(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
2020 年 4 月 30 日 (30.04.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/082559 A1

(51) 国际专利分类号:
*G06Q 30/06* (2012.01)

(21) 国际申请号: PCT/CN2018/122745

(22) 国际申请日: 2018 年 12 月 21 日 (21.12.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811254500.2 2018年10月25日 (25.10.2018) 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 518000 (CN)。

(72) 发明人: 魏晓茹 (WEI, Xiaoru); 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 518000 (CN)。 郑成凯 (ZHENG, Chengkai); 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 518000 (CN)。

(74) 代理人: 深圳市世纪恒程知识产权代理事务所 (CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区粤海街道高新技术产业园北区松坪山路3号奥特讯电力大厦201, Guangdong 518057 (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,

(54) **Title:** RISK DETECTION METHOD, APPARATUS AND DEVICE BASED ON ASSOCIATION GRAPH, AND STORAGE MEDIUM

(54) **发明名称**: 基于关联图谱的风险检测方法、装置、设备及存储介质

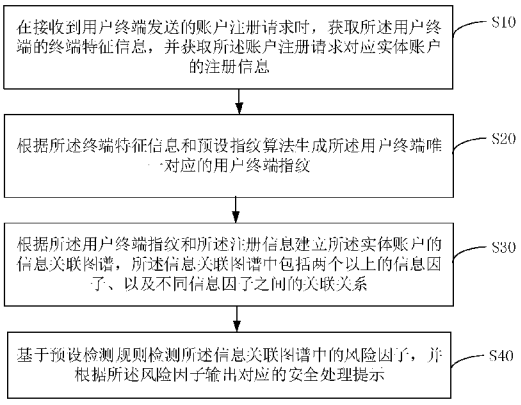


图 2

S10 When an account registration request sent by a user terminal is received, acquire terminal feature information of the user terminal, and acquire registration information of an entity account corresponding to the account registration request

S20 Generate, according to the terminal feature information and a pre-set fingerprint algorithm, a user terminal fingerprint uniquely corresponding to the user terminal

S30 Establish an information association graph of the entity account according to the user terminal fingerprint and the registration information, wherein the information association graph comprises two or more information factors and an association relationship between different information factors

S40 Detect a risk factor in the information association graph based on a pre-set detection rule, and output a corresponding security processing prompt according to the risk factor

(57) **Abstract:** A risk detection method, apparatus and device based on a knowledge graph, and a readable storage medium. The method comprises: when a user carries out account registration, collecting related data of the user, and integrating the data by means of an association graph (knowledge graph), so that it is convenient for merchants or risk control personnel to know the association between pieces of information; and then carrying out risk detection according to the association graph, such that the user data is analyzed by means of knowledge relation analysis so as to predict a potential service risk, thereby realizing early warning of an electronic commerce risk, and improving the risk detection capability and the service security.

(57) **摘要**: 一种基于知识图谱的风险检测方法、装置、设备及可读存储介质，在用户进行账户注册时即收集用户的相关数据，然后通过关联图谱(知识图谱)的方式对这些数据进行整合，方便商家或风控人员了解各项信息之间的关联性；再根据该关联图谱进行风险检测，从而以知识关系分析的方式对用户数据进行分析，以对潜在业务风险进行预测，实现了电子商务风险预警，提高风险检测的能力和业务安全性。

WO 2020/082559 A1

[见续页]

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, 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))。

# 基于关联图谱的风险检测方法、装置、设备及存储介质

本申请要求于 2018 年 10 月 25 日提交中国专利局、申请号为201811254500.2、发明名称为“基于关联图谱的风险检测方法、装置、设备及存储介质”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

本申请涉及知识图谱技术领域，尤其涉及一种基于关联图谱的风险检测方法、装置、设备及存储介质。

## 背景技术

随着网络技术进步，电子商务蓬勃发展，同时也对交易安全性提出了越来越高的要求；对商家而言，对风险账户进行及时处理，有利于维护电子商务活动的正常进行。但目前的电子商务活动中，主要是在遭受欺诈时进行被动的防御和补救处理，这种业务安全处理方法缺乏提前的风险评估，无法在欺诈发生前提前对风险进行预测，也就不能有效的进行风险监控处理。

## 发明内容

本申请的主要目的在于提供一种基于关联图谱的风险检测方法、装置、设备及存储介质，旨在实现对业务风险监控，提高业务安全性。

为实现上述目的，本申请提供一种基于关联图谱的风险检测方法，所述风险检测方法包括：

在接收到用户终端发送的账户注册请求时，获取所述用户终端的终端特征信息，并获取所述账户注册请求对应实体账户的注册信息；

根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹；

根据所述用户终端指纹和所述注册信息建立所述实体账户的信

息关联图谱，所述信息关联图谱中包括两个以上的信息因子、以及不同信息因子之间的关联关系；

基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示。

此外，为实现上述目的，本申请还提供一种基于关联图谱的风险检测装置，所述风险检测装置包括：

信息获取模块，用于在接收到用户终端发送的账户注册请求时，获取所述用户终端的终端特征信息，并获取所述账户注册请求对应实体账户的注册信息；

指纹生成模块，用于根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹；

图谱建立模块，用于根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱，所述信息关联图谱中包括两个以上的信息因子、以及不同信息因子之间的关联关系；

风险检测模块，用于基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示。

此外，为实现上述目的，本申请还提供一种基于关联图谱的风险检测设备，所述风险检测设备包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的计算机可读指令，其中所述计算机可读指令被所述处理器执行时，实现如上述的基于关联图谱的风险检测方法的步骤。

此外，为实现上述目的，本申请还提供一种存储介质，所述存储介质上存储有计算机可读指令，其中所述计算机可读指令被处理器执行时，实现如上述的基于关联图谱的风险检测方法的步骤。

本申请在用户进行账户注册时即收集用户的相关数据，然后通过关联图谱（知识图谱）的方式对这些数据进行整合，方便商家或风控人员了解各项信息之间的关联性；再根据该关联图谱进行风险检测，从而以知识关系分析的方式对用户数据进行分析，以对潜在业务风险进行预测，实现了电子商务风险预警，提高风险检测的能力和业务安全性。

