

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 11 月 21 日 (21.11.2019)



(10) 国际公布号
WO 2019/218699 A1

(51) 国际专利分类号:
G06Q 30/00 (2012.01)

(21) 国际申请号: PCT/CN2019/070159

(22) 国际申请日: 2019 年 1 月 3 日 (03.01.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810479060.4 2018 年 5 月 18 日 (18.05.2018) CN

(71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518052 (CN)。

(72) 发明人: 石建(SHI, Jian); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong

518052 (CN)。 陈飞腾(CHEN, Feiteng); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518052 (CN)。

(74) 代理人: 广州华进联合专利商标代理有限公司(ADVANCE CHINA IP LAW OFFICE); 中国广东省广州市天河区珠江东路 6 号 4501 房 (部位: 自编 01-03 和 08-12 单元) (仅限办公用途), Guangdong 510623 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: FRAUD TRANSACTION DETERMINING METHOD AND APPARATUS, COMPUTER DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 欺诈交易判断方法、装置、计算机设备和存储介质

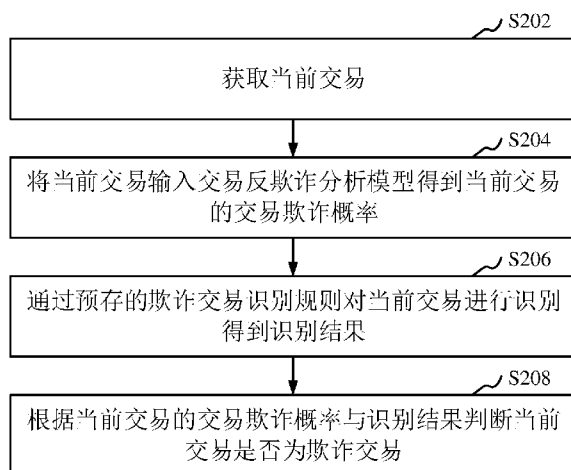


图 2

S202 Obtain current transaction
S204 Input the current transaction to a transaction anti-fraud analysis model to obtain the transaction fraud probability of the current transaction
S206 Identify the current transaction by means of a pre-stored fraud transaction identification rule to obtain the identification result
S208 Determine whether the current transaction is a fraud transaction according to the transaction fraud probability of the current transaction and the identification result

(57) Abstract: A fraud transaction determining method, comprising: obtaining current transaction; inputting the current transaction to a transaction anti-fraud analysis model to obtain the transaction fraud probability of the current transaction; identifying the current transaction by means of a pre-stored fraud transaction identification rule to obtain the identification result; and determining whether the current transaction is a fraud transaction according to the transaction fraud probability of the current transaction and the identification result.

(57) 摘要: 一种欺诈交易判断方法, 包括: 获取当前交易; 将当前交易输入交易反欺诈分析模型得到当前交易的交易欺诈概率; 通过预存的欺诈交易识别规则对当前交易进行识别得到识别结果; 根据当前交易的交易欺诈概率与识别结果判断当前交易是否为欺诈交易。

[见续页]



WO 2019/218699 A1

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国(除另有指明，要求每一种可提供的地区
保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

- 包括国际检索报告(条约第21条(3))。

发明名称：欺诈交易判断方法、装置、计算机设备和存储介质

相关申请的交叉引用

本申请要求于 2018 年 5 月 18 日提交中国专利局，申请号为 2018104790604，申请名称为“欺诈交易判断方法、装置、计算机设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及一种欺诈交易判断方法、装置、计算机设备和存储介质。

背景技术

随着现代网络技术的发展，电子交易在生活中被越来越广泛地应用，随之而来也存在电子交易为欺诈交易的风险，如信息泄露或者交易违法等；因此需要在交易中对当前交易的交易数据进行欺诈分析，当根据交易数据分析出当前交易可能为欺诈交易时，则结束当前交易。

传统地，一般利用一些交易反欺诈实时评分模型对当前交易进行分析，如 FICO（一种个人信用评级法）、SAS（STATISTICAL ANALYSIS SYSTEM，数据分析系统，银行可通过部署 SAS 欺诈管理，进行反欺诈分析）、同盾的交易反欺诈模型等；然而，发明人意识到，这些模型的通用性较差，对实际交易中发生的欺诈交易判断的准确率较低。

发明内容

根据本申请公开的各种实施例，提供一种欺诈交易判断方法、装置、计算机设备和存储介质。

一种欺诈交易判断方法，所述方法包括：

获取当前交易；

将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈概率；

通过预存的欺诈交易识别规则对所述当前交易进行识别得到识别结果；

及

根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是否为欺诈交易。

一种欺诈交易判断装置，所述装置包括：

数据获取模块，用于获取当前交易；

概率分析模块，用于将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈概率；

规则识别模块，用于通过预存的欺诈交易识别规则对所述当前交易进行识别得到识别结果；及

5 结果获取模块，用于根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是否为欺诈交易。

一种计算机设备，包括存储器和一个或多个处理器，所述存储器中储存有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述一个或多个处理器执行以下步骤：

10 获取当前交易；

将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈概率；

通过预存的欺诈交易识别规则对所述当前交易进行识别得到识别结果；及

15 根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是否为欺诈交易。

一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：

20 获取当前交易；

将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈概率；

通过预存的欺诈交易识别规则对所述当前交易进行识别得到识别结果；及

25 根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是否为欺诈交易。

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其它特征和优点将从说明书、附图以及权利要求书变得明显。

30 附图说明

为了更清楚地说明本申请实施例中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

35 图 1 为根据一个或多个实施例中欺诈交易判断方法的应用场景图。

图 2 为根据一个或多个实施例中欺诈交易判断方法的流程示意图。

图 3 为根据一个或多个实施例中模型训练步骤的流程示意图。

图 4 为根据一个或多个实施例中图 3 中的步骤 S304 的流程示意图。

图 5 为根据一个或多个实施例中欺诈交易判断装置的框图。

5 图 6 为根据一个或多个实施例中计算机设备的框图。

具体实施方式

为了使本申请的技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

10 本申请提供的欺诈交易判断方法，可以应用于如图 1 所示的应用环境中。其中，终端与服务器通过网络进行通信。终端从服务器中获取当前交易，将当前交易输入交易反欺诈分析模型得到当前交易的交易欺诈概率，并通过欺诈交易识别规则对当前交易进行识别，通过当前交易的交易欺诈概率与欺诈交易识别规则的识别结果两个方案的结合，判断当前交易是否为欺诈交易。

15 其中，终端可以但不限于各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备，服务器可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

20 在一些实施例中，如图 2 所示，提供了一种欺诈交易判断方法，以该方法应用于图 1 中的终端为例进行说明，包括以下步骤：

S202，获取当前交易。

当前交易是指需要判断其是否为欺诈交易的交易，如需要对多笔交易进行欺诈性判断，则分别将多笔交易按顺序作为当前交易进行后续操作；当前交易可以包括一笔交易的交易金额、时间、账户数据等信息。

25 具体地，终端从服务器获取需要判断是否为欺诈交易的当前交易，服务器可以是业务系统或其他交易系统，其中业务系统可以为交易网站或存储交易数据的数据库，其他交易系统可以是其他合作网站等。

S204，将当前交易输入交易反欺诈分析模型得到当前交易的交易欺诈概率。

30 其中，交易反欺诈分析模型是用于分析输入的当前交易的交易欺诈概率的模型；交易反欺诈分析模型可以是技术人员以历史交易数据作为样本数据训练得到的神经网络模型或规则模型。

