0038] 参阅图1，本发明的联合金融欺诈检测系统主要分为两部分：服务器端A和客户端B_i(i为正整数)，客户端B_i即银行或者金融机构。

[0039] 在客户端B_i，本地数据集被收集并存储在各客户端节点，作为各客户端B_i训练用的样本数据集D_i。各客户端B_i利用各自的样本数据集D_i训练自己的本地欺诈检测系统，并以迭

代的方式更新欺诈检测模型的参数，同时，统计资源消耗量。当本地的欺诈检测模型的参数更新一定轮数后，将最后的欺诈检测模型的参数(作为本地参数)和统计的资源消耗量等参数传输至服务器端A，进行聚合计算。

[0040] 在服务器端A，服务器整合各客户端B_i上传的欺诈检测模型的本地参数，生成全局参数，并将该全局参数发送回各客户端B_i，进行下一次的本地迭代循环。

[0041] 在实际应用中，每个客户端的本地更新和服务器端的全局更新都会消耗一定的计算资源和通信资源。在一些分布式机器学习的欺诈检测系统中并未考虑系统的通信成本，系统的计算资源和通信资源的消耗对整个系统具有较大的影响甚至会成为整个系统的性能瓶颈。考虑到消耗的资源量可能会随时间变化，所以服务器端还需要协调全局聚合的频率、模型训练精度和资源消耗之间复杂的关系。本实施例中，当服务器端A在将该全局参数发送回各客户端B_i时，还同时将资源控制参数发送回各客户端B_i，具体主要表现为控制下一轮全局更新前的本地迭代的轮数τ。

[0042] 具体地，结合图2和图3所示，本实施例提供的一种资源敏感和保护隐私的联合金融欺诈检测模型训练方法，包括：

[0043] S01、初始化：服务器端A将欺诈检测模型的参数初始化为初始的全局参数w(0)。

[0044] 在此过程中，服务器端A还定义了一系列资源控制参数：将欺诈检测模型两轮全局更新间的的一次本地迭代包含的轮数τ初始化为τ_0，$\tau_0 \geq 1$，这里优选$\tau_0=1$；同时，还定义资源计算器s来统计资源使用情况，并设置一个STOP标志位，当该标志位被标记时，则停止迭代训练。初始化时，资源计算器s为0，初始化STOP标志位不被标记。服务器在初始化全局参数和这些资源控制参数后，将其发送给各客户端B_i。

[0045] S02、模型训练，包括：

[0046] S021、本地迭代：各客户端B_i分别从服务器端A获取(下载)全局参数，用各自的样本数据集D_i分别训练欺诈检测模型后，更新欺诈检测模型的参数作为本地参数传回服务器端A。

[0047] 优选地，在该步骤S021中，各客户端B_i在各自的样本数据集D_i下使用梯度下降法对欺诈检测模型进行本地迭代训练。

[0048] S022、全局更新：服务器端A整合收到的本地参数后生成全局参数，并将全局参数发送回各客户端B_i进行步骤S021的本地迭代。

[0049] 在进行第一次本地迭代过程(还未执行步骤S022全局更新)时，客户端B_i获取到的全局参数为w(0)，各客户端B_i利用全局参数进行τ轮本地迭代训练后，将最后一轮本地迭代更新后的欺诈检测模型的参数作为本地参数传输给服务器端A，同时也将资源使用情况传回；服务器端A根据各客户端B_i传回的本地参数进行整合，形成新的全局参数，并根据资源使用情况计算到下一轮全局更新前的本地迭代的轮数τ，并将新的全局参数传回各客户端B_i进行一次全局更新。当进行一次全局更新后，全局参数发生变化，到下一轮全局更新前的本地迭代的轮数τ也发生变化，因此，既可以实现各客户端B_i之间的大规模协作，提高机器学习的精度和准确性，又能实时动态地调整全局聚合的频率，自适应地进行资源优化，避免资源瓶颈对于计算效率的影响，在固定资源预算下训练最优化、效果最佳的模型。

[0050] S03、训练完成，生成采用最后的全局参数w*的欺诈检测模型。

[0051] 如图1所示，假设有N个客户端，各个客户端B_i的样本数据集D_i分别为D_1，D_2，D_3，…

D_N。对于第i个客户端B_i上的样本数据集D_i,其损失函数定义为:

[0052] $$F_i(w)=\frac{1}{|D_i|}\sum_{j\in D_i}f_j(w);$$

[0053] 这里,定义$D_i=|D_i|$,|·|表示计算数据集的大小。$D=\sum_{i=1}^{N}D_i$,当i≠i′有$D_i\cap D_{i'}=\emptyset$。则在所有样本数据集上的全局损失函数为:

[0054] $$F(w)=\frac{\sum_{j\in\cup_i D_i}f_j(w)}{|\cup_i D_i|}=\frac{\sum_{i=1}^{N}D_iF_i(w)}{D};$$

[0055] 因此,整个系统的目标函数可以转换为找到一组全局参数w*,使得F(w)最小,即最后的全局参数w*满足:

[0056] $w^*=\mathrm{argmin}F(w)$,且$$F(w)=\frac{\sum_{i=1}^{N}D_iF_i(w)}{D},\ F_i(w)=\frac{1}{|D_i|}\sum_{j\in D_i}f_j(w);$$

[0057] 其中,F(w)为所有样本数据集上的全局损失函数,$F_i(w)$为第i个客户端上的样本数据集的本地损失函数,$f_j(w)$为第i个客户端上的第j个样本数据的本地损失,D_i为第i个客户端B_i上的样本数据集,$|D_i|$为样本数据集D_i的大小,i、j均为正整数。

[0058] 对于每一轮全局更新t=1,2,…T,客户端从服务器端接收全局参数w(t)和到下一轮全局更新前的本地迭代更新轮数τ。这里,定义每进行一轮全局更新,所有客户端的本地迭代更新消耗c(c>0)个单元的资源,每一次的全局更新消耗b(b>0)个单元的资源,对于给定的总的全局更新轮数T和每两轮全局更新间的本地迭代更新轮数τ,整个迭代过程消耗的资源量为$T(c+\frac{b}{\tau})$,R为已知的总的资源预算,则上述问题重新定义为:

[0059] $$\min_{T,\tau}\ F(w(T)),\ \text{其满足:}\ T*(c+\frac{b}{\tau})\le R;$$

[0060] 通过最小化F(w(T))-F(w^*)的上界,即可求得最优模型。

[0061] 本实施例假设:

[0062] (1)本地损失函数$F_i(w)$满足利普希茨(Lipschitz)条件,其中,ρ为利普希茨常数;

[0063] (2)$F_i(w)$是β-smooth的函数(β光滑函数),通过理论计算有:

[0064] $$F(w(T))-F(w^*)\le\frac{1}{T(\omega\eta\left(1-\frac{\beta\eta}{2}\right)-\frac{\rho h(\tau)}{\tau\varepsilon^2})};$$

[0065] 其中,ω、ε为中间变量,η已知,为梯度下降的步长,ρ为第一全局中间参数、β为第二全局中间参数,η≤1/β。

[0066] 而又由于本地损失函数梯度$\nabla F_i(w)$与全局损失函数梯度$\nabla F(w)$之差的收敛的上界δ满足:

[0067] $$\delta=\frac{\sum_i D_i\delta_i}{D},\ ||\nabla F_i(w)-\nabla F(w)||\le\delta_i;\qquad \text{公式(1)}$$

[0068] $$h(\tau)=\frac{\delta}{\beta}\left(\left(\eta\beta+1\right)^{\tau}-1\right)-\eta\delta\tau;\qquad \text{公式(2)}$$

[0069] 整个系统的优化目标为:

[0070] $\min\limits_{T,\tau} \frac{1}{T(\omega\eta\left(1-\frac{\beta\eta}{2}\right)-\frac{\rho h(\tau)}{\tau\varepsilon^2})}$，其满足：$T \le \frac{R\tau}{c\tau+b}$；

[0071] 相当于：

[0072] $\tau=1,2,3,\ldots \max \frac{R\tau}{c\tau+b}(\omega\eta\left(1-\frac{\beta\eta}{2}\right)-\frac{\rho h(\tau)}{\tau\varepsilon^2})$；

[0073] 上式除以Rω/c，令控制参数$\varphi=\frac{\rho}{\omega\varepsilon^2}$，最后的优化目标为：

[0074] $\tau^* = \arg\max\limits_{\tau} G(\tau)$； 公式（3）

[0075] $G(\tau) = \frac{\tau}{\tau+b/c}(\eta\left(1-\frac{\beta\eta}{2}\right)-\frac{\varphi h(\tau)}{\tau})$； 公式（4）