## 附图说明

图1为本申请实施例方案中涉及的基于关联图谱的风险检测设备的硬件结构示意图；

图2为本申请基于关联图谱的风险检测方法第一实施例的流程示意图；

图3为本申请基于关联图谱的风险检测装置第一实施例的功能模块示意图。

本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

## 具体实施方式

应当理解，此处所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。

本申请实施例涉及的基于关联图谱的风险检测方法主要应用于基于关联图谱的风险检测设备，该风险检测设备可以是个人计算机（personal computer，PC）、笔记本电脑、服务器等具有数据处理功能的设备。

参照图 1，图 1 为本申请实施例方案中涉及的基于关联图谱的风险检测设备的硬件结构示意图。本申请实施例中，该风险检测设备可以包括处理器 1001( 例如中央处理器 Central Processing Unit ,CPU )，通信总线 1002 ,用户接口 1003 ,网络接口 1004 ,存储器 1005。其中，通信总线 1002 用于实现这些组件之间的连接通信 ;用户接口 1003 可以包括显示屏 ( Display )、输入单元比如键盘 ( Keyboard ) ; 网络接口 1004 可选的可以包括标准的有线接口、无线接口（如无线保真 WIreless-FIdelity，WI-FI 接口）; 存储器 1005 可以是高速随机存取存储器（random access memory，RAM），也可以是稳定的存储器（non-volatile memory），例如磁盘存储器，存储器 1005 可选的还可以是独立于前述处理器 1001 的存储装置。本领域技术人员可以理解，图 1 中示出的硬件结构并不构成对本申请的限定 ,可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

继续参照图 1，图 1 中作为一种计算机可读存储介质的存储器 1005 可以包括操作系统、网络通信模块以及计算机可读指令。在图 1 中，网络通信模块可用于连接数据库，与数据库进行数据通信；而处理器 1001 可以调用存储器 1005 中存储的计算机可读指令，并执行本申请实施例提供的基于关联图谱的风险检测方法。

本申请实施例提供了一种基于关联图谱的风险检测方法。

参照图 2，图 2 为本申请基于关联图谱的风险检测方法第一实施例的流程示意图。

本实施例中，所述风险检测方法包括以下步骤：

步骤 S10，在接收到用户终端发送的账户注册请求时，获取所述用户终端的终端特征信息，并获取所述账户注册请求对应实体账户的注册信息；

随着网络技术进步，电子商务蓬勃发展，同时也对交易安全性提出了越来越高的要求；对商家而言，对风险账户进行及时处理，有利于维护电子商务活动的正常进行。但目前的电子商务活动中，主要是在遭受欺诈时进行被动的防御和补救处理，这种业务安全处理方法缺乏提前的风险评估，无法在欺诈发生前提前对风险进行预测，也就不能有效的进行风险监控处理。对此，本实施例中提出一种基于关联图谱的风险检测方法，在用户进行账户注册时即收集用户的相关数据，然后通过关联图谱（智慧图谱）的方式对这些数据进行整合，方便商家或风控人员了解各项信息之间的关联性；再根据该关联图谱进行风险检测，从而以大数据分析的方式对风险进行预测，实现了电子商务风险预警，有利于维护业务安全。

本实施例中基于关联图谱的风险检测方法是由基于关联图谱的风险检测设备实现的，该风险检测设备以检测服务器为例进行说明。本实施例中，用户在进行电子商务活动前，首先需要通过用户终端（如个人电脑 PC、笔记本电脑、手机、平板电脑等）上进行账户注册操作，用户终端则根据用户的操作向检测服务器发送对应的账户注册请求。检测服务器在接收到用户终端发送的账户注册请求时，将会获取该用户终端的终端特征信息，该终端特征信息可以包括终端机型特征

（如终端品牌、终端型号、生产时间等）、终端操作系统 OS 特征（如操作系统类型、操作系统版本、是否越狱等）、浏览器特征（如浏览器类型、浏览器版本、用户代理 UA、插件配置、Canvas 特征等）、传感器特征（如重力传感器特征、加速传感器特征等）、设备配置特征（如网络配置、系统 flash 的配置等）等。对于上述终端特征信息的获取，可以是检测服务器在得到用户授权后，通过安装在该用户终端中的特征获取 SDK（Software Development Kit，软件开发工具包）或其它技术抓取用户终端的终端特征信息；也可以是检测服务器在得到用户的授权后，从运营商处获取该用户终端的终端特征信息。

本实施例中，检测服务器在接收到账户注册请求时，还将根据该账户注册请求获取对应实体账户的注册信息，以将该注册信息与用户注册的实体账户进行绑定，完成注册操作。其中，这些注册信息又可以包括个人信息和环境信息；个人信息包括用户名、手机号、邮箱、身份证号、银行卡号、第三方支付平台账户等；环境信息包括注册时间、用户终端当前的用户终端 IP 地址（Internet Protocol Address，互联网协议地址）、终端 GPS 地址等。对于这些注册信息，可以是用户在通过用户终端进行账户注册操作时进行录入，由用户终端发送至检测服务器；也可以是检测服务器主动检测得到。

步骤 S20，根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹；

本实施例中，检测服务器在得到用户终端的终端特征信息和注册信息时，将根据该终端特征信息和预设指纹算法生成该用户终端唯一对应的用户终端指纹；该用户终端指纹是可以用于唯一标识出该终端的终端特征，或认为是该用户终端独特的终端标识。对于该预设指纹算法，可以是根据实际情况进行设置，例如可以是哈希 hash 算法、又或者是机器学习算法。例如可以是通过 sha256 算法进行，通过 sha256 算法将最大长度不超过 2^64 bit 的终端特征信息按 512-bit 分组进行处理，生成 256-bit 的用户终端指纹。

步骤 S30，根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱，所述信息关联图谱中包括两个以上的信息因子、

以及不同信息因子之间的关联关系；

本实施例中，在得到用户终端指纹时，检测服务器将根据该用户终端指纹和注册信息建立实体账户的信息关联图谱，以“关系”的方式将实体账户涉及的信息进行整合，并以可视化关联图的方式进行表示；对于该信息关联图谱，用户终端指纹和注册信息以信息因子的方式进行表示，信息关联图谱中包括两个以上（此处“以上”包括本数，下同）的信息因子；而不同信息因子则通过关联关系线条进行连接，该关联关系线条代表信息因子之间的“关系”（当时不是任何两个信息因子之间都一定会存在关联关系），从而方便商家或风控人员了解不同类型信息之间关联，并据此分析潜在的风险因素。

