(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106296406 A
(43)申请公布日 2017.01.04

(21)申请号 201510244028.4

(22)申请日 2015.05.13

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 付杨

(74)专利代理机构 北京鸿德海业知识产权代理事务所(普通合伙) 11412
代理人 倪志华

(51)Int.Cl.
G06Q 40/08(2012.01)

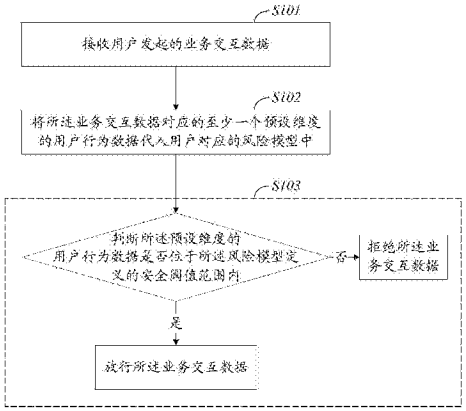
权利要求书2页 说明书8页 附图3页

(54)发明名称

交互数据的处理方法及装置

(57)摘要

本申请揭示了一种交互数据的处理方法及装置,其中,所述方法包括:接收用户发起的业务交互数据;将所述业务交互数据对应的至少一个预设维度的用户行为数据代入用户对应的风险模型中;判断所述预设维度的用户行为数据是否位于所述风险模型定义的安全阈值范围内,若是,则放行所述业务交互数据,若否,则拒绝所述业务交互数据。本申请通过用户在发起业务交互数据前的历史行为,构建业务交互数据的风险模型,以通过该风险模型判断当前业务交互数据的安全性,降低了对用户的打扰率,提升网络通信效率。



CN 106296406 A

1. 一种交互数据的处理方法，其特征在于，所述方法包括：

接收用户发起的业务交互数据；

将所述业务交互数据对应的至少一个预设维度的用户行为数据代入用户对应的风险模型中，其中，所述预设维度和用户与业务交互数据所涉及的第三方之间交互行为相关；

判断所述预设维度的用户行为数据是否位于所述风险模型定义的安全阈值范围内，若是，则放行所述业务交互数据，若否，则拒绝所述业务交互数据。

2. 根据权利要求 1 所述的交互数据的处理方法，其特征在于，所述方法还包括建立风险模型，其具体包括：

获取用户在第一时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

计算在第一时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第一平均值或第一方差；

获取用户在第二时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

计算在第二时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第二平均值或第二方差；

将所述第一平均值或第一方差和所述第二平均值或第二方差，或所述第一平均值和第二平均值的差值，运用决策树计算出与每个预设维度对应的安全阈值范围并构建与用户对应的风险模型，其中，第一时间区间长度大于第二时间区间。

3. 根据权利要求 1 所述的交互数据的处理方法，其特征在于，将所述业务交互数据对应的至少一个预设维度的用户行为的值代入风险模型具体包括：

判断是否存在与所述业务交互数据对应的预设维度的用户行为数据；

若是，则将所述业务交互数据对应的至少一个预设维度的用户行为的值代入风险模型。

4. 根据权利要求 1～3 中任一项所述的交互数据的处理方法，其特征在于，所述预设维度和用户与业务交互数据所涉及的第三方之间即时信息交互行为相关。

5. 根据权利要求 4 所述的交互数据的处理方法，其特征在于，所述预设用户行为包括：

用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小，以及用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间。

6. 根据权利要求 5 所述的交互数据的处理方法，其特征在于，判断所述预设维度的用户行为数据是否位于所述风险模型的安全阈值范围内具体包括：

判断用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小、用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间是否均落入对应的安全阈值范围内。

7. 一种交互数据的处理装置，其特征在于，所述装置包括：

交互模块，用于接收用户发起的业务交互数据；

处理模块，用于将所述业务交互数据对应的至少一个预设维度的用户行为数据代入用户对应的风险模型中，其中，所述预设维度和用户与业务交互数据所涉及的第三方之间交

互行为相关；以及

判断所述预设维度的用户行为数据是否位于所述风险模型定义的安全阈值范围内，若是，则放行所述业务交互数据，若否，则拒绝所述业务交互数据。

8. 根据权利要求 7 所述的交互数据的处理装置，其特征在于，所述装置还包括模型建构模块，用于：

获取用户在第一时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

计算在第一时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第一平均值或第一方差；

获取用户在第二时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

计算在第二时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第二平均值或第一方差；

将所述第一平均值或第一方差和所述第二平均值或第二方差，或所述第一平均值和第二平均值的差值，运用决策树计算出与每个预设维度对应的安全阈值范围并构建与用户对应的风险模型，其中，第一时间区间长度大于第二时间区间。