交易欺诈概率是终端通过交易反欺诈分析模型对当前交易进行判断得到当前交易为欺诈交易的概率；交易欺诈概率可以以百分比的形式展示，也可以采用其他数学表示方法。

具体地，终端将获取到的当前交易输入到根据历史交易数据以及历史交易数据中的欺诈信息作为样本数据训练得到的交易反欺诈分析模型中，根据模型训练的规则得到当前交易为欺诈交易的概率。

S206，通过预存的欺诈交易识别规则对当前交易进行识别得到识别结果。

5 其中，欺诈交易识别规则是根据不同的交易特征制定的用于评判当前交易是否为欺诈交易的规则。欺诈交易识别规则可以包括基于高频交易的限额限次规则和基于历史风险交易特征提取的欺诈交易识别规则决策组合等；基于高频交易的限额限次规则即查看执行当前交易的账户在一段时间内的交易次数和交易金额，当该账户在短时间内进行多次大金额的交易，则该账户进
10 行的交易为欺诈交易的可能性较高；基于历史风险交易特征提取的欺诈交易识别规则可以是基于执行当前交易的账户的历史交易信息制定的欺诈交易识别规则：如该账户的设备曾经使用该设备登录多个账户、或者执行当前交易的账户在注册之后的短时间内进行了多次大额交易等，都可以作为该当前交易为欺诈交易的评判标准。

15 具体地，终端将制定好欺诈交易识别规则预存在终端或服务器中，在接收到当前交易时，终端可以先调取此预存的欺诈交易识别规则对当前交易进行识别，判断当前交易是否存在欺诈风险。

S208，根据当前交易的交易欺诈概率与识别结果判断当前交易是否为欺诈交易。

20 具体地，当前交易通过步骤 S204 中的交易反欺诈分析模型得到的交易欺诈概率与步骤 S206 中通过预存的欺诈交易识别规则对当前交易的识别结果结合起来，判断当前交易是否为欺诈交易。

可选地，当前交易通过交易反欺诈分析模型得到的交易欺诈概率大于预设值时，则表示该当前交易很可能为欺诈交易；若通过预存的欺诈交易识别
25 规则识别后也认为当前交易的账户信息或交易金额等数据较为可疑，则可以判断当前交易为欺诈交易。然后终端将当前交易交由验证部门进行核实，若核实结果确定当前交易为欺诈交易，可以对发起该交易的账户进行警告或者封锁等处理步骤。

若交易反欺诈分析模型和预存的欺诈交易识别规则对当前交易是否为风险交易的判断结果差异性较大时，则需要进一步对当前交易进行人工核查，
30 并根据核查结果检查交易反欺诈分析模型和预存的欺诈交易识别规则判断结果差别较大的原因，从而纠正交易反欺诈分析模型或欺诈交易识别规则。

上述欺诈交易判断方法还可以是，先将当前交易输入欺诈交易识别规则中，再将欺诈交易识别规则对于当前交易的识别结果作为交易反欺诈分析模型对于当前交易判断的参考因素，能够使得交易反欺诈分析模型更全面地对
35

当前交易进行分析。

上述实施例中，终端通过根据实际交易训练出的交易反欺诈分析模型与预存的欺诈交易识别规则结合起来对当前交易是否为欺诈交易进行判断，提高了对实际交易中发生的欺诈交易的判断的准确率。

5 在一些实施例中，请参见图 3，上述欺诈交易判断方法中的步骤 S202 获取当前交易之前，还可以包括模型训练的步骤，该模型训练的步骤可以包括：S302，获取样本数据。

其中，样本数据为用于训练交易反欺诈分析模型的交易数据，可以是与当前交易相关的历史数据，如当需要对今年的每一单交易数据进行欺诈性判
10 断，则可以采用上一年度的交易数据为样本数据。

具体地，在训练交易反欺诈分析模型时，需要先获取用于训练的样本数据。可选地，样本数据可以包括正样本数据和负样本数据；正样本数据是正常交易数据，由于大部分交易为正常交易，所以可以对正样本数据进行随机抽样，抽取一段时间内的正常交易的数据；负样本数据是通过业务核查后，
15 提取历史交易数据中发生欺诈的欺诈交易数据；其中，样本数据就可以包括交易数据、绑卡数据、开户数据等。

S304，对样本数据进行清洗，并从清洗后的样本数据中选择训练变量。

其中，训练变量是输入随机森林算法模型的变量，如交易金额、交易设备型号等变量。

20 具体地，对获取的样本数据进行清洗，按照预设的清洗规则筛出不满足需求的数据；例如，当苹果账户的样本数据与欺诈数据类型相似时，则剔除使用苹果账户进行支付的样本数据，以免影响模型的准确性。步骤 S202 中获取的样本数据为交易数据，每一笔交易可能包含多种变量，如交易金额、客户姓名、交易设备的 IP 号码、流水号等，而在训练交易反欺诈分析模型时只需要提取与交易欺诈判断相关的变量即可，此处终端提取与交易欺诈判断相关的变量需要先筛选出输入随机森林算法的训练变量。

可选地，可以通过 R 语言（一种计算机编译语言）中的 cor 函数（计算列与列之间的相关系数的函数），将样本数据中的多个变量剔除高相关性变量，对样本数据进行清洗。

30 S306，通过随机森林算法模型从训练变量中选择入模变量以及入模变量对应的出模变量。

其中，随机森林算法模型是用于从训练变量中选取入模变量的算法模型；随机森林是一个包含多个决策树的分类器；即用随机的方式建立一个森林，森林里面有很多的决策树组成，随机森林的每一棵决策树之间是没有关联的。
35 在得到森林之后，当有一个新的输入数据进入的时候，就让森林中的每一棵

决策树分别进行判断，通过多个决策树对输入数据进行分类。

入模变量是用于训练交易反欺诈分析模型的变量，是经过随机森林算法模型选择出的与交易欺诈判断相关的变量，如交易金额等。出模变量是与入模变量对应的变量，如入模变量为交易金额时，出模变量为交易金额大于 10 万元时，此交易为欺诈交易的概率为 70%。

具体地，将训练变量输入随机森林算法模型，通过该算法中的多个决策树，分析每个训练变量对交易欺诈概率的判断结果的重要性，最终得到重要性大于预设值的训练变量作为入模变量以及和入模变量对应的用于计算交易欺诈概率的出模变量。

S308，获取预设的初始神经网络模型。

具体地，步骤 S206 中选取入模变量以及入模变量对应的出模变量之后，则可以获取预设的初始神经网络模型对其进行训练。

S310，根据入模变量与入模变量对应的出模变量对初始神经网络模型进行训练得到交易反欺诈分析模型。

具体地，根据步骤 S306 中得到的入模变量以及入模变量对应的出模变量对初始神经网络进行训练，得到能够计算输入的当前交易的交易欺诈概率的交易反欺诈分析模型。

上述实施例中，将获取的样本数据进行清洗等处理后，按照训练好的随机森林算法模型选择入模变量以及与其对应的出模变量，对初始神经网络模型进行训练，得到能够准确判断输入的当前交易的交易欺诈概率的交易反欺诈分析模型；由于样本数据为与当前交易相关的历史交易数据，对当前交易的交易欺诈概率的计算更准确。