具体的，检测服务器首先将根据预设转移规则对用户终端指纹和注册信息进行转译，得到至少一个因子关系组，其中每个因子关系组中均包括两个信息因子和信息因子之间的关联关系，该因子关系组的形式可以为（信息因子 1，信息因子 2，信息因子 1 和信息因子 2 的关联关系）；因子关系组中的每个信息因子与一项注册信息或用户终端指纹对应，而信息因子之间的关联关系则可以根据注册信息的类型获该注册信息的描述角度确定；例如对于用户终端指纹 A 和注册手机号 P，两者对应的因子关系组为（终端指纹因子，手机号因子，终端所用手机号）；又例如对于用户名 Z、注册手机号 P，两者对应的因子关系组为（用户名因子，手机号因子，用户名绑定手机号）。

在得到因子关系组时，检测服务器即可根据因子关系绘制实体账户的信息关联图谱；对于每个因子关系组的信息因子，可以用一节点（如圆）表示信息因子，因子关联组中的关联关系则用关联关系线条表示，也即不同信息因子通过关联关系线条进行连接，从而得到信息关联图谱。

步骤 S40，基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示。

本实施例中，在得到了信息关联图谱后，检测服务器根据预设检测规则对信息关联图谱进行风险检测，检测出其中的风险因子（具有风险的信息因子），并根据该风险因子输出对应的安全处理提示，从

而实现风险预警。其中。其中，对于风险因子的检测可以是通过多种方式实现的，例如可以是通过因子稳定性的方式进行检测、风险传导（染黑或染灰逻辑的方式）等多种方式实现。

可选地，当用户终端指纹或某个注册信息属于黑名单信息时，可以是通过风险传导（染黑/染灰逻辑）的方式进行风险因子的检测。具体的，当用户终端指纹或某个注册信息确定属于黑名单信息时，该黑名单信息对应的信息因子可称为关联黑名单信息因子；其中该黑名单信息的确定，可以是通过第三方机构构建的黑名单信息库得到（例如黑产手机号码库、黑产邮箱等），也可以是通过其它方式得到。此时，检测服务器将对与该关联黑名单信息因子具有关联关系的信息因子进行风险检测，该被检测的信息因子可称为待检测信息因子。检测服务器首先将根据关联黑名单信息因子的因子类型确定该关联黑名单信息因子的黑名单风险值，用以表征风险程度；例如关联黑名单信息因子为手机号因子，其黑名单风险值为 80；又例如关联黑名单信息因子为邮箱号因子，其黑名单风险值为 75 等。同时，检测服务器还将根据该关联黑名单信息因子与待检测信息因子之间的关联关系确定两者之间的关系度；例如，绑定手机号的关系度为 0.8，绑定邮箱号的关系度为 0.6 等。

在确定关联黑名单信息因子的黑名单风险值以及其对应的关系度时，检测服务器将会根据预设风险传导公式计算待检测信息因子的待检测风险值，根据该待检测风险值来判断该待检测信息因子是否属于风险因子；如果该待检测风险值大于一预设风险阈值，则可认为该待检测信息因子属于风险因子；而如果该待检测风险值小于或等于该预设风险阈值，则可认为该待检测信息因子不属于风险因子。而该预设风险传导公式为：

$$f=\sum_{i=1}^{n}(k_i x_i)$$

其中，$f$ 为所述待检测信息因子的待检测风险值；$k_i$ 为第 $i$ 个关联黑名单信息因子对应的关系度，$k_i>0$，$i\geq 1$；$x_i$ 为第 $i$ 个关联黑名单信息因子对应的黑名单风险值，$x_i>0$。通过上述利用风险传导的

方式进行风险检测，可在黑名单数据量覆盖度不足的情况下提高风险检测的能力，减少了风险漏判率，有利于提高业务安全性。

进一步的，本实施例中的关联黑名单信息因子可能是黑名单 IP 因子，也即用户终端所用的 IP 地址为黑名单 IP；对于该黑名单 IP 因子，可以是通过蜜罐投放的方式进行确定方法（或识别）。具体的，检测服务器预先向网络中投放若干的测试代理 IP 地址，并以免费的方式供网络用户使用。当检测到某一测试代理 IP 地址被某一终端使用时，检测服务器将会通过该测试代理 IP 地址监测该终端的网络行为，为描述方便，该使用测试代理 IP 地址的终端可称为代理终端。检测服务器在检测到该代理终端通过测试代理 IP 地址进行攻击行为时，即可认为该测试代理终端具有一定的危险性；此时检测服务器将会获取该代理终端的真实 IP 地址，并将该真实 IP 地址确定为黑名单信息，该真实 IP 地址对应的信息因子即为黑名单 IP 因子，并用以进行风险传导分析。

可选地，关联图谱中的风险因子，还可以是通过因子稳定性的方式进行检测的。具体的，对于某一个风险性不明确的信息因子，检测服务器可在预设账户库中查询与该信息因子匹配的历史匹配账户（也即查询是否存在与当前的实体账户使用相同信息或相似信息进行注册的历史匹配账户）；若查询到了该历史匹配账户，检测服务器将会获取该历史匹配账户的历史注册时间。

当检测服务器查询完毕时，检测服务器将根据该历史匹配账户的历史注册时间进行筛选，并统计在预设注册周期内注册的历史匹配账户数。例如，当前实体账户 Z1 的注册时间为 18 年 6 月，其绑定手机号为 P；对此检测服务器检测到具有相同绑定手机号的历史匹配账户 Z2、Z3、Z4，其中历史匹配账户 Z2 的历史注册时间为 18 年 2 月，历史匹配账户 Z3 的历史注册时间为 18 年 3 月，历史匹配账户 Z4 的历史注册时间为 17 年 4 月；预设注册周期为实体账户 Z1 的注册时间前移 6 个月（即 18 年 1 月）；则此时在预设注册周期内注册的历史匹配账户数为 2 个（历史匹配账户 Z2 和历史匹配账户 Z3）。在得到历史匹配账户数时，检测服务器会将其与一预设匹配阈值进行比较，若