[0076] 因此，只需给定控制参数φ为常量，即可通过计算得出ρ、β、ω、ε、δ、h(τ)，从而得到优化目标τ^*。

[0077] 因此，固定系统总的资源预算R，给定控制参数φ以及搜索范围修正参数γ，这里，为避免因初始的各种参数估计不准确导致τ增长过快，给定的资源控制参数还包括给定搜索范围修正参数γ（γ＞0），γ限制了搜索空间也避免了因为初始参数估计不准确使得τ增长过快的情况发生。

[0078] 结合图2和图3所示，联合金融欺诈检测模型训练方法具体包括：

[0079] S01、初始化。

[0080] S02、模型训练，其中：

[0081] S021、本地迭代：各客户端B_i的一轮本地迭代的过程包括：从样本数据集D_i中选取一个样本数据，计算出该样本数据对应的本地损失函数的梯度$\nabla f_j(w)$，用梯度下降法更新欺诈检测模型的参数，重复上述过程直至遍历样本数据集D_i中的样本数据，即完成一轮本地迭代。

[0082] 在客户端，当τ轮本地迭代完成后，用t_0存储下一次全局更新前的最后一轮本地迭代的迭代索引，即$t_0 \leftarrow t$。每一轮本地迭代更新各客户端B_i的欺诈检测模型的参数$\widetilde{w}_i(t) \leftarrow w(t)$，即，如果尚未进行全局更新，则$\widetilde{w}_i(t) = w_i(t)$，如果存在全局更新，则$\widetilde{w}_i(t) = w(t) = \frac{\sum_{i=1}^{N} D_i w_i(t)}{D}$。

[0083] 各客户端B_i利用各自的样本数据集D_i计算第一中间参数ρ_i、第二中间参数β_i以及样本数据集D_i的本次本地迭代中的最后一轮本地迭代t_0的本地损失函数梯度$\nabla F_i(w_i(t_0))$，其中，

[0084] $\rho_i \leftarrow \frac{||F_i(w_i(t))-F_i(w(t)||}{||w_i(t)-w(t)||}$； 公式（5）

[0085] $\beta_i \leftarrow \frac{||\nabla F_i(w_i(t))-\nabla F_i(w(t)||}{||w_i(t)-w(t)||}$； 公式（6）

[0086] $w_i(t)$代表第i个客户端上的第t轮迭代的欺诈检测模型的参数，w(t)代表全局参数。

[0087] 在每轮本地迭代过程中，利用各样本数据集D_i计算第i个客户端的第t轮本地迭代的欺诈检测模型的参数$w_i(t)$：

[0088] $$w_i(t) = \widetilde{w}_i(t-1) - \eta \nabla F_i(\widetilde{w}_i(t-1)); \qquad \text{公式（7）}$$

[0089] $$\widetilde{w}_i(t) \leftarrow w_i(t);$$

[0090] 估计第i个客户端Bi每一轮的资源消耗量c_i，并将本地迭代的欺诈检测模型的参数$w_i(t)$、资源消耗量c_i、第一中间参数ρ_i、第二中间参数β_i和样本数据集D_i的本次本地迭代中的最后一轮本地迭代t_0的本地损失函数梯度$\nabla F_i\left(w_i(t_0)\right)$传送给服务器端进行欺诈检测模型的参数的全局更新、τ的更新以及资源消耗的计算。

[0091] S022、全局更新：

[0092] 在服务器端，服务器端A在接收各个客户端的欺诈检测模型的参数$w_i(t)$、资源消耗量c_i、第一中间参数ρ_i、第二中间参数β_i和样本数据集D_i的本次本地迭代中的最后一轮本地迭代t_0的本地损失函数梯度$\nabla F_i\left(w_i(t_0)\right)$后，更新欺诈检测模型的全局参数w(t)：

[0093] $$w(t) = \frac{\sum_{i=1}^{N} D_i w_i(t)}{D}; \qquad \text{公式（8）}$$

[0094] 根据第一中间参数ρ_i、第二中间参数β_i、样本数据集D_i的本次本地迭代中的最后一轮本地迭代t_0的本地损失函数梯度$\nabla F_i\left(w_i(t_0)\right)$分别得到第一全局中间参数ρ、第二全局中间参数β、所有样本数据集的本次本地迭代中的最后一轮本地迭代t_0的全局损失函数梯度$\nabla F\left(w(t_0)\right)$，其中：

[0095] $$\rho \leftarrow \frac{\sum_{i=1}^{N} D_i \rho_i}{D}; \qquad \text{公式（9）}$$