在一些实施例中，上述欺诈交易判断方法中的步骤 S304，即对样本数据进行清洗，并从清洗后的样本数据中选择训练变量的步骤，可以包括：

S402，获取内容为空的数据，并识别内容为空的数据对应的数据类型。

其中，内容空的数据可以是数据中的内容为 NULL 值的数据；数据类型是用于制定和获取对应替换逻辑的内容为空的数据的一个或多个类型，如离散型数据和连续型等。

具体地，获取样本数据后，为保证合理判定其中的内容为空的数据，避免出现数据遗漏的情况，需要判断样本数据中内容为空的数据是否无意义，而为对其进行判断，需要先识别内容为空的数据的数据类型，即识别出无意义的数据。

S404，获取数据类型获取对应的替换逻辑，并根据所获取的替换逻辑将样本数据中的内容为空的数据进行替换。

其中，替换逻辑是用于根据内容为空的数据的数据类型对其进行替换的

逻辑规则，可以根据经验制定得到；如在 R 语言中离散变量中 NULL 值均由字符 U 替换，连续型变量（如数值等）中 NULL 值均由数值 0 做替换等；在制定替换逻辑后可将其存储在预设位置中，该存储制定的替换逻辑的预设位置可以称为逻辑库，使用时根据关键字等规则从逻辑库中调取。

具体地，根据样本数据的数据类型，从逻辑库获取对应的替换逻辑，对样本数据中的内容为空的数据按照该替换逻辑进行对应的替换操作。

可选地，终端将 NULL 值占比高于预设比例以上的无实际含义的字段作为是内容为空的字段，终端可以直接移除；其中的预设比例可根据经验设定，如 30% 等。

S406，获取替换后的样本数据中的非高相关性变量作为第一变量。

其中，第一变量是从替换后的样本数据中选取的非高相关性变量，如姓名等；非高相关性变量是从样本数据中将高相关性变量筛除后得到的变量，可以通过按照业务操作制定相应的规则对样本数据中的变量的相关性进行分析，确定样本数据中多个变量之间的相关性关系，如姓名和姓氏等变量，在业务操作中作用相同，则可能为是高相关性变量。

具体地，步骤 S404 中得到的替换后样本数据可能包括相关性较高的重复变量，，选取其中非高相关性变量，继续后面的操作。

S408，计算第一变量的信息价值。

其中，信息价值（IV，information value）是自变量对目标变量影响程度的指标；第一变量的信息价值越大，该变量对判断交易是否为欺诈交易的结果影响越大。将分组后的第一变量进行 WOE（Weight of Evidence，证据权重）的转换，其转换公式为：

$$WOE_i = \ln(p_{yi}/p_{ni}) = \ln\left(\frac{\#y_i / \#y_T}{\#n_i / \#n_T}\right) = \ln\left(\frac{\#y_i / \#n_i}{\#y_T / \#n_T}\right)$$

(1)

其中 p_{yi} 是一组交易数据中欺诈交易与所有交易的比例， p_{ni} 是一组交易数据中正常交易与所有交易的比例， $\#y_i$ 是这个组中欺诈交易的数量， $\#n_i$ 是这个组中正常交易的数量， $\#y_T$ 是所有交易数据中所有欺诈交易的数量， $\#n_T$ 是所有交易数据中所有正常交易的数量。

一组第一变量的信息价值可根据上述 WOE 计算公式得出：

$$IV_i = (p_{yi} - p_{ni}) * WOE_i \quad (2)$$

则第一变量的 IV 值为所有组别第一变量的信息价值的累加。

具体地，在步骤 S306 中获取第一变量后，需要判断第一变量中是否所有的变量都对欺诈交易的判断结果存在影响，若存在影响，则可以作为训练交

易反欺诈分析模型的变量；若无影响，则可将其删除。可选地，可以通过引用 R 语言中的数据算法包来计算第一变量对应的信息价值。

S410，选取信息价值高于预设值的第一变量作为训练变量。

具体地，当第一变量的信息价值高于预设值时，则可以认为其对欺诈交易的判断结果存在影响，可以考虑将其作为训练交易反欺诈分析模型的入模变量。其中预设值可以通过大数据分析或者经验设置。

上述实施例中，通过对样本数据中内容为空的数据进行对应的替换操作，以及删除高相关性的变量并从中选取信息价值高于预设值的步骤，更为准确地为训练交易反欺诈分析模型选取入模变量，提高了模型训练的准确性和训练效率。

在一些实施例中，上述欺诈交易判断方法中的步骤 S304 对样本数据进行清洗，可以包括：获取样本数据中的第二变量，并获取第二变量对应的业务规则；根据业务规则从第二变量中选取业务作用的相似度大于预设值的第二变量，并从所业务作用相似度大于预设值的第二变量中选取其中一个作为清洗后的样本数据。

其中，第二变量是从样本数据中获取的用于进行相似度判断的变量；如交易金额等。

业务规则是用于计算多个变量之间相似度的设定好的规则；如当需要计算的变量为身份证号码、交易金额和出生年月时，可设定身份证号和出生年月的相似度为 90%，身份证号码和交易金额的相似度为 0%；业务规则设定好后可以存储在规则库中，根据关键字进行调用。

具体地，从样本数据中获取用于进行相似度判断的第二变量；且从设定好规则库中调用与第二变量相关的业务规则，根据业务规则计算第二变量之间的相似度，当两个或多个第二变量之间的相似度高于预设值时，则可以认为这些第二变量在业务活动中的作用相似，只保留一个进行后续的操作即可。

上述实施例中，根据业务规则对样本数据中的变量进行相似度计算，多个相似度较高的变量仅保留一个，减少在交易反欺诈分析模型训练和实际应用时的数据计算，提高了模型训练和应用的效率。

在一些实施例中，上述欺诈交易判断方法中的步骤 S304 对样本数据进行清洗，可以包括：获取样本数据中的第三变量；检测第三变量的变量类型；当变量类型为连续型，根据预设条件推理树获取递归分割算法，并根据递归分割算法对第三变量进行分段。

其中，第三变量是从样本数据中获取的，用于检测变量类型的变量；如交易金额等。

条件推理树（conditional inference trees, Ctree）是一种基于树的

分类算法，如 R 语言中的 plot、text 函数等。

递归 (Recursion) 指在函数的定义中使用函数自身的方法；而递归分割算法是基于递归算法对输入的变量进行多次分割的机器算法；即通过多次调用递归分割算法将第三变量分割为离散型变量，如交易金额为 0~100 万不等，
5 通过递归分割算法将其分割为 0 至 5 万一段、5 至 10 万一段的变量表示方法。

具体地，从样本数据中获取用于检测变量类型的第三变量；当检测到第三变量的变量类型为连续型时，根据预设条件推理树获取对第三变量进行分段的递归分割算法，然后根据递归分割算法对第三变量进行分段处理，得到便于训练初始神经网络模型的变量形式。

10 上述实施例中，通过将样本数据中的连续型变量进行分段，使得样本数据中的变量更符合模型训练的表示形式，便于训练初始神经网络模型。

在一些实施例中，上述欺诈交易判断方法中的步骤 S204 将当前交易输入交易反欺诈分析模型得到当前交易的交易欺诈概率之后，还可以包括：根据以下公式将交易欺诈概率转换成交易欺诈评分： $Score = A - B \log(odds)$ ；其中
15 $odds = p / (1 - p)$ ，Score 为交易欺诈评分，p 为交易欺诈概率，A 和 B 是预设常数；根据当前交易的交易欺诈概率与识别结果判断当前交易是否为欺诈交易，包括：根据当前交易的交易欺诈评分与识别结果判断当前交易是否为欺诈交易。