该历史匹配账户数大于该预设匹配阈值,则说明该信息因子在短时间内被多次使用,此时可认为该信息因子不稳定,其存在一定的风险性,并将其确定为风险因子;而若该历史匹配账户数小于或等于该预设匹配阈值,则可认为该信息因子较稳定,其在通过因子稳定性的方式进行检测时不属于风险因子。

值得说明的是,对于上述两种方式在具体实施中可以结合使用,例如可先通过因子稳定性的方式检测出某个风险因子,然后再将该风险因子作为风险传导方式中的关联黑名单信息因子,用以检测其它与之关联的信息因子的风险性,从而提高风险检测的能力,减少了风险漏判率,进一步提高业务安全性。

本实施例中,在检测出信息关联图谱中的风险因子时,检测服务器可根据该风险因子输出对应的安全处理提示。值得说明的是,由于不同实体账户的信息关联图谱中,所包括的风险因子数也可能不同,则可认为实体账户的风险情况也不相同,本实施例中为了进一步提高风险预警的准确性,方便商家或风控人员进行对应处理,可以是根据不同的风险等级进行不同的处理。具体的,检测服务器可以对信息关联图谱中的风险因子数进行统计,然后根据风险因子数确定该实体账户的风险等级;例如0个风险因子的实体账户,其风险等级为低风险;1至3个风险因子的实体账户,其风险等级为中低风险;4至6个风险因子的实体账户,其风险等级为中风险;7个以上风险因子的实体账户,其风险等级为高风险。在确定实体账户的风险等级时,检测服务器可根据该风险等级输出对应的安全处理提示;例如对于低风险的实体账户,其任何的业务功能均可正常使用;对于中低风险的实体账户,可输出建议限制其交易额度的提示;对于中风险的实体账户,可输出建议禁用一部分业务功能的提示;对于高风险的实体账户,可输出建议人工复核安全性的提示。

本实施例中,在接收到用户终端发送的账户注册请求时,获取所述用户终端的终端特征信息,并获取所述账户注册请求对应实体账户的注册信息;根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹;根据所述用户终端指纹和所述注册信息

建立所述实体账户的信息关联图谱，所述信息关联图谱中包括两个以上的信息因子、以及不同信息因子之间的关联关系；基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示。通过以上方式，本实施例在用户进行账户注册时即收集用户的相关数据，然后通过关联图谱（知识图谱）的方式对这些数据进行整合，方便商家或风控人员了解各项信息之间的关联性；再根据该关联图谱进行风险检测，从而以知识关系分析的方式对用户数据进行分析，以对潜在业务风险进行预测，实现了电子商务风险预警，提高风险检测的能力和业务安全性。

基于上述图 2 所述实施例，提出本申请基于大数据的风险检测方法的第二实施例。

本实施例中，步骤 S40 之后还包括：

在经过预设洗白周期时，检测所述实体账户在所述预设洗白周期内是否命中风险特征行为；

本实施例中，信息关联图谱中的某个信息因子被检测为风险因子后，还可以设置相应的洗白机制对其进行洗白，从而使得风险检测能够更符合实际使用情况，降低误判率。具体的，某个信息因子被检测为风险因子后，检测服务器会对实体账户的行为进行记录；当经过预设洗白周期时，检测服务器将会检测该实体账户在预设洗白周期内是否存在风险特征行为。

若所述实体账户在所述预设洗白周期内不存在所述风险特征行为，则基于预设洗白规则对所述风险因子进行洗白；

本实施例中，如果该实体账户在预设洗白周期内存在风险特征行为，则不会对其进行洗白；而如果该实体账户在预设洗白周期内不存在风险特征行为，则可基于预设洗白规则对该风险因子进行洗白。例如，对于风险因子可设置一个风险值，该风险值将被设置成可衰减的形式，其衰减程度可以以时间作为度量进行计算（当然也可以从其它维度设置风险衰减规则），例如某一信息因子是在 2016 年 1 月被确定为风险因子，其初始的风险值为 30；在经过预设洗白周期 6 个月后，其对应的实体账户不存在风险特征行为，则其风险值开始根据时间和

一预设衰减函数进行衰减；而在 2017 年 6 月时该风险因子的风险值衰减至 0，则可认为该信息因子不再属于风险因子，即该风险因子被洗白。通过这种风险衰减的方式，可以将一些黑名单信息逐渐洗白，从而在一定程度避免了风险误判的发生。当然，在实际中，若还采用了风险传导的方式进行风险检测，则当某一个风险因子被洗白时，检测服务器将重新根据风险传导的方式检测与该洗白的风险因子关联的因子风险性。

此外，本申请实施例还提供一种基于关联图谱的风险检测装置。

参照图 3，图 3 为本申请基于大数据的风险检测装置第一实施例的功能模块示意图。

本实施例中，所述风险检测装置包括：

信息获取模块 10，用于在接收到用户终端发送的账户注册请求时，获取所述用户终端的终端特征信息，并获取所述账户注册请求对应实体账户的注册信息；

指纹生成模块 20，用于根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹；

图谱建立模块 30，用于根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱，所述信息关联图谱中包括两个以上的信息因子、以及不同信息因子之间的关联关系；

风险检测模块 40，用于基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示。

其中，上述风险检测装置的各虚拟功能模块存储于图 1 所示基于关联图谱的风险检测设备的存储器 1005 中，用于实现计算机可读指令的所有功能；各模块被处理器 1001 执行时，可实现通过关联图谱的方式进行信息整合和风险检测的功能。

进一步的，图谱建立模块 30 包括：

信息转译单元，用于基于预设转译规则对所述用户终端指纹和所述注册信息进行转译，得到至少一个因子关系组，其中每个因子关系组中均包括两个信息因子和信息因子之间的关联关系；

图谱生成单元，用于根据所述因子关系组绘制所述实体账户的信

息关联图谱。

进一步的 ,所述信息关联图谱中包括待检测信息因子和至少一个关联黑名单信息因子 ,所述待检测信息因子和所述关联黑名单信息因子之间具有关联关系 ,

所述风险检测模块 40 包括 :

风险值确定单元 ,用于根据所述关联黑名单信息因子的因子类型确定所述关联黑名单信息因子的黑名单风险值 ,并根据所述关联黑名单信息因子与所述待检测信息因子之间的关联关系确定对应的关系度 ;