[0096] $$\beta \leftarrow \frac{\sum_{i=1}^{N} D_i \beta_i}{D}; \qquad \text{公式（10）}$$

[0097] $$\nabla F(w(t_0)) \leftarrow \frac{\sum_{i=1}^{N} D_i \nabla F_i(w(t_0))}{D}; \qquad \text{公式（11）}$$

[0098] 计算各样本数据集D_i的本地损失函数梯度$\nabla F_i(w)$与全局损失函数梯度$\nabla F(w)$之差的收敛的上界δ：

[0099] $$\delta_i \leftarrow \left|\left|\nabla F_i\left(w(t_0)\right) - \nabla F\left(w(t_0)\right)\right|\right|;$$

[0100] $$\delta \leftarrow \frac{\sum_{i=1}^{N} D_i \delta_i}{D}; \qquad \text{公式（12）}$$

[0101] 由上述式子，计算得出中间变量ω、ε，最后由公式$\tau^* = \underset{\tau}{\arg max} G(\tau)$，$G(\tau) = \frac{\tau}{\tau + b/c}\left(\eta\left(1 - \frac{\beta\eta}{2}\right) - \frac{\varphi h(\tau)}{\tau}\right)$，即可计算得出新的轮数τ。将$\tau_{max} \leftarrow \gamma\tau$，得出本地迭代轮数的可能的最大值$\tau_{max}$作为接下来的本地迭代轮数τ，将生成的全局参数w(t)、新的τ传送给各客户端B_i。

[0102] 具体在生成可能的最大值τ_{max}时，服务器端根据各客户端传输回的资源消耗量c_i

和上一个轮数τ,计算出本轮全局更新的资源消耗量b和本轮全局更新后下一次本地迭代的每一轮资源消耗量c,并计算剩余资源量是否可供当前轮的全局更新和接下来的本地迭代。在实际计算过程中,c的值是根据客户端节点的资源消耗的测量值估算的,估算方法取决于所考虑的资源类型。例如,当资源为能源时,所有客户端节点上的总能源消耗(本地迭代中的每一轮更新)被视为c;当资源为时间时,所有客户端节点上的最大计算时间(本地迭代中的每一轮更新)视为c。同样的道理,b的值是根据服务器端的资源消耗测量值估算的,例如服务器端消耗的能源或者计算所用的时间。其中,能源和时间可以直接测量得到。

[0103] 服务器端基于估算值b、c监控总资源消耗s,并将总资源消耗与总的资源预算R进行比较。具体是,总资源消耗量s的计算:

[0104] $s \leftarrow s+c\tau+b$;

[0105] 如果$s+c\tau+b \geq R$,则减小τ到可能的最大值τ_{max},使得本轮全局更新后剩下的本地迭代需要消耗的资源量在总的资源预算R之内,同时,标记STOP标志位,代表训练完成,将全局参数w(t)返回作为欺诈检测模型的最后的全局参数,即,进行下一步骤S03,生成采用最后的全局参数w*的欺诈检测模型,随后即可进行欺诈检测。

[0106] 本发明还提供了一种资源敏感和保护隐私的联合金融欺诈检测方法,在上述的联合金融欺诈检测模型训练方法训练欺诈检测模型后,将欺诈检测模型用来预测待检测数据即可。

[0107] 本发明通过构建一种能进行资源优化的联合的机器学习框架,使得各个银行或者金融机构之间打破数据壁垒,在不共享自己私有数据集的前提下协同训练欺诈检测模型,使得银行或者各金融机构间的大规模协作成为可能,解决了数据孤岛问题,而又不会侵犯客户隐私或泄露商业秘密,提升了金融欺诈检测效率和准确性。同时,还可以对整个系统的资源(如计算资源和通信资源)消耗情况进行统计分析,通过控制本地迭代更新轮数和共享模型的全局参数更新次数,自适应地协调整个欺诈检测系统的计算资源与通信资源,使得整个系统在有限的资源预算下获得最佳的学习性能。

[0108] 以上所述仅是本申请的具体实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本申请原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本申请的保护范围。