具体地，为将交易反欺诈分析模型对当前交易是否为欺诈交易的分析结果更直观地展现给技术人员，可以将其转换成交易欺诈评分，其转换公式为
20 $Score = A - B \log(odds)$ ，其中 $odds = p / (1 - p)$ ；Score 为交易欺诈评分，p 为交易欺诈概率，A 和 B 是预设常数，可以根据经验获得；评分可直观体现欺诈风险，高分值代表低风险，低分值代表高风险。

上述实施例中，通过将当前交易的交易欺诈概率根据入模变量获取该变量对应的欺诈评分，使得交易反欺诈分析模型的结果更加便于分析和查看。
25

在一些实施例中，上述欺诈交易判断方法还可以包括：获取验证交易，将验证交易输入交易反欺诈分析模型得到验证欺诈概率；获取验证交易对应的标准欺诈概率，计算验证欺诈概率与标准欺诈概率的差值；获取验证交易对应的标准欺诈概率，计算验证欺诈概率与标准欺诈概率的差值；当差值大于预设值时，根据标准欺诈概率纠正交易反欺诈分析模型。
30

其中，验证交易是用于对交易反欺诈分析模型进行验证的交易数据；如交易反欺诈分析模型是以上一年度的交易为样本数据训练的，则可以用本年度一月份的交易或从中随机抽样的交易为验证交易。

验证欺诈概率是通过交易反欺诈分析模型对验证交易进行判断后，得到
35 验证交易为欺诈交易的概率；验证欺诈概率与交易欺诈概率形式一致，可以

以百分比的形式展示，也可以采用其他数学表示方法。

标准欺诈概率是验证交易实际为欺诈交易的概率；其与验证欺诈概率形式一致，可以以百分比的形式展示，也可以采用其他数学表示方法。

具体地，从存储验证交易的地址读取验证交易，将获取到的验证交易输入到根据历史交易数据以及历史交易数据中的欺诈信息作为样本数据训练得到的神经网络模型或规则模型中，根据模型训练的规则，得到验证交易为验证交易的概率；然后获取到验证交易实际为欺诈交易的标准欺诈概率，将标准欺诈概率与验证欺诈概率相比较，当二者差值较小时，则证明此交易反欺诈分析模型准确性较高；当二者差值较大，则该交易反欺诈分析模型可能存在错误，根据标准欺诈概率对其纠正。

可选地，可以通过分层抽样方法、随机抽样方法分别将历史交易数据分段，如 2-8 分段，80%数据作为样本数据对交易反欺诈分析模型进行模型训练，20%的数据作为验证交易对交易反欺诈分析模型进行验证。或者，将所有的历史交易数据作为样本数据，如对上年度抽样后的交易数据，取样本数据日期之后的交易数据，如本年度一月份的交易数据，作为验证交易对交易反欺诈分析模型进行验证

上述实施例中，通过交易反欺诈分析模型的验证步骤能够保证模型对当前交易的欺诈概率判断的准确性。

应该理解的是，虽然图 2 至图 4 的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，图 2 至图 4 中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些子步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

在一些实施例中，如图 5 所示，提供了一种欺诈交易判断装置，包括：数据获取模块 100、概率分析模块 200、规则识别模块 300 和结果获取模块 400，其中：

数据获取模块 100，用于获取当前交易。

概率分析模块 200，用于将当前交易输入交易反欺诈分析模型得到当前交易的交易欺诈概率。

规则识别模块 300，用于通过预存的欺诈交易识别规则对当前交易进行识别得到识别结果。

结果获取模块 400，用于根据当前交易的交易欺诈概率与识别结果判断

当前交易是否为欺诈交易。

在一些实施例中，上述欺诈交易判断装置还可以包括：

样本获取模块，用于获取样本数据。

清洗模块，用于对样本数据进行清洗，并从清洗后的样本数据中选择训练变量。

变量选择模块，用于通过随机森林算法模型从训练变量中选择入模变量以及入模变量对应的出模变量。

初始模型获取模块，用于获取预设的初始神经网络模型。

模型训练模块，用于根据入模变量与入模变量对应的出模变量对初始神经网络模型进行训练得到交易反欺诈分析模型。

在一些实施例中，上述欺诈交易判断装置中的清洗模块可以包括：

空数据获取单元，用于获取内容为空的数据，并识别内容为空的数据对应的数据类型。

替换单元，用于获取数据类型获取对应的替换逻辑，并根据所获取的替换逻辑将样本数据中的内容为空的数据进行替换。

相关性分析单元，用于获取替换后的样本数据中的非高相关性变量作为第一变量。

价值计算单元，用于计算第一变量的信息价值。

训练变量选取单元，用于选取信息价值高于预设值的第一变量作为训练变量。

在一些实施例中，上述欺诈交易判断装置中的清洗模块可以包括：

业务规则获取单元，用于获取样本数据中的第二变量，并获取第二变量对应的业务规则。

变量相似度分析单元，用于根据业务规则从第二变量中选取业务作用的相似度大于预设值的第二变量，并从所业务作用相似度大于预设值的第二变量中选取其中一个作为清洗后的样本数据。

在一些实施例中，上述欺诈交易判断装置中的清洗模块可以包括：

样本变量获取单元，用于获取样本数据中的第三变量。

变量类型识别单元，用于检测第三变量的变量类型。

连续型变量分割单元，用于当变量类型为连续型，根据预设条件推理树获取递归分割算法，并根据递归分割算法对第三变量进行分段。

在一些实施例中，上述欺诈交易判断装置还可以包括：

评分转化模块，用于根据以下公式将交易欺诈概率转换成交易欺诈评分：

$$\text{Score} = A - B \log(\text{odds})$$

其中 $\text{odds} = p / (1 - p)$ ，Score 为交易欺诈评分，p 为交易欺诈概率，A 和 B

是预设常数。

则结果获取模块 400，可以用于：根据当前交易的交易欺诈评分与识别结果判断当前交易是否为欺诈交易。

在一些实施例中，上述欺诈交易判断装置还可以包括：

5 验证交易获取模块，用于获取验证交易。

验证欺诈概率获取模块，用于将验证交易输入交易反欺诈分析模型得到验证欺诈概率。

差值计算模块，用于获取验证交易对应的标准欺诈概率，计算验证欺诈概率与标准欺诈概率的差值。

10 纠正模块，用于当差值大于预设值时，根据标准欺诈概率纠正交易反欺诈分析模型。

关于欺诈交易判断装置的具体限定可以参见上文中对于欺诈交易判断方法的限定，在此不再赘述。上述欺诈交易判断装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

在一些实施例中，提供了一种计算机设备，该计算机设备可以是终端，其内部结构图可以如图 6 所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口、显示屏和输入装置。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存存储。该非易失性存储介质存储有操作系统和计算机可读指令。该内存存储为非易失性存储介质中的操作系统和计算机可读指令的运行提供环境。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机可读指令被处理器执行时以实现一种欺诈交易判断方法。该计算机设备的显示屏可以是液晶显示屏或者电子墨水显示屏，该计算机设备的输入装置可以是显示屏上覆盖的触摸层，也可以是计算机设备外壳上设置的按键、轨迹球或触控板，还可以是外接的键盘、触控板或鼠标等。