9. 根据权利要求 7 所述的交互数据的处理装置，其特征在于，所述装置还包括适配模块，用于：

判断是否存在与所述业务交互数据对应的预设维度的用户行为数据。

10. 根据权利要求 7 ～ 9 中任一项所述的交互数据的处理装置，其特征在于，所述预设维度和用户与业务交互数据所涉及的第三方之间即时信息交互行为相关。

11. 根据权利要求 10 所述的交互数据的处理装置，其特征在于，所述预设用户行为包括：

用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小，以及用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间。

12. 根据权利要求 11 所述的交互数据的处理装置，其特征在于，所述处理模块具体用于：

判断用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小，、用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间是否均落入对应的安全阈值范围内。

交互数据的处理方法及装置

技术领域

[0001] 本申请涉及计算机领域，尤其是涉及一种交互数据的处理方法及装置。

背景技术

[0002] 为了避免他人冒充用户在互联网上交互数据（特别是涉及资金的数据、交易的数据等），现有的做法是，通过采集用户终端设备的设备信息，和/或用户所处的环境信息（例如，地理位置、IP 地址等）来判断当前发起的交互数据的安全性，例如判断是否为用户本人发起的交互数据。

[0003] 然而，一旦用户更换了终端设备或者更换了环境，又或者未采集到用户终端设备的设备信息和环境信息，现有技术将无法判断当前发起的交互数据的安全性，只能向用户发出身份验证信息，这会带来很高的用户打扰率。

发明内容

[0004] 本申请的目的在于提供一种交互数据的处理方法及装置，可以提升交互数据的安全性，降低用户打扰率。

[0005] 为实现上述申请目的之一，本申请一实施方式提供了一种交互数据的处理方法，所述方法包括：

[0006] 接收用户发起的业务交互数据；

[0007] 将所述业务交互数据对应的至少一个预设维度的用户行为数据代入用户对应的风险模型中，其中，所述预设维度和用户与业务交互数据所涉及的第三方之间交互行为相关；

[0008] 判断所述预设维度的用户行为数据是否位于所述风险模型定义的安全阈值范围内，若是，则放行所述业务交互数据，若否，则拒绝所述业务交互数据。

[0009] 作为本申请一实施方式的进一步改进，所述方法还包括建立风险模型，其具体包括：

[0010] 获取用户在第一时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

[0011] 计算在第一时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第一平均值或第一方差；

[0012] 获取用户在第二时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

[0013] 计算在第二时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第二平均值或第二方差；

[0014] 将所述第一平均值或第一方差和所述第二平均值或第二方差，或所述第一平均值和第二平均值的差值，运用决策树计算出与每个预设维度对应的安全阈值范围并构建与用户对应的风险模型，其中，第一时间区间长度大于第二时间区间。

[0015] 作为本申请一实施方式的进一步改进，将所述业务交互数据对应的至少一个预设维度的用户行为的值代入风险模型具体包括：

[0016] 判断是否存在与所述业务交互数据对应的预设维度的用户行为数据；

[0017] 若是，则将所述业务交互数据对应的至少一个预设维度的用户行为的值代入风险模型。

[0018] 作为本申请一实施方式的进一步改进，所述预设维度和用户与业务交互数据所涉及的第三方之间即时信息交互行为相关。

[0019] 作为本申请一实施方式的进一步改进，所述预设用户行为包括：

[0020] 用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小，以及用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间。

[0021] 作为本申请一实施方式的进一步改进，判断所述预设维度的用户行为数据是否位于所述风险模型的安全阈值范围内具体包括：

[0022] 判断用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小、用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间是否均落入对应的安全阈值范围内。

[0023] 为实现上述申请目的之一，本申请一实施方式提供了一种交互数据的处理装置，所述装置包括：

[0024] 交互模块，用于接收用户发起的业务交互数据；

[0025] 处理模块，用于将所述业务交互数据对应的至少一个预设维度的用户行为数据代入用户对应的风险模型中，其中，所述预设维度和用户与业务交互数据所涉及的第三方之间交互行为相关；以及