风险值计算单元 ,用于根据预设风险传导公式、所述黑名单风险值和所述关系度计算所述待检测信息因子的待检测风险值 ,并根据所述待检测风险值判断所述待检测信息因子是否属于风险因子 ,所述预设风险传导公式为 :

$$f=\sum_{i=1}^{n}(k_i x_i)$$

其中 , $f$ 为所述待检测信息因子的待检测风险值 ;

$k_i$ 为第 $i$ 个关联黑名单信息因子对应的关系度 , $k_i>0$ , $i\geq 1$ ;

$x_i$ 为第 $i$ 个关联黑名单信息因子对应的黑名单风险值 , $x_i>0$ 。

进一步的 , 所述关联黑名单信息因子包括黑名单 IP 因子 ,

所述风险检测装置还包括 :

IP 投放模块 , 用于向网络中投放预设数量的测试代理 IP 地址 ;

IP 确定模块 , 用于当检测到所述测试代理 IP 地址被代理终端使用并进行攻击行为 , 获取所述代理终端的真实 IP 地址 , 并根据所述真实 IP 地址确定对应的黑名单 IP 因子。

进一步的 , 所述风险检测模块 40 包括 :

账户查询单元 ,用于在预设账户库中查询与所述信息因子匹配的历史匹配账户 , 并获取所述历史匹配账户的历史注册时间 ;

账户数判断单元 ,用于根据所述历史注册时间统计在预设注册周期内注册的历史匹配账户数 ,并根据所述历史匹配账户数与预设匹配阈值的大小关系判断所述信息因子是否属于风险因子。

进一步的，所述风险检测装置还包括：

行为检测模块，用于在经过预设洗白周期时，检测所述实体账户在所述预设洗白周期内是否存在风险特征行为；

因子洗白模块，用于若所述实体账户在所述预设洗白周期内不存在所述风险特征行为，则基于预设洗白规则对所述风险因子进行洗白。

进一步的，所述风险检测模块 40 包括：

等级确定单元，用于统计所述信息关联图谱中的风险因子数，并根据所述风险因子数确定所述实体账户的风险等级；

提示输出单元，用于根据所述实体账户的风险等级输出对应的安全处理提示。

其中，上述风险检测装置中各个模块的功能实现与上述基于关联图谱的风险检测方法实施例中各步骤相对应，其功能和实现过程在此处不再一一赘述。

此外，本申请实施例还提供一种存储介质，所述存储介质可以为非易失性可读存储介质。

本申请存储介质上存储有计算机可读指令，其中所述计算机可读指令被处理器执行时，实现如上述的基于关联图谱的风险检测方法的步骤。

其中，计算机可读指令被执行时所实现的方法可参照本申请基于关联图谱的风险检测方法的各个实施例，此处不再赘述。

需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，

当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个存储介质(如 ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本申请各个实施例所述的方法。

以上仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

# 权 利 要 求 书

1、一种基于关联图谱的风险检测方法，其特征在于，所述风险检测方法包括：

在接收到用户终端发送的账户注册请求时，获取所述用户终端的终端特征信息，并获取所述账户注册请求对应实体账户的注册信息；

根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹；

根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱，所述信息关联图谱中包括两个以上的信息因子、以及不同信息因子之间的关联关系；

基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示。

2、如权利要求 1 所述的风险检测方法，其特征在于，所述根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱的步骤包括：

基于预设转译规则对所述用户终端指纹和所述注册信息进行转译，得到至少一个因子关系组，其中每个因子关系组中均包括两个信息因子和信息因子之间的关联关系；

根据所述因子关系组生成所述实体账户的信息关联图谱。

3、如权利要求 1 所述的风险检测方法，其特征在于，所述信息关联图谱中包括待检测信息因子和至少一个关联黑名单信息因子，所述待检测信息因子和所述关联黑名单信息因子之间具有关联关系，

所述基于预设检测规则检测所述信息关联图谱中的风险因子的步骤包括：

根据所述关联黑名单信息因子的因子类型确定所述关联黑名单信息因子的黑名单风险值，并根据所述关联黑名单信息因子与所述待检测信息因子之间的关联关系确定对应的关系度；

根据预设风险传导公式、所述黑名单风险值和所述关系度计算所述待检测信息因子的待检测风险值，并根据所述待检测风险值判断所

述待检测信息因子是否属于风险因子，所述预设风险传导公式为：

$$f=\sum_{i=1}^{n}(k_i x_i)$$

其中，$f$ 为所述待检测信息因子的待检测风险值；

$k_i$ 为第 $i$ 个关联黑名单信息因子对应的关系度，$k_i>0$，$i\geq 1$；

$x_i$ 为第 $i$ 个关联黑名单信息因子对应的黑名单风险值，$x_i>0$。

4、如权利要求 3 所述的风险检测方法，其特征在于，所述关联黑名单信息因子包括黑名单 IP 因子，

所述风险检测方法还包括：

向网络中投放预设数量的测试代理 IP 地址；

当检测到所述测试代理 IP 地址被代理终端使用并进行攻击行为，获取所述代理终端的真实 IP 地址，并根据所述真实 IP 地址确定对应的黑名单 IP 因子。

5、如权利要求 1 所述的风险检测方法，其特征在于，所述基于预设检测规则检测所述信息关联图谱中的风险因子的步骤包括：

在预设账户库中查询与所述信息因子匹配的历史匹配账户，并获取所述历史匹配账户的历史注册时间；

根据所述历史注册时间统计在预设注册周期内注册的历史匹配账户数，并根据所述历史匹配账户数与预设匹配阈值的大小关系判断所述信息因子是否属于风险因子。

6、如权利要求 1 所述的风险检测方法，其特征在于，所述基于预设检测规则检测所述信息关联图谱中的风险因子的步骤之后，还包括：

在经过预设洗白周期时，检测所述实体账户在所述预设洗白周期内是否存在风险特征行为；

若所述实体账户在所述预设洗白周期内不存在所述风险特征行为，则基于预设洗白规则对所述风险因子进行洗白。

7、如权利要求 1 所述的风险检测方法，其特征在于，所述根据所述风险因子输出对应的安全处理提示的步骤包括：

统计所述信息关联图谱中的风险因子数，并根据所述风险因子数

确定所述实体账户的风险等级；

根据所述实体账户的风险等级输出对应的安全处理提示。

8、一种基于关联图谱的风险检测装置，其特征在于，所述风险检测装置包括：

信息获取模块，用于在接收到用户终端发送的账户注册请求时，获取所述用户终端的终端特征信息，并获取所述账户注册请求对应实体账户的注册信息；

指纹生成模块，用于根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹；

图谱建立模块，用于根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱，所述信息关联图谱中包括两个以上的信息因子、以及不同信息因子之间的关联关系；