本领域技术人员可以理解，图 6 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

一种计算机设备，包括存储器和一个或多个处理器，存储器中储存有计算机可读指令，计算机可读指令被处理器执行时，使得一个或多个处理器执行以下步骤：

35 获取当前交易；

将当前交易输入交易反欺诈分析模型得到当前交易的交易欺诈概率；
通过预存的欺诈交易识别规则对当前交易进行识别得到识别结果；及
根据当前交易的交易欺诈概率与识别结果判断当前交易是否为欺诈交易。

5 在一些实施例中，处理器执行计算机可读指令时实现的获取当前交易之前，还可以包括：

获取样本数据；

对样本数据进行清洗，并从清洗后的样本数据中选择训练变量；

10 通过随机森林算法模型从训练变量中选择入模变量以及入模变量对应的出模变量；

获取预设的初始神经网络模型；及

根据入模变量与入模变量对应的出模变量对初始神经网络模型进行训练得到交易反欺诈分析模型。

15 在一些实施例中，处理器执行计算机可读指令时实现的对样本数据进行清洗，并从清洗后的样本数据中选择训练变量，可以包括：

获取内容为空的数据，并识别内容为空的数据对应的数据类型；

获取数据类型获取对应的替换逻辑，并根据所获取的替换逻辑将样本数据中的内容为空的数据进行替换；

获取替换后的样本数据中的非高相关性变量作为第一变量；

20 计算第一变量的信息价值；及

选取信息价值高于预设值的第一变量作为训练变量。

在一些实施例中，处理器执行计算机可读指令时实现的对样本数据进行清洗，可以包括：

获取样本数据中的第二变量，并获取第二变量对应的业务规则；及

25 根据业务规则从第二变量中选取业务作用的相似度大于预设值的第二变量，并从所业务作用相似度大于预设值的第二变量中选取其中一个作为清洗后的样本数据。

在一些实施例中，处理器执行计算机可读指令时实现的对样本数据进行清洗，可以包括：

30 获取样本数据中的第三变量；

检测第三变量的变量类型；及

当变量类型为连续型，根据预设条件推理树获取递归分割算法，并根据递归分割算法对第三变量进行分段。

35 在一些实施例中，处理器执行计算机可读指令时实现的将当前交易输入交易反欺诈分析模型得到当前交易的交易欺诈概率之后，还可以包括：

根据以下公式将交易欺诈概率转换成交易欺诈评分：
 $Score = A - B \log(odds)$;

其中 $odds = p / (1 - p)$ ，Score 为交易欺诈评分，p 为交易欺诈概率，A 和 B 是预设常数；及

5 处理器执行计算机可读指令时实现的根据当前交易的交易欺诈概率与识别结果判断当前交易是否为欺诈交易，可以包括：

根据当前交易的交易欺诈评分与识别结果判断当前交易是否为欺诈交易。

10 在一些实施例中，该处理器执行计算机可读指令时还可以实现以下步骤：
获取验证交易；

将验证交易输入交易反欺诈分析模型得到验证欺诈概率；

获取验证交易对应的标准欺诈概率，计算验证欺诈概率与标准欺诈概率的差值；及

当差值大于预设值时，根据标准欺诈概率纠正交易反欺诈分析模型。

15 一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：

获取当前交易；

将当前交易输入交易反欺诈分析模型得到当前交易的交易欺诈概率；

20 通过预存的欺诈交易识别规则对当前交易进行识别得到识别结果；及
根据当前交易的交易欺诈概率与识别结果判断当前交易是否为欺诈交易。

在一些实施例中，计算机可读指令被处理器执行时实现的获取当前交易之前，还可以包括：

25 获取样本数据；

对样本数据进行清洗，并从清洗后的样本数据中选择训练变量；

通过随机森林算法模型从训练变量中选择入模变量以及入模变量对应的出模变量；

获取预设的初始神经网络模型；及

30 根据入模变量与入模变量对应的出模变量对初始神经网络模型进行训练得到交易反欺诈分析模型。

在一些实施例中，计算机可读指令被处理器执行时实现的对样本数据进行清洗，并从清洗后的样本数据中选择训练变量，可以包括：

获取内容为空的数据，并识别内容为空的数据对应的数据类型；

35 获取数据类型获取对应的替换逻辑，并根据所获取的替换逻辑将样本数

据中的内容为空的数据进行替换；

获取替换后的样本数据中的非高相关性变量作为第一变量；

计算第一变量的信息价值；及

选取信息价值高于预设值的第一变量作为训练变量。

5 在一些实施例中，计算机可读指令被处理器执行时实现的对样本数据进行清洗，可以包括：

获取样本数据中的第二变量，并获取第二变量对应的业务规则；及

10 根据业务规则从第二变量中选取业务作用的相似度大于预设值的第二变量，并从所业务作用相似度大于预设值的第二变量中选取其中一个作为清洗后的样本数据。

在一些实施例中，计算机可读指令被处理器执行时实现的对样本数据进行清洗，可以包括：

获取样本数据中的第三变量；

检测第三变量的变量类型；及

15 当变量类型为连续型，根据预设条件推理树获取递归分割算法，并根据递归分割算法对第三变量进行分段。

在一些实施例中，计算机可读指令被处理器执行时实现的将当前交易输入交易反欺诈分析模型得到当前交易的交易欺诈概率之后，还可以包括：

根据以下公式将交易欺诈概率转换成交易欺诈评分：

20 $Score = A - B \log(odds)$ ；

其中 $odds = p / (1 - p)$ ，Score 为交易欺诈评分，p 为交易欺诈概率，A 和 B 是预设常数；及

计算机可读指令被处理器执行时实现的根据当前交易的交易欺诈概率与识别结果判断当前交易是否为欺诈交易，可以包括：

25 根据当前交易的交易欺诈评分与识别结果判断当前交易是否为欺诈交易。

在一些实施例中，计算机可读指令被处理器执行时还可以实现以下步骤：
获取验证交易；

将验证交易输入交易反欺诈分析模型得到验证欺诈概率；

30 获取验证交易对应的标准欺诈概率，计算验证欺诈概率与标准欺诈概率的差值；及

当差值大于预设值时，根据标准欺诈概率纠正交易反欺诈分析模型。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一非易失性计算机可读取存储介质中，该计算机可读指令在
35

执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器（ROM）、可编程 ROM（PROM）、电可编程 ROM（EPROM）、电可擦除可编程 ROM（EEPROM）或闪存。易失性存储器可包括随机存取存储器（RAM）或者外部高速缓冲存储器。作为说明而非局限，RAM 以多种形式可得，诸如静态 RAM（SRAM）、动态 RAM（DRAM）、同步 DRAM（SDRAM）、双数据率 SDRAM（DDRSDRAM）、增强型 SDRAM（ESDRAM）、同步链路（Synchlink） DRAM（SLDRAM）、存储器总线（Rambus）直接 RAM（RDRAM）、直接存储器总线动态 RAM（DRDRAM）、以及存储器总线动态 RAM（RDRAM）等。