[0026] 判断所述预设维度的用户行为数据是否位于所述风险模型定义的安全阈值范围内，若是，则放行所述业务交互数据，若否，则拒绝所述业务交互数据。

[0027] 作为本申请一实施方式的进一步改进，所述装置还包括模型建构模块，用于：

[0028] 获取用户在第一时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

[0029] 计算在第一时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第一平均值或第一方差；

[0030] 获取用户在第二时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

[0031] 计算在第二时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第二平均值或第二方差；

[0032] 将所述第一平均值或第一方差和所述第二平均值或第二方差，或所述第一平均值和第二平均值的差值，运用决策树计算出与每个预设维度对应的安全阈值范围并构建与用户对应的风险模型，其中，第一时间区间长度大于第二时间区间。

[0033] 作为本申请一实施方式的进一步改进，所述装置还包括适配模块，用于：

[0034] 判断是否存在与所述业务交互数据对应的预设维度的用户行为数据。

[0035] 作为本申请一实施方式的进一步改进，所述预设维度和用户与业务交互数据所涉及的第三方之间即时信息交互行为相关。

[0036] 作为本申请一实施方式的进一步改进，所述预设用户行为包括：

[0037] 用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小，以及用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间。

[0038] 作为本申请一实施方式的进一步改进，所述处理模块具体用于：

[0039] 判断用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小、用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间是否均落入对应的安全阈值范围内。

[0040] 相对于现有技术，本申请的技术效果在于：通过用户在发起业务交互数据前的历史行为，构建业务交互数据的风险模型，以通过该风险模型判断当前业务交互数据的安全性，降低了对用户的打扰率，提升网络通信效率。

附图说明

[0041] 图 1 是本申请一实施方式中交互数据的处理方法的流程图；

[0042] 图 2 是本申请一实施方式中建立风险模型的流程图。

[0043] 图 3 是本申请一实施方式中交互数据的处理装置的模块图。

具体实施方式

[0044] 以下将结合附图所示的具体实施方式对本申请进行详细描述。但这些实施方式并不限制本申请，本领域的普通技术人员根据这些实施方式所做出的结构、方法、或功能上的变换均包含在本申请的保护范围内。

[0045] 如图 1 所示，在本申请一实施方式中，所述交互数据的处理方法，包括：

[0046] S101、接收用户发起的业务交互数据；

[0047] S102、将所述业务交互数据对应的至少一个预设维度的用户行为数据代入用户对应的风险模型中；

[0048] S103、判断所述预设维度的用户行为数据是否位于所述风险模型定义的安全阈值范围内，若是，则放行所述业务交互数据，若否，则拒绝所述业务交互数据。

[0049] 在本实施方式中，以网络交易业务的业务交互数据为例对本申请的技术方案进行详尽说明。当然，所述业务交互数据可不局限与网络交易业务的业务交互数据，本领域技术人员可通过惯用技术手段将本申请的技术方案应用到其他业务中，在此不再赘述。

[0050] 以网络交易业务的业务交互数据为例，用户发起的实时交易可产生该业务交易数据，在产生所述业务交易数据后，交易系统 / 服务器可接收该业务交易数据。此时，为避免他人冒充用户本人发起实时交易，保证用户资金安全，在交易系统 / 服务器中，需要对该业务交易数据进行评估，判断其是否安全。在本实施方式中，判断所述业务交易数据是否安全是通过用户对应的风险模型（例如通过用户 ID 确认其对应的风险模型），以及与该业务交易数据对应的预设维度的用户行为数据进行的。其中，所述预设维度和用户与业务交互数

据所涉及的第三方之间交互行为相关。

[0051] 另外，在本实施方式中，为了降低交易系统 / 服务器的运算量，所述风险模型可为当前网络交易业务发起时间的 24 小时前的历史业务交互数据对应的预设维度的用户历史行为所更新的风险模型。