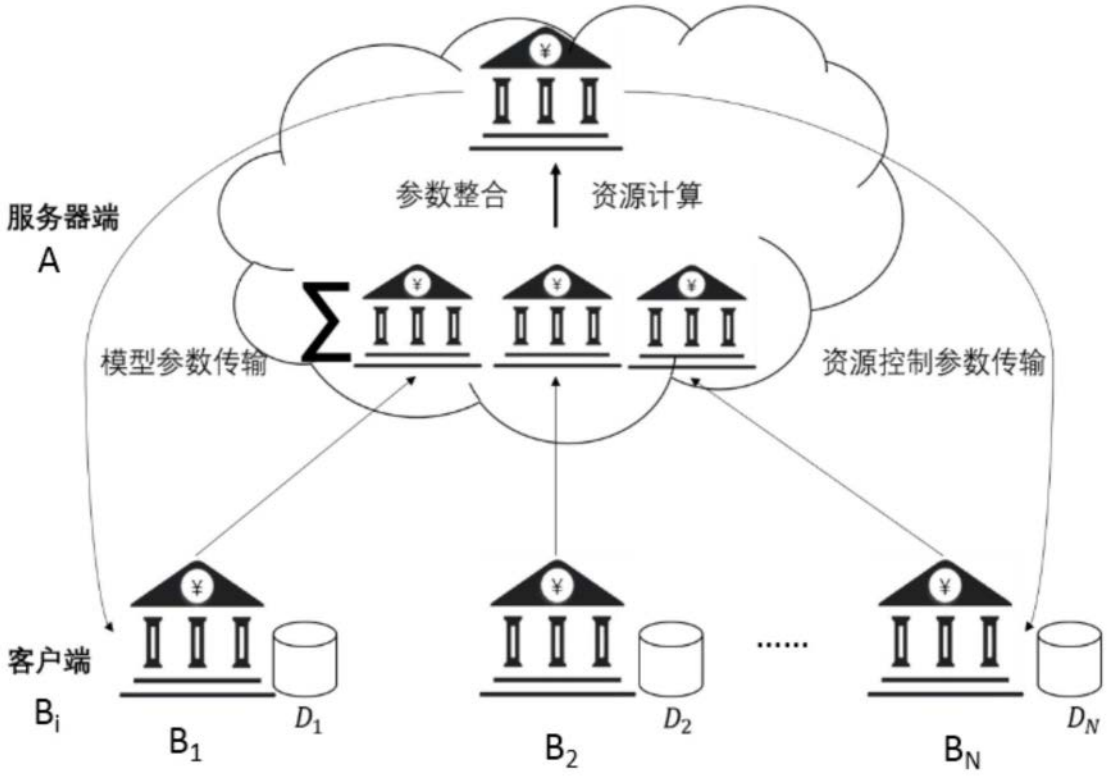

服务器端
A
参数整合
资源计算
模型参数传输
资源控制参数传输
客户端
B_i
B_1
D_1
B_2
D_2
.....
B_N
D_N

图1

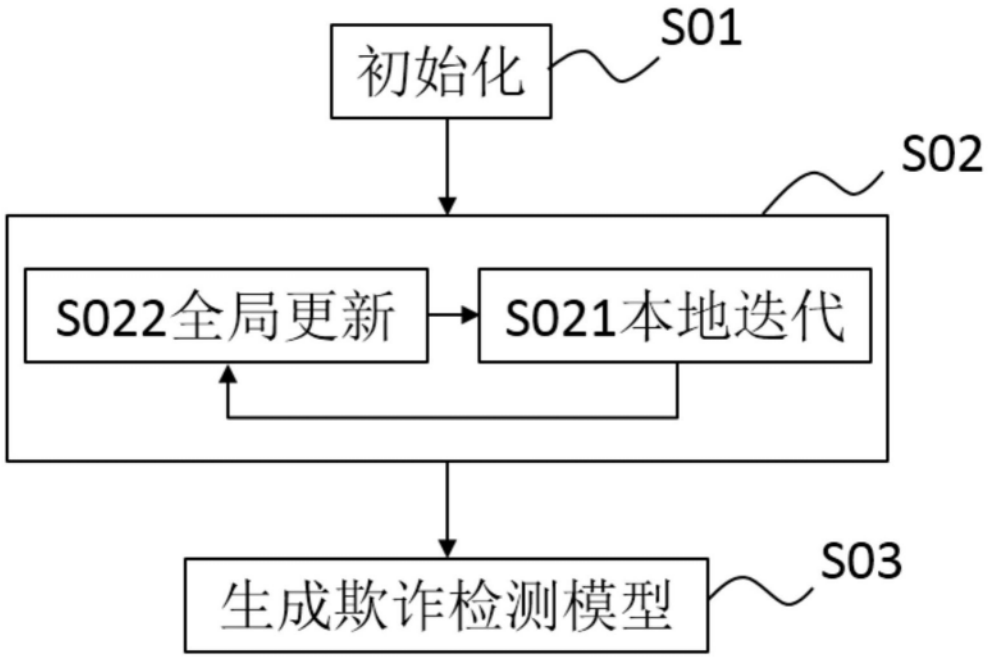

初始化
S01
S02
S022全局更新
S021本地迭代
生成欺诈检测模型
S03

图2