以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

权利要求书

1、一种欺诈交易判断方法，所述方法包括：

获取当前交易；

将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈概率；

5 通过预存的欺诈交易识别规则对所述当前交易进行识别得到识别结果；
及

根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是否为欺诈交易。

2、根据权利要求 1 所述的方法，其特征在于，所述获取当前交易之前，
10 还包括：

获取样本数据；

对所述样本数据进行清洗，并从清洗后的样本数据中选择训练变量；

通过随机森林算法模型从所述训练变量中选择入模变量以及所述入模变量对应的出模变量；

15 获取预设的初始神经网络模型；及

根据所述入模变量与所述入模变量对应的出模变量对初始神经网络模型进行训练得到交易反欺诈分析模型。

3、根据权利要求 2 所述的方法，其特征在于，所述对所述样本数据进行清洗，并从清洗后的样本数据中选择训练变量，包括：

20 获取内容为空的数据，并识别所述内容为空的数据对应的数据类型；

获取所述数据类型获取对应的替换逻辑，并根据所获取的替换逻辑将所述样本数据中的所述内容为空的数据进行替换；

获取替换后的所述样本数据中的非高相关性变量作为第一变量；

计算所述第一变量的信息价值；及

25 选取所述信息价值高于预设值的所述第一变量作为训练变量。

4、根据权利要求 2 所述的方法，其特征在于，所述对所述样本数据进行清洗，包括：

获取样本数据中的第二变量，并获取所述第二变量对应的业务规则；及

30 根据所述业务规则从所述第二变量中选取业务作用的相似度大于预设值的第二变量，并从所述业务作用相似度大于预设值的第二变量中选取其中一个作为清洗后的样本数据。

5、根据权利要求 2 所述的方法，其特征在于，所述对所述样本数据进行清洗，包括：

获取所述样本数据中的第三变量；

检测所述第三变量的变量类型；及

当所述变量类型为连续型，根据预设条件推理树获取递归分割算法，并根据所述递归分割算法对所述第三变量进行分段。

6、根据权利要求 1 所述的方法，其特征在于，所述将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈概率之后，还包括：

根据以下公式将所述交易欺诈概率转换成交易欺诈评分：

$$\text{Score} = A - B \log(\text{odds})$$

其中 $\text{odds} = p / (1 - p)$ ，Score 为交易欺诈评分，p 为交易欺诈概率，A 和 B 是预设常数；及

所述根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是否为欺诈交易，包括：

根据所述当前交易的交易欺诈评分与所述识别结果判断所述当前交易是否为欺诈交易。

7、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

获取验证交易；

将所述验证交易输入所述交易反欺诈分析模型得到验证欺诈概率；

获取所述验证交易对应的标准欺诈概率，计算所述验证欺诈概率与所述标准欺诈概率的差值；及

当所述差值大于预设值时，根据所述标准欺诈概率纠正所述交易反欺诈分析模型。

8、一种欺诈交易判断装置，所述装置包括：

数据获取模块，用于获取当前交易；

概率分析模块，用于将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈概率；

规则识别模块，用于通过预存的欺诈交易识别规则对所述当前交易进行识别得到识别结果；及

结果获取模块，用于根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是否为欺诈交易。

9、根据权利要求 8 所述的装置，其特征在于，所述装置还包括：

样本获取模块，用于获取样本数据；

清洗模块，用于对所述样本数据进行清洗，并从清洗后的样本数据中选择训练变量；

变量选择模块，用于通过随机森林算法模型从所述训练变量中选择入模变量以及所述入模变量对应的出模变量；

初始模型获取模块，用于获取预设的初始神经网络模型；及
模型训练模块，用于根据所述入模变量与所述入模变量对应的出模变量对初始神经网络模型进行训练得到交易反欺诈分析模型。

10、一种计算机设备，包括存储器及一个或多个处理器，所述存储器中
5 储存有计算机可读指令，所述计算机可读指令被所述一个或多个处理器执行时，使得所述一个或多个处理器执行以下步骤：

获取当前交易；

将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈
概率；

10 通过预存的欺诈交易识别规则对所述当前交易进行识别得到识别结果；
及

根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是
否为欺诈交易。

11、根据权利要求 10 所述的计算机设备，其特征在于，所述处理器执行
15 所述计算机可读指令时实现的所述获取当前交易之前，还包括：

获取样本数据；

对所述样本数据进行清洗，并从清洗后的样本数据中选择训练变量；

通过随机森林算法模型从所述训练变量中选择入模变量以及所述入模变
量对应的出模变量；

20 获取预设的初始神经网络模型；及

根据所述入模变量与所述入模变量对应的出模变量对初始神经网络模型
进行训练得到交易反欺诈分析模型。

12、根据权利要求 11 所述的计算机设备，其特征在于，所述处理器执行
25 所述计算机可读指令时实现的所述对所述样本数据进行清洗，并从清洗后的
样本数据中选择训练变量，包括：

获取内容为空的数据，并识别所述内容为空的数据对应的数据类型；

获取所述数据类型获取对应的替换逻辑，并根据所获取的替换逻辑将所
述样本数据中的所述内容为空的数据进行替换；

获取替换后的所述样本数据中的非高相关性变量作为第一变量；

30 计算所述第一变量的信息价值；及

选取所述信息价值高于预设值的所述第一变量作为训练变量。

13、根据权利要求 11 所述的计算机设备，其特征在于，所述处理器执行
所述计算机可读指令时实现的所述对所述样本数据进行清洗，包括：

获取样本数据中的第二变量，并获取所述第二变量对应的业务规则；及

35 根据所述业务规则从所述第二变量中选取业务作用的相似度大于预设值

的第二变量，并从所业务作用相似度大于预设值的第二变量中选取其中一个作为清洗后的样本数据。

14、根据权利要求 11 所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时实现的所述对所述样本数据进行清洗，包括：

5 获取所述样本数据中的第三变量；

检测所述第三变量的变量类型；及

当所述变量类型为连续型，根据预设条件推理树获取递归分割算法，并根据所述递归分割算法对所述第三变量进行分段。

15、根据权利要求 10 所述的计算机设备，其特征在于，所述处理器执行
10 所述计算机可读指令时实现的所述将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈概率之后，还包括：

根据以下公式将所述交易欺诈概率转换成交易欺诈评分：

$$\text{Score} = A - B \log(\text{odds})$$

15 其中 $\text{odds} = p / (1 - p)$ ，Score 为交易欺诈评分，p 为交易欺诈概率，A 和 B 是预设常数；及

所述根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是否为欺诈交易，包括：

20 根据所述当前交易的交易欺诈评分与所述识别结果判断所述当前交易是否为欺诈交易。

16、根据权利要求 10 所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：

获取验证交易；

将所述验证交易输入所述交易反欺诈分析模型得到验证欺诈概率；

25 获取所述验证交易对应的标准欺诈概率，计算所述验证欺诈概率与所述标准欺诈概率的差值；及

当所述差值大于预设值时，根据所述标准欺诈概率纠正所述交易反欺诈分析模型。

17、一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行以下步骤：

获取当前交易；

30 将所述当前交易输入交易反欺诈分析模型得到所述当前交易的交易欺诈概率；

通过预存的欺诈交易识别规则对所述当前交易进行识别得到识别结果；

及

根据所述当前交易的交易欺诈概率与所述识别结果判断所述当前交易是否为欺诈交易。

18、根据权利要求 17 所述的存储介质，其特征在于，所述计算机可读指令被所述处理器执行时实现的所述获取当前交易之前，还包括：

获取样本数据；

5 对所述样本数据进行清洗，并从清洗后的样本数据中选择训练变量；

通过随机森林算法模型从所述训练变量中选择入模变量以及所述入模变量对应的出模变量；

获取预设的初始神经网络模型；及

根据所述入模变量与所述入模变量对应的出模变量对初始神经网络模型进行训练得到交易反欺诈分析模型。

10 19、根据权利要求 18 所述的存储介质，其特征在于，所述计算机可读指令被所述处理器执行时实现的所述对所述样本数据进行清洗，并从清洗后的样本数据中选择训练变量，包括：