风险检测模块，用于基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示。

9、如权利要求 8 所述的风险检测装置，其特征在于，所述图谱建立模块包括：

信息转译单元，用于基于预设转译规则对所述用户终端指纹和所述注册信息进行转译，得到至少一个因子关系组，其中每个因子关系组中均包括两个信息因子和信息因子之间的关联关系；

图谱生成单元，用于根据所述因子关系组绘制所述实体账户的信息关联图谱。

10、如权利要求 8 所述的风险检测装置，其特征在于，所述信息关联图谱中包括待检测信息因子和至少一个关联黑名单信息因子，所述待检测信息因子和所述关联黑名单信息因子之间具有关联关系，

所述风险检测模块包括：

风险值确定单元，用于根据所述关联黑名单信息因子的因子类型确定所述关联黑名单信息因子的黑名单风险值，并根据所述关联黑名单信息因子与所述待检测信息因子之间的关联关系确定对应的关系度；

风险值计算单元，用于根据预设风险传导公式、所述黑名单风险

值和所述关系度计算所述待检测信息因子的待检测风险值，并根据所述待检测风险值判断所述待检测信息因子是否属于风险因子，所述预设风险传导公式为：

$$f=\sum_{i=1}^{n}(k_i x_i)$$

其中，$f$ 为所述待检测信息因子的待检测风险值；

$k_i$ 为第 $i$ 个关联黑名单信息因子对应的关系度，$k_i>0$，$i\geq 1$；

$x_i$ 为第 $i$ 个关联黑名单信息因子对应的黑名单风险值，$x_i>0$。

11、如权利要求 10 所述的风险检测装置，其特征在于，所述关联黑名单信息因子包括黑名单 IP 因子，

所述风险检测装置还包括：

IP 投放模块，用于向网络中投放预设数量的测试代理 IP 地址；

IP 确定模块，用于当检测到所述测试代理 IP 地址被代理终端使用并进行攻击行为，获取所述代理终端的真实 IP 地址，并根据所述真实 IP 地址确定对应的黑名单 IP 因子。

12、如权利要求 8 所述的风险检测装置，其特征在于，所述风险检测模块包括：

账户查询单元，用于在预设账户库中查询与所述信息因子匹配的历史匹配账户，并获取所述历史匹配账户的历史注册时间；

账户数判断单元，用于根据所述历史注册时间统计在预设注册周期内注册的历史匹配账户数，并根据所述历史匹配账户数与预设匹配阈值的大小关系判断所述信息因子是否属于风险因子。

13、如权利要求 8 所述的风险检测装置，其特征在于，所述风险检测装置还包括：

行为检测模块，用于在经过预设洗白周期时，检测所述实体账户在所述预设洗白周期内是否存在风险特征行为；

因子洗白模块，用于若所述实体账户在所述预设洗白周期内不存在所述风险特征行为，则基于预设洗白规则对所述风险因子进行洗白。

14、如权利要求 8 所述的风险检测装置，其特征在于，所述风险检测模块包括：

等级确定单元，用于统计所述信息关联图谱中的风险因子数，并根据所述风险因子数确定所述实体账户的风险等级；

提示输出单元，用于根据所述实体账户的风险等级输出对应的安全处理提示。

15、一种基于关联图谱的风险检测设备，其特征在于，所述风险检测设备包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的计算机可读指令，其中所述计算机可读指令被所述处理器执行时，实现如下步骤：

在接收到用户终端发送的账户注册请求时，获取所述用户终端的终端特征信息，并获取所述账户注册请求对应实体账户的注册信息；

根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹；

根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱，所述信息关联图谱中包括两个以上的信息因子、以及不同信息因子之间的关联关系；

基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示。

16、如权利要求 15 所述的风险检测设备，其特征在于，所述根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱的步骤包括：

基于预设转译规则对所述用户终端指纹和所述注册信息进行转译，得到至少一个因子关系组，其中每个因子关系组中均包括两个信息因子和信息因子之间的关联关系；

根据所述因子关系组生成所述实体账户的信息关联图谱。

17、如权利要求 15 所述的风险检测设备，其特征在于，所述信息关联图谱中包括待检测信息因子和至少一个关联黑名单信息因子，所述待检测信息因子和所述关联黑名单信息因子之间具有关联关系，

所述基于预设检测规则检测所述信息关联图谱中的风险因子的步骤包括：

根据所述关联黑名单信息因子的因子类型确定所述关联黑名单

信息因子的黑名单风险值，并根据所述关联黑名单信息因子与所述待检测信息因子之间的关联关系确定对应的关系度；

根据预设风险传导公式、所述黑名单风险值和所述关系度计算所述待检测信息因子的待检测风险值，并根据所述待检测风险值判断所述待检测信息因子是否属于风险因子，所述预设风险传导公式为：

$$f=\sum_{i=1}^{n}(k_i x_i)$$

其中，$f$ 为所述待检测信息因子的待检测风险值；

$k_i$ 为第 $i$ 个关联黑名单信息因子对应的关系度，$k_i>0$，$i\geq 1$；

$x_i$ 为第 $i$ 个关联黑名单信息因子对应的黑名单风险值，$x_i>0$。

18、一种存储介质，其特征在于，所述存储介质上存储有计算机可读指令，其中所述计算机可读指令被处理器执行时，实现如下步骤：

在接收到用户终端发送的账户注册请求时，获取所述用户终端的终端特征信息，并获取所述账户注册请求对应实体账户的注册信息；

根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹；

根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱，所述信息关联图谱中包括两个以上的信息因子、以及不同信息因子之间的关联关系；

基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示。

19、如权利要求 18 所述的存储介质，其特征在于，所述根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱的步骤包括：