[0052] 进一步地，将所述业务交互数据对应的至少一个预设维度的用户行为的值代入风险模型具体包括 ：

[0053] 判断是否存在与所述业务交互数据对应的预设维度的用户行为数据 ；

[0054] 若是，则将所述业务交互数据对应的至少一个预设维度的用户行为的值代入风险模型。

[0055] 在某些情况下，业务交互数据未具有相应的预设维度的用户行为，例如，用户 A 在进行本次网络交易业务时，并未与业务交互数据所涉及的第三方之间有交互行为，可以理解，在这样的情况下，是无法通过预设维度的用户行为数据代入风险模型判断本次业务交互数据的安全性。此时，可通过比较传统的技术方案来判断本次业务交互数据的安全性，例如，通过采集用户终端设备的设备信息，和 / 或用户所处的环境信息（例如，地理位置、IP 地址等）来判断当前发起的交互数据的安全性。

[0056] 而当本次业务交互数据存在对应的预设维度的用户行为数据时，即可通过预设维度的用户行为数据带入风险模型判断本次业务交互数据的安全性。

[0057] 当然，还有一种情况，例如用户 A 的网络交易业务数量较小，或者用户 A 的网络交易业务的业务交互数据存在对应的预设维度的用户行为较少，其并不足够形成对应用户 A 的风险模型，即是交易系统 / 服务器中未建立有对应用户 A 的风险模型，可以理解，在这样的情况下，是无法通过预设维度的用户行为数据代入风险模型判断本次业务交互数据的安全性。此时，可通过比较传统的技术方案来判断本次业务交互数据的安全性，例如，通过采集用户终端设备的设备信息，和 / 或用户所处的环境信息（例如，地理位置、IP 地址等）来判断当前发起的交互数据的安全性。

[0058] 进一步地，在本实施方式中，所述预设维度和用户与业务交互数据所涉及的第三方之间即时信息交互行为相关。

[0059] 所述预设维度的用户行为数据包括 ：用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小，以及用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间。

[0060] 经过对大数据的分析，用户在网络交易时有对商品的详情、是否有想要的款式以及是否包邮等交易细节与卖家（第三方）进行沟通的习惯。不同的用户和卖家交流的时间长度、和卖家交流的记录数据大小，以及和卖家交流完成到发起支付的间隔时间都有着自己独特的行为习惯，而利用用户的这些行为习惯可识别当前用户是否是用户本人，当前业务交互数据是否安全，将对用户购物时的买家支付安全起到一个很好的保护作用。

[0061] 进一步地，在本实施方式中，判断所述预设维度的用户行为数据是否位于所述风险模型的安全阈值范围内具体包括 ：判断用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小、用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间是

否均落入对应的安全阈值范围内，即是上述三个维度均要落入对应的安全阈值范围内，才表示该业务交互数据安全。

[0062] 如图 2 所示，在本申请一实施方式中，所述方法还包括建立风险模型，其具体包括：

[0063] S201、获取用户在第一时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

[0064] S202、计算在第一时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第一平均值或第一方差；

[0065] S203、获取用户在第二时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

[0066] S204、计算在第二时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第二平均值或第二方差；

[0067] S205、将所述第一平均值或第一方差和所述第二平均值或第二方差，或所述第一平均值和第二平均值的差值，运用决策树计算出与每个预设维度对应的安全阈值范围并构建与用户对应的风险模型，其中，第一时间区间长度大于第二时间区间。

[0068] 下面以一具体示例进行说明：

[0069] 先以用户 ID 为主键获取用户一年内所有或指定平台上的交易前和卖家的聊天记录，包括：用户和卖家交流的时间长度、和卖家交流的记录数据大小，以及和卖家交流完成到发起支付的间隔时间。

[0070] 再选取在过去网络交易业务满足一定条件（比如网络交易业务数量大于或等于预设数量）的用户。并逐个对选取出用户的用户和卖家交流的时间长度、和卖家交流的记录数据大小、和卖家交流完成到发起支付的间隔时间分别做聚合。

[0071] 如此，可得到每个选取的用户和卖家交流的时间长度的平均值或方差、和卖家交流的记录数据大小的平均值或方差、和卖家交流完成到发起支付的间隔时间的平均值或方差。即可到用户在发起业务交互数据（交易支付前）和卖家交流的历史行为数据。

[0072] 然后，选取新的一段时间（比如 1 个月）内的交易前和卖家的聊天记录作为样本，按照上述方式，得到每个选取用户在这段时间内和卖家交流的时间长度的平均值或方差、和卖家交流的记录数据大小的平均值或方差、和卖家交流完成到发起支付的间隔时间的平均值或方差。即可得到样本行为数据。当然，该样本行为数据的计算也可在历史行为数据的计算前或同时进行。