获取内容为空的数据，并识别所述内容为空的数据对应的数据类型；

获取所述数据类型获取对应的替换逻辑，并根据所获取的替换逻辑将所述样本数据中的所述内容为空的数据进行替换；

15 获取替换后的所述样本数据中的非高相关性变量作为第一变量；

计算所述第一变量的信息价值；及

选取所述信息价值高于预设值的所述第一变量作为训练变量。

20、根据权利要求 18 所述的存储介质，其特征在于，所述计算机可读指令被所述处理器执行时实现的所述对所述样本数据进行清洗，并从清洗后的样本数据中选择训练变量，包括：

20 获取样本数据中的第二变量，并获取所述第二变量对应的业务规则；及

根据所述业务规则从所述第二变量中选取业务作用的相似度大于预设值的第二变量，并从所业务作用相似度大于预设值的第二变量中选取其中一个作为清洗后的样本数据。

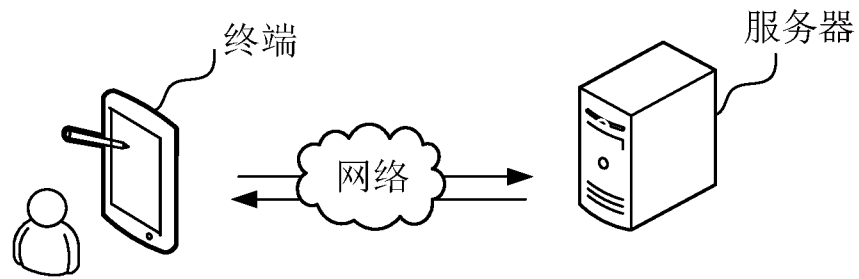


图 1

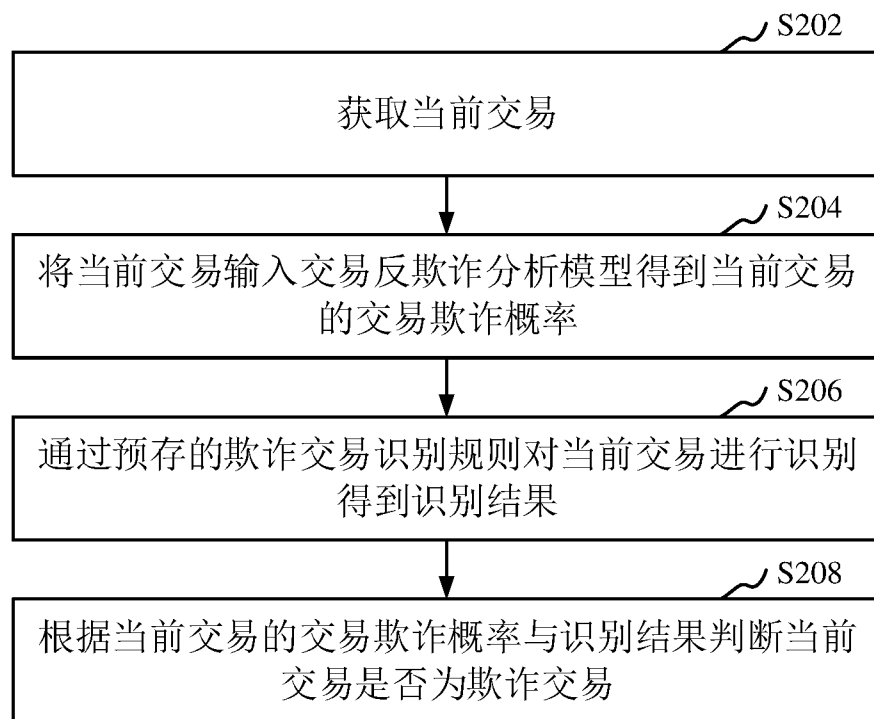


图 2

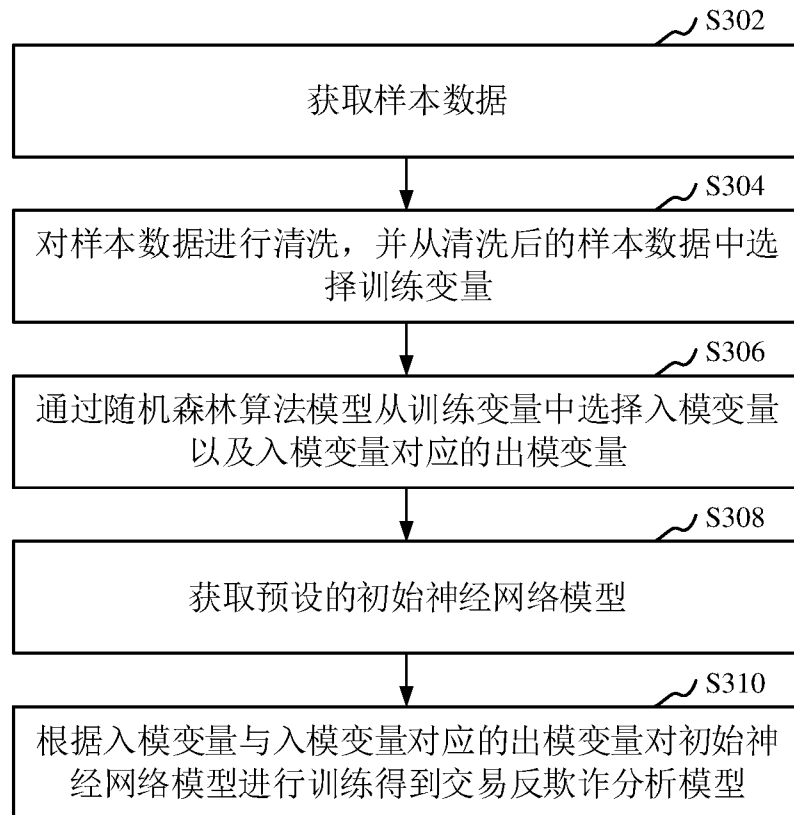


图 3

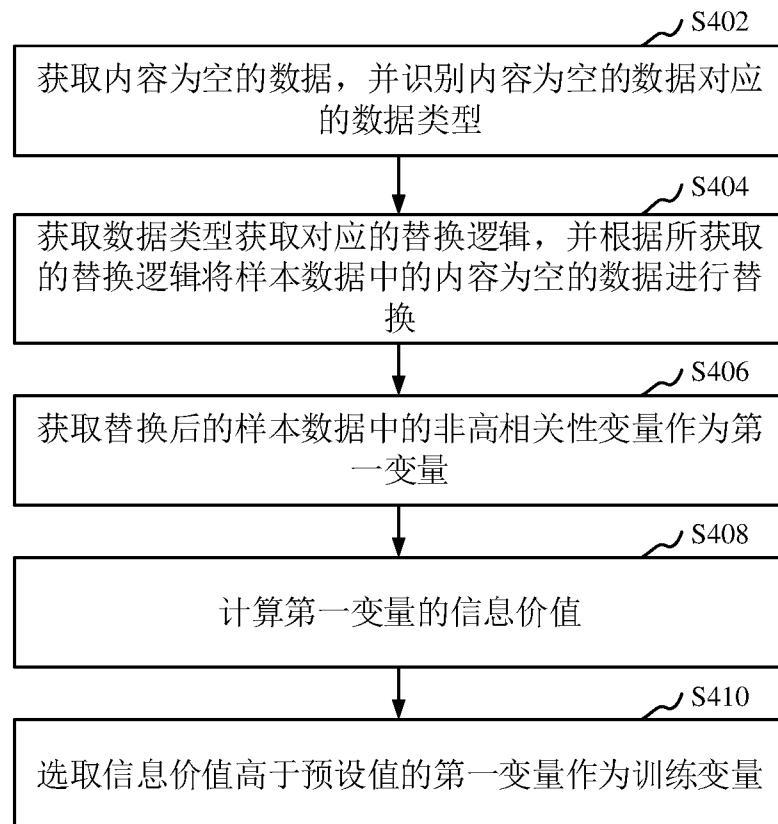


图 4

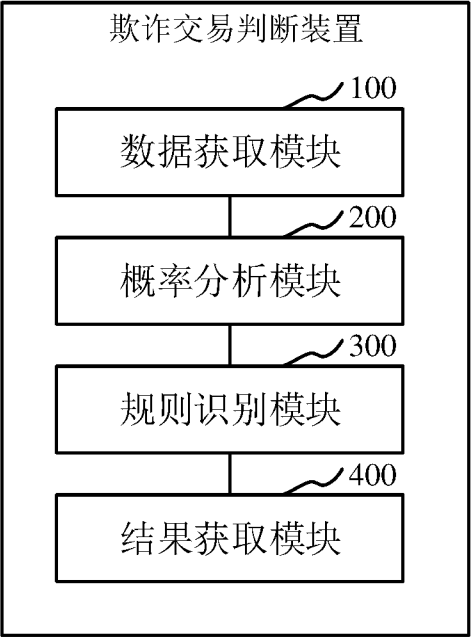


图 5

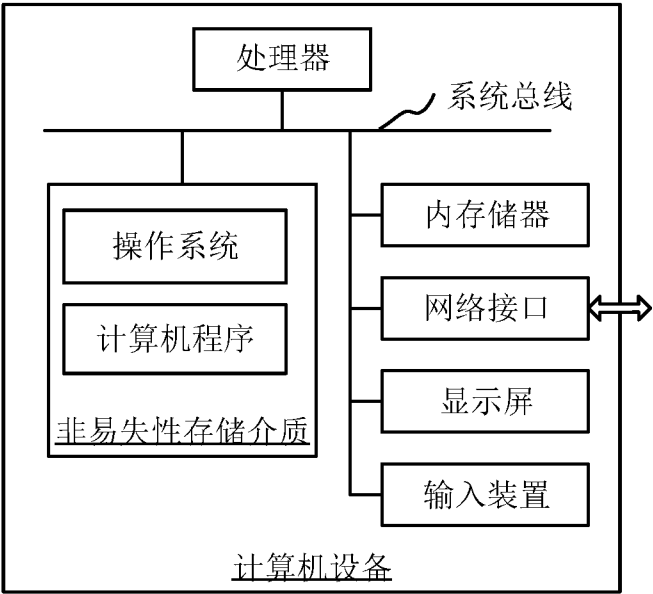


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/070159

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 30/00(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q 30/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNKI, DWPI, SIPOABS: 交易, 贸易, 欺诈, 欺骗, 诈骗, 分析, 模型, 识别, 规则, 概率, 判断, 训练, 逻辑, BUSINESS, TRADE, CHEATING, FRAUD, DECEIVE, ANALYSE, MODEL, IDENTIFY, RULE, PROBABILITY, JUDGEMENT, TRAINING, LOGIC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 108717638 A (ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) 30 October 2018 (2018-10-30) claims 1-10, and description, paragraphs 055-186	1-20
X	CN 105005901 A (BIOVOICE INFORMATION TECHNOLOGY CO., LTD.) 28 October 2015 (2015-10-28) claims 1-4, description, paragraphs 13-38, and figures 1-2	1-20
A	CN 107679862 A (CHINA UNIONPAY CO., LTD.) 09 February 2018 (2018-02-09) entire document	1-20

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

18 March 2019

Date of mailing of the international search report

02 April 2019

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/070159

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	108717638	A	30 October 2018	None	
CN	105005901	A	28 October 2015	None	
CN	107679862	A	09 February 2018	None	

国际检索报告

国际申请号

PCT/CN2019/070159

A. 主题的分类 G06Q 30/00 (2012.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类														