基于预设转译规则对所述用户终端指纹和所述注册信息进行转译，得到至少一个因子关系组，其中每个因子关系组中均包括两个信息因子和信息因子之间的关联关系；

根据所述因子关系组生成所述实体账户的信息关联图谱。

20、如权利要求 18 所述的存储介质，其特征在于，所述信息关联图谱中包括待检测信息因子和至少一个关联黑名单信息因子，所述

待检测信息因子和所述关联黑名单信息因子之间具有关联关系，

所述基于预设检测规则检测所述信息关联图谱中的风险因子的步骤包括：

根据所述关联黑名单信息因子的因子类型确定所述关联黑名单信息因子的黑名单风险值，并根据所述关联黑名单信息因子与所述待检测信息因子之间的关联关系确定对应的关系度；

根据预设风险传导公式、所述黑名单风险值和所述关系度计算所述待检测信息因子的待检测风险值，并根据所述待检测风险值判断所述待检测信息因子是否属于风险因子，所述预设风险传导公式为：

$$f=\sum_{i=1}^{n}(k_i x_i)$$

其中，$f$ 为所述待检测信息因子的待检测风险值；

$k_i$ 为第 $i$ 个关联黑名单信息因子对应的关系度，$k_i>0$，$i\geq 1$；

$x_i$ 为第 $i$ 个关联黑名单信息因子对应的黑名单风险值，$x_i>0$。

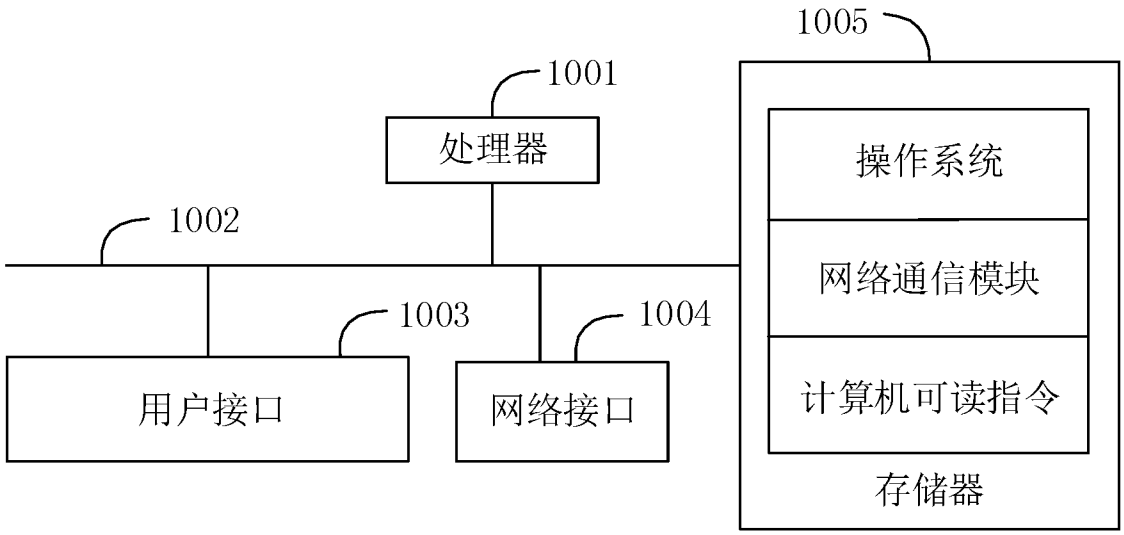
1005
1001
处理器
操作系统
1002
网络通信模块
1003
1004
计算机可读指令
用户接口
网络接口
存储器

图 1

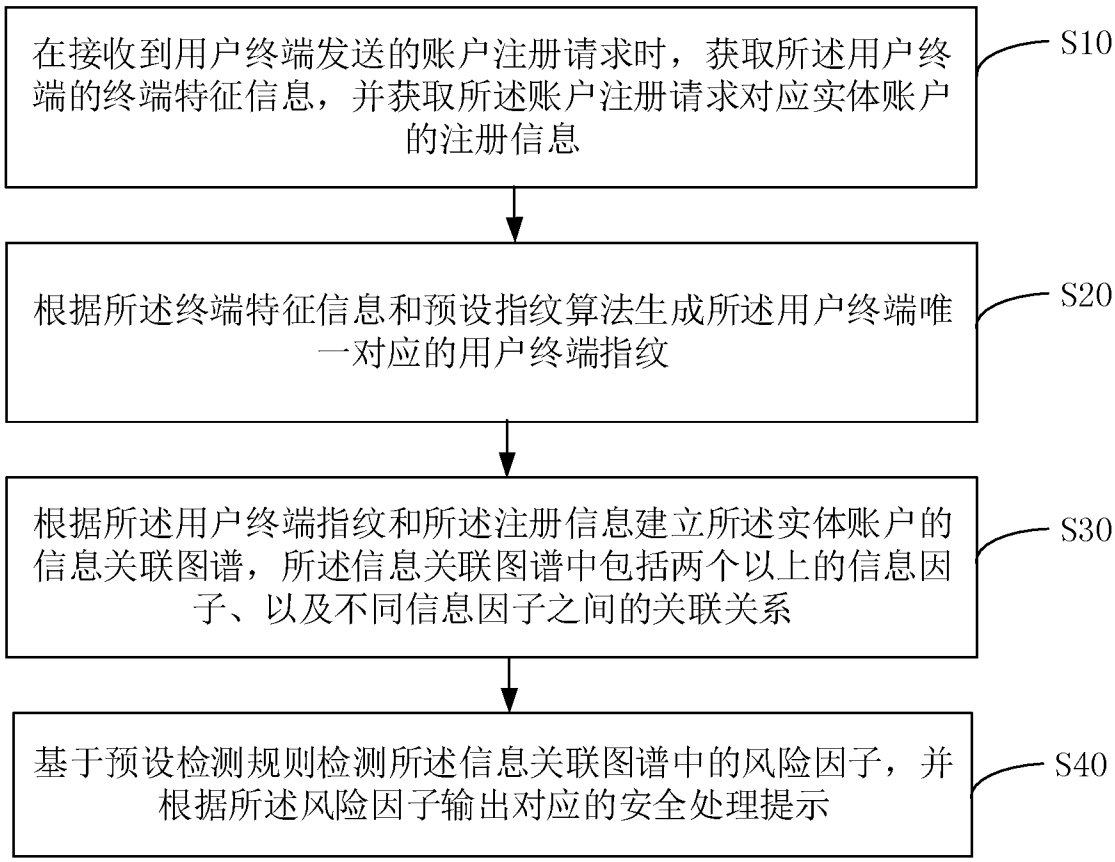
在接收到用户终端发送的账户注册请求时，获取所述用户终端的终端特征信息，并获取所述账户注册请求对应实体账户的注册信息
S10
根据所述终端特征信息和预设指纹算法生成所述用户终端唯一对应的用户终端指纹
S20
根据所述用户终端指纹和所述注册信息建立所述实体账户的信息关联图谱，所述信息关联图谱中包括两个以上的信息因子、以及不同信息因子之间的关联关系
S30
基于预设检测规则检测所述信息关联图谱中的风险因子，并根据所述风险因子输出对应的安全处理提示
S40