[0073] 这样，可根据上述历史行为数据和样本行为数据，并运用决策树建构风险模型；当然，也可先计算样本行为数据与上述历史行为数据中相应数据的偏差的绝对值，再根据所述绝对值，运用决策树构建风险模型，该风险模型可定义每个预设维度（用户和卖家交流的时间长度、和卖家交流的记录数据大小、和卖家交流完成到发起支付的间隔时间）对应的安全阈值范围。

[0074] 如图 3 所示，在本申请一实施方式中，所述交互数据的处理装置，包括：

[0075] 交互模块 100，用于接收用户发起的业务交互数据；

[0076] 处理模块 200，用于将所述业务交互数据对应的至少一个预设维度的用户行为数据代入用户对应的风险模型 400 中；以及

[0077] 判断所述预设维度的用户行为数据是否位于所述风险模型 400 定义的安全阈值范围内，若是，则放行所述业务交互数据，若否，则拒绝所述业务交互数据。

[0078] 在本实施方式中，以网络交易业务的业务交互数据为例对本申请的技术方案进行详尽说明。当然，所述业务交互数据可不局限与网络交易业务的业务交互数据，本领域技术人员可通过惯用技术手段将本申请的技术方案应用到其他业务中，在此不再赘述。

[0079] 以网络交易业务的业务交互数据为例，用户发起的实时交易可产生该业务交易数据，在产生所述业务交易数据后，交易系统 / 服务器可接收该业务交易数据。此时，为避免他人冒充用户本人发起实时交易，保证用户资金安全，在交易系统 / 服务器中，需要对该业务交易数据进行评估，判断其是否安全。

[0080] 在本实施方式中，判断所述业务交易数据是否安全是通过用户对应的风险模型 400（例如通过用户 ID 确认其对应的风险模型 400），以及与该业务交易数据对应的预设维度的用户行为数据进行的。其中，所述预设维度和用户与业务交互数据所涉及的第三方之间交互行为相关。

[0081] 另外，在本实施方式中，为了降低交易系统 / 服务器的运算量，所述风险模型 400 可为当前网络交易业务发起时间的 24 小时前的历史业务交互数据对应的预设维度的用户历史行为所更新的风险模型。

[0082] 进一步地，将所述装置还包括适配模块 500，其用于判断是否存在与所述业务交互数据对应的预设维度的用户行为数据 ；

[0083] 若是，则通过处理模块 200 将所述业务交互数据对应的至少一个预设维度的用户行为的值代入风险模型 400。

[0084] 在某些情况下，业务交互数据未具有相应的预设维度的用户行为，例如，用户 A 在进行本次网络交易业务时，并未与业务交互数据所涉及的第三方之间有交互行为，可以理解，在这样的情况下，是无法通过预设维度的用户行为数据代入风险模型 400 判断本次业务交互数据的安全性。此时，可通过比较传统的技术方案来判断本次业务交互数据的安全性，例如，通过采集用户终端设备的设备信息，和 / 或用户所处的环境信息（例如，地理位置、IP 地址等）来判断当前发起的交互数据的安全性。

[0085] 而当本次业务交互数据存在对应的预设维度的用户行为数据时，即可通过预设维度的用户行为数据带入风险模型 400 判断本次业务交互数据的安全性。

[0086] 当然，还有一种情况，例如用户 A 的网络交易业务数量较小，或者用户 A 的网络交易业务的业务交互数据存在对应的预设维度的用户行为较少，其并不足够形成对应用户 A 的风险模型，即是交易系统 / 服务器中未建立有对应用户 A 的风险模型，可以理解，在这样的情况下，是无法通过预设维度的用户行为数据代入风险模型判断本次业务交互数据的安全性。此时，可通过比较传统的技术方案来判断本次业务交互数据的安全性，例如，通过采集用户终端设备的设备信息，和 / 或用户所处的环境信息（例如，地理位置、IP 地址等）来判断当前发起的交互数据的安全性。