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) G06Q 30/- 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNABS, CNKI, DWPI, SIPOABS: 交易, 贸易, 欺诈, 欺骗, 诈骗, 分析, 模型, 识别, 规则, 概率, 判断, 训练, 逻辑, BUSINESS, TRADE, CHEATING, FRAUD, DECEIVE, ANALYSE, MODEL, IDENTIFY, RULE, PROBABILITY, JUDGEMENT, TRAINING, LOGIC														
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 108717638 A (深圳壹账通智能科技有限公司) 2018年 10月 30日 (2018 - 10 - 30) 权利要求1-10, 说明书第055-186段</td> <td>1-20</td> </tr> <tr> <td>X</td> <td>CN 105005901 A (厦门快商通信息技术有限公司) 2015年 10月 28日 (2015 - 10 - 28) 权利要求1-4, 说明书第13-38段、附图1-2</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 107679862 A (中国银联股份有限公司) 2018年 2月 9日 (2018 - 02 - 09) 全文</td> <td>1-20</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 108717638 A (深圳壹账通智能科技有限公司) 2018年 10月 30日 (2018 - 10 - 30) 权利要求1-10, 说明书第055-186段	1-20	X	CN 105005901 A (厦门快商通信息技术有限公司) 2015年 10月 28日 (2015 - 10 - 28) 权利要求1-4, 说明书第13-38段、附图1-2	1-20	A	CN 107679862 A (中国银联股份有限公司) 2018年 2月 9日 (2018 - 02 - 09) 全文	1-20
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求												
PX	CN 108717638 A (深圳壹账通智能科技有限公司) 2018年 10月 30日 (2018 - 10 - 30) 权利要求1-10, 说明书第055-186段	1-20												
X	CN 105005901 A (厦门快商通信息技术有限公司) 2015年 10月 28日 (2015 - 10 - 28) 权利要求1-4, 说明书第13-38段、附图1-2	1-20												
A	CN 107679862 A (中国银联股份有限公司) 2018年 2月 9日 (2018 - 02 - 09) 全文	1-20												
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。														
<table border="0"> <tr> <td> * 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 </td> <td> “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件 </td> </tr> </table>			* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件										
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件													
国际检索实际完成的日期	国际检索报告邮寄日期													
2019年 3月 18日	2019年 4月 2日													
ISA/CN的名称和邮寄地址	受权官员													
中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	王少锋													
传真号 (86-10)62019451	电话号码 86-(010)-62411714													

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/070159

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	108717638	A	2018年 10月 30日	无	
CN	105005901	A	2015年 10月 28日	无	
CN	107679862	A	2018年 2月 9日	无	