图 2

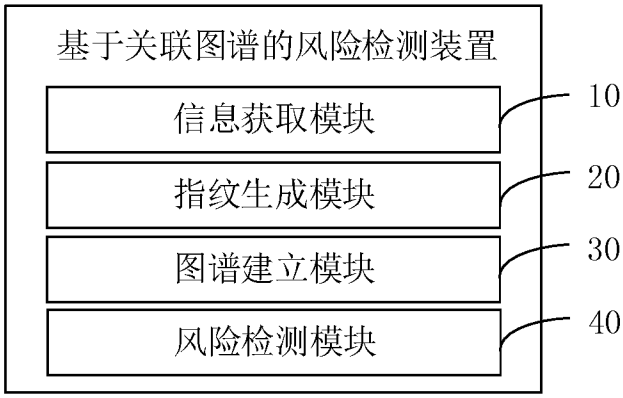


图 3

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2018/122745**

## A. CLASSIFICATION OF SUBJECT MATTER

G06Q 30/06(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

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)

EPODOC, WPI, CNPAT, CNKI, IEEE: 业务, 注册, 账户, 请求, 风险, 评估, 分析, 评测, 因子, 关系, 关联, 图谱, 设备, 摘要, 指纹, 唯一, service, request, register, login, risk, account, evaluate, associate, relationship, gene, hash, sha256

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CN 108399509 A (ALIBABA GROUP HOLDING LIMITED) 14 August 2018 (2018-08-14)<br>description, paragraphs [0006]-[0026] and [0039]-[0057] | 1-20 |
| A | CN 107067157 A (BEIJING QIYI CENTURY SCIENCE & TECHNOLOGY CO., LTD.) 18 August 2017 (2017-08-18)<br>entire document | 1-20 |
| A | CN 106998315 A (ALIBABA GROUP HOLDING LIMITED) 01 August 2017 (2017-08-01)<br>entire document | 1-20 |
| A | WO 2015096053 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 02 July 2015 (2015-07-02)<br>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 | Date of mailing of the international search report |
|---|---|
| **19 June 2019** | **30 July 2019** |
| Name and mailing address of the ISA/CN<br>**National Intellectual Property Administration, PRC (ISA/CN)**<br>**No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088**<br>**China**<br>Facsimile No. **(86-10)62019451** | Authorized officer<br><br>Telephone No. |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/CN2018/122745**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| CN 108399509 A | 14 August 2018 | None | |
| CN 107067157 A | 18 August 2017 | None | |
| CN 106998315 A | 01 August 2017 | None | |
| WO 2015096053 A1 | 02 July 2015 | EP 3079326 A1 | 12 October 2016 |
| | | CN 104169952 A | 26 November 2014 |
| | | KR 20160096202 A | 12 August 2016 |
| | | JP 2017500667 A | 05 January 2017 |
| | | US 2016321628 A1 | 03 November 2016 |

# 国际检索报告

国际申请号
PCT/CN2018/122745

A. 主题的分类

G06Q 30/06(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

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））

EPODOC, WPI, CNPAT, CNKI, IEEE: 业务，注册，账户，请求，风险，评估，分析，评测，因子，关系，关联，图谱，设备，摘要，指纹，唯一，service, request, register, login, risk, account, evaluate, associate, relationship, gene, hash, sha256

C. 相关文件

| 类 型* | 引用文件，必要时，指明相关段落 | 相关的权利要求 |
|---|---|---|
| X | CN 108399509 A (阿里巴巴集团控股有限公司) 2018年 8月 14日 (2018-08-14)<br>说明书第[0006]-[0026]、[0039]-[0057]段 | 1-20 |
| A | CN 107067157 A (北京奇艺世纪科技有限公司) 2017年 8月 18日 (2017-08-18)<br>全文 | 1-20 |
| A | CN 106998315 A (阿里巴巴集团控股有限公司) 2017年 8月 1日 (2017-08-01)<br>全文 | 1-20 |
| A | WO 2015096053 A1 (华为技术有限公司) 2015年 7月 2日 (2015-07-02)<br>全文 | 1-20 |

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 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 6月 19日 | 2019年 7月 30日 |
| ISA/CN的名称和邮寄地址<br>中国国家知识产权局(ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10)62019451 | 受权官员<br>高民芳<br>电话号码 86-(10)-53961520 |

表 PCT/ISA/210 (第2页) (2015年1月)

# 国际检索报告
## 关于同族专利的信息

国际申请号
PCT/CN2018/122745

| 检索报告引用的专利文件 | | | 公布日<br>(年/月/日) | 同族专利 | | | 公布日<br>(年/月/日) |
|---|---|---|---|---|---|---|---|
| CN | 108399509 | A | 2018年 8月 14日 | 无 | | | |
| CN | 107067157 | A | 2017年 8月 18日 | 无 | | | |
| CN | 106998315 | A | 2017年 8月 1日 | 无 | | | |
| WO | 2015096053 | A1 | 2015年 7月 2日 | EP | 3079326 | A1 | 2016年 10月 12日 |
| | | | | CN | 104169952 | A | 2014年 11月 26日 |
| | | | | KR | 20160096202 | A | 2016年 8月 12日 |
| | | | | JP | 2017500667 | A | 2017年 1月 5日 |
| | | | | US | 2016321628 | A1 | 2016年 11月 3日 |