[0087] 进一步地，在本实施方式中，所述预设维度和用户与业务交互数据所涉及的第三方之间即时信息交互行为相关。

[0088] 所述预设维度的用户行为数据包括 ：用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小，

以及用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间。

[0089] 经过对大数据的分析，用户在网络交易时有对商品的详情、是否有想要的款式以及是否包邮等交易细节与卖家（第三方）进行沟通的习惯。不同的用户和卖家交流的时间长度、和卖家交流的记录数据大小，以及和卖家交流完成到发起支付的间隔时间都有着自己独特的行为习惯，而利用用户的这些行为习惯可识别当前用户是否是用户本人，当前业务交互数据是否安全，将对用户购物时的买家支付安全起到一个很好的保护作用。

[0090] 进一步地，在本实施方式中，所述处理模块 200 具体用于：判断用户与业务交互数据所涉及的第三方的即时信息交互的通信时间、用户与业务交互数据所涉及的第三方的即时信息交互的数据大小、用户与业务交互数据所涉及的第三方的即时信息交互结束至发起业务交互数据的间隔时间是否均落入对应的安全阈值范围内，即是上述三个维度均要落入对应的安全阈值范围内，才表示该业务交互数据安全。

[0091] 如图 2 所示，在本申请一实施方式中，所述装置还包括模型建构模块 300，其用于：

[0092] 获取用户在第一时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

[0093] 计算在第一时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第一平均值或第一方差；

[0094] 获取用户在第二时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值；

[0095] 计算在第二时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第二平均值或第二方差；

[0096] 将所述第一平均值或第一方差和所述第二平均值或第二方差，或所述第一平均值和第二平均值的差值，运用决策树计算出与每个预设维度对应的安全阈值范围并构建与用户对应的风险模型 400，其中，第一时间区间长度大于第二时间区间。

[0097] 下面以一具体示例进行说明：

[0098] 先以用户 ID 为主键获取用户一年内所有或指定平台上的交易前和卖家的聊天记录，包括：用户和卖家交流的时间长度、和卖家交流的记录数据大小，以及和卖家交流完成到发起支付的间隔时间。

[0099] 再选取在过去网络交易业务满足一定条件（比如网络交易业务数量大于或等于预设数量）的用户。并逐个对选取出用户的用户和卖家交流的时间长度、和卖家交流的记录数据大小、和卖家交流完成到发起支付的间隔时间分别做聚合。

[0100] 如此，可得到每个选取的用户和卖家交流的时间长度的平均值或方差、和卖家交流的记录数据大小的平均值或方差、和卖家交流完成到发起支付的间隔时间的平均值或方差。即可到用户在发起业务交互数据（交易支付前）和卖家交流的历史行为数据。

[0101] 然后，选取新的一段时间（比如 1 个月）内的交易前和卖家的聊天记录作为样本，按照上述方式，得到每个选取用户在这段时间内和卖家交流的时间长度的平均值或方差、和卖家交流的记录数据大小的平均值或方差、和卖家交流完成到发起支付的间隔时间的平均值或方差。即可得到样本行为数据。当然，该样本行为数据的计算也可在历史行为数据的计算前或同时进行。

[0102] 这样，可根据上述历史行为数据和样本行为数据，并运用决策树建构风险模型400；当然，也可先计算样本行为数据与上述历史行为数据中相应数据的偏差的绝对值，再根据所述绝对值，运用决策树构建风险模型400，该风险模型400可定义每个预设维度（用户和卖家交流的时间长度、和卖家交流的记录数据大小、和卖家交流完成到发起支付的间隔时间）对应的安全阈值范围。

[0103] 综上所述，本申请通过用户在发起业务交互数据前的历史行为，构建业务交互数据的风险模型，以通过该风险模型判断当前业务交互数据的安全性，降低了对用户的打扰率，提升网络通信效率。

[0104] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的装置，装置和模块的具体工作过程，可以参考前述方法实施方式中的对应过程，在此不再赘述。

[0105] 在本申请所提供的几个实施方式中，应该理解到，所揭露的装置，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施方式仅仅是示意性的，例如，所述模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个模块或组件可以结合或者可以集成到另一个装置，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或模块的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0106] 所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施方式方案的目的。

[0107] 另外，在本申请各个实施方式中的各功能模块可以集成在一个处理模块中，也可以是各个模块单独物理存在，也可以2个或2个以上模块集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用硬件加软件功能模块的形式实现。