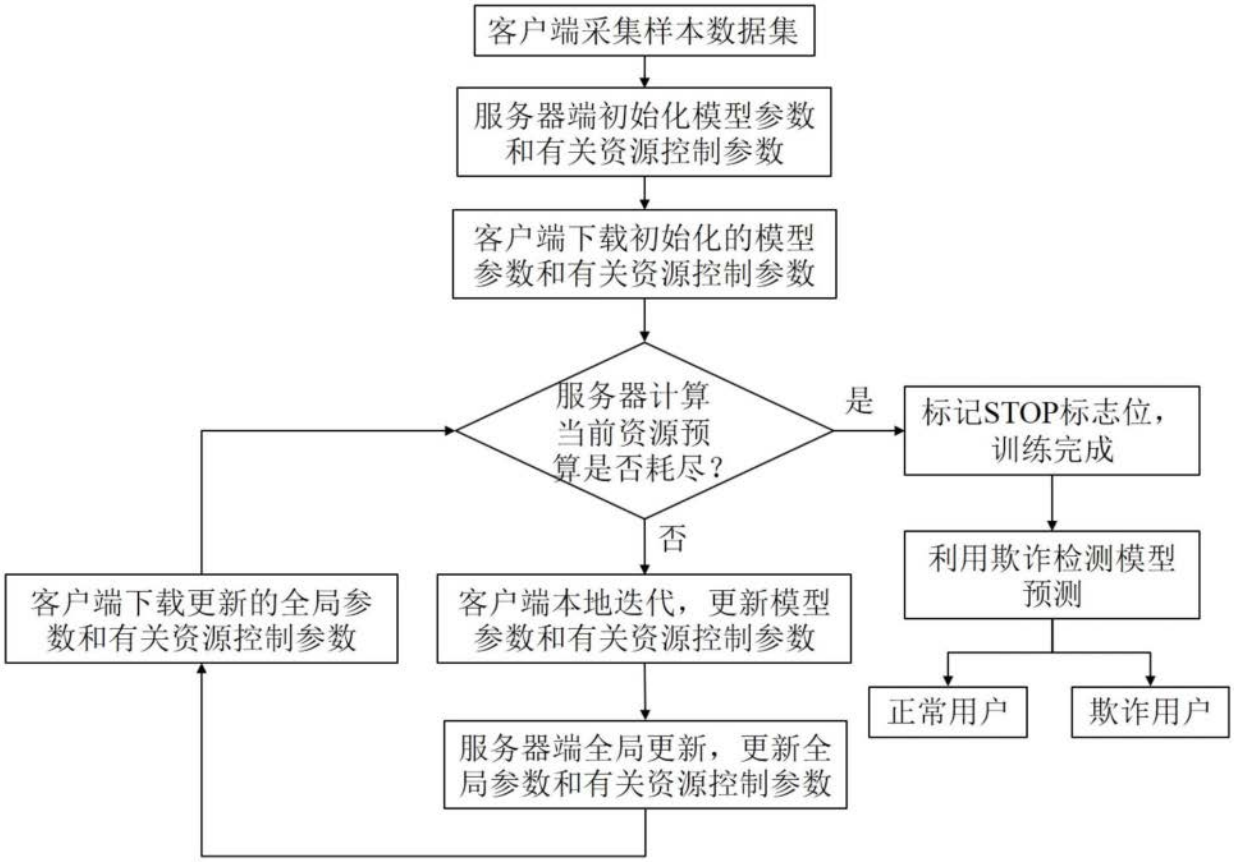

客户端采集样本数据集
服务器端初始化模型参数和有关资源控制参数
客户端下载初始化的模型参数和有关资源控制参数
服务器计算当前资源预算是否耗尽？
是
标记STOP标志位，训练完成
利用欺诈检测模型预测
正常用户
欺诈用户
否
客户端本地迭代，更新模型参数和有关资源控制参数
服务器端全局更新，更新全局参数和有关资源控制参数
客户端下载更新的全局参数和有关资源控制参数

图3