[0108] 上述以软件功能模块的形式实现的集成的模块，可以存储在一个计算机可读取存储介质中。上述软件功能模块存储在一个存储介质中，包括若干指令用以使得一台计算机装置（可以是个人计算机，服务器，或者网络装置等）或处理器（processor）执行本申请各个实施方式所述方法的部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0109] 最后应说明的是：以上实施方式仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施方式对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施方式所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施方式技术方案的精神和范围。

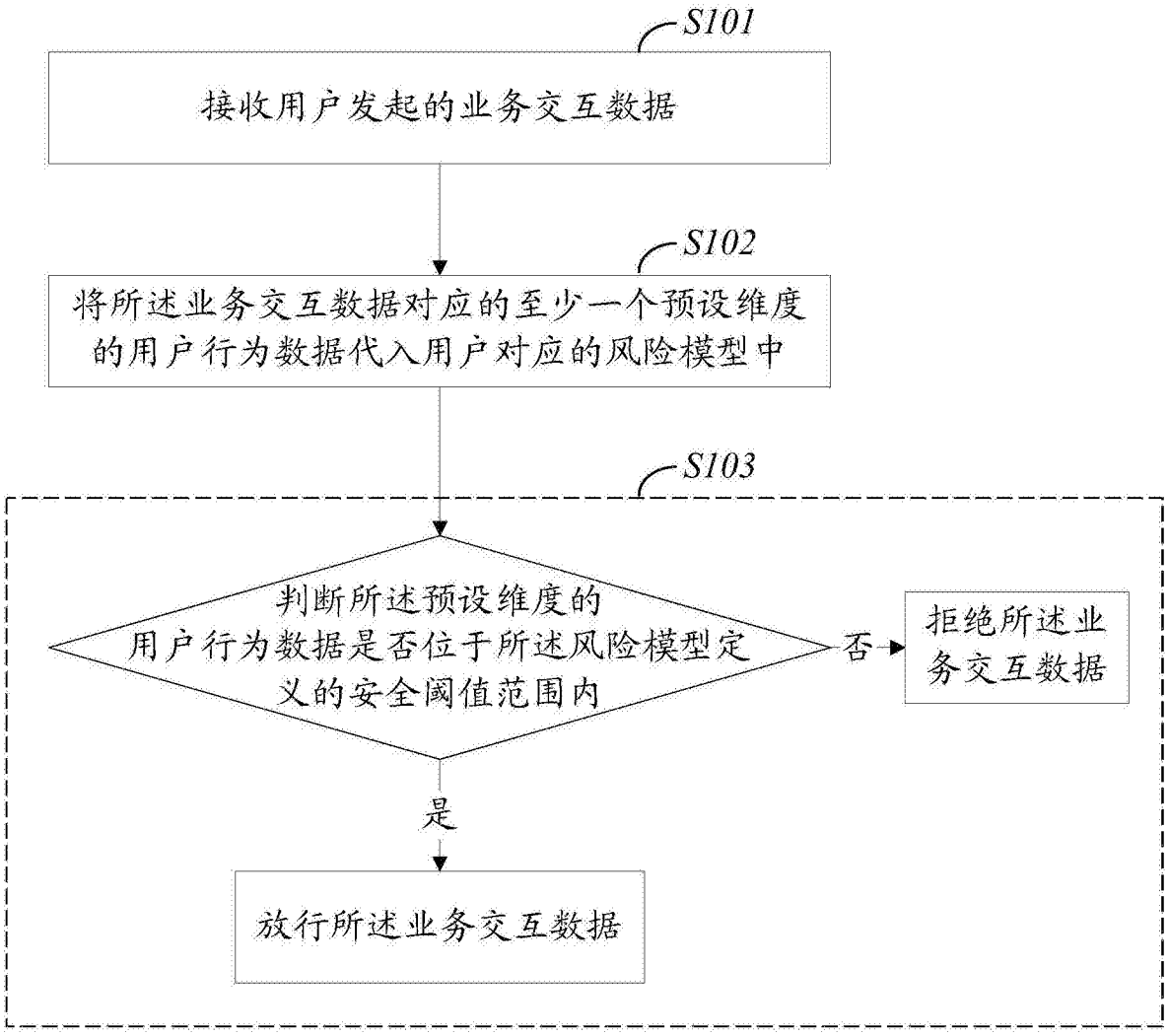

S101
接收用户发起的业务交互数据
S102
将所述业务交互数据对应的至少一个预设维度的用户行为数据代入用户对应的风险模型中
S103
判断所述预设维度的用户行为数据是否位于所述风险模型定义的安全阈值范围内
否
拒绝所述业务交互数据
是
放行所述业务交互数据

图 1

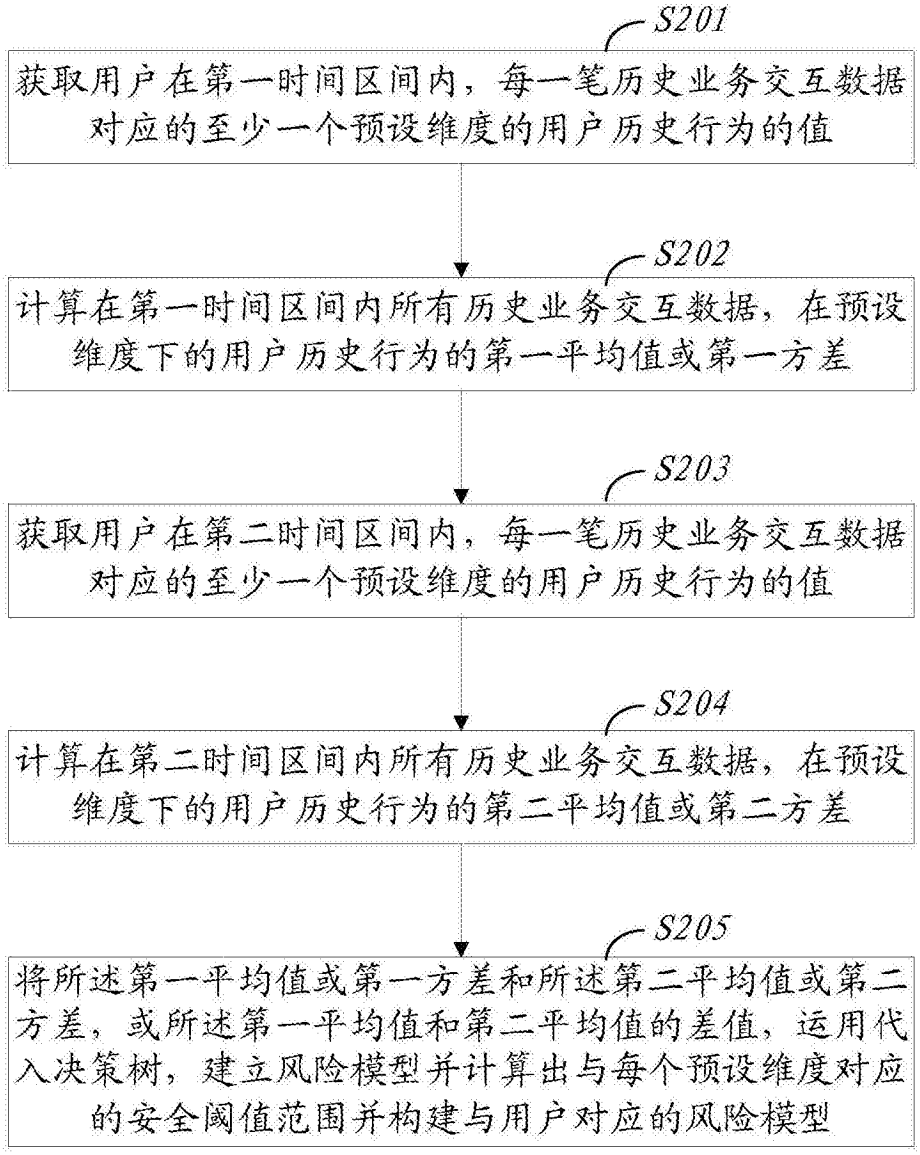

S201
获取用户在第一时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值
S202
计算在第一时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第一平均值或第一方差
S203
获取用户在第二时间区间内，每一笔历史业务交互数据对应的至少一个预设维度的用户历史行为的值
S204
计算在第二时间区间内所有历史业务交互数据，在预设维度下的用户历史行为的第二平均值或第二方差
S205
将所述第一平均值或第一方差和所述第二平均值或第二方差，或所述第一平均值和第二平均值的差值，运用代入决策树，建立风险模型并计算出与每个预设维度对应的安全阈值范围并构建与用户对应的风险模型

图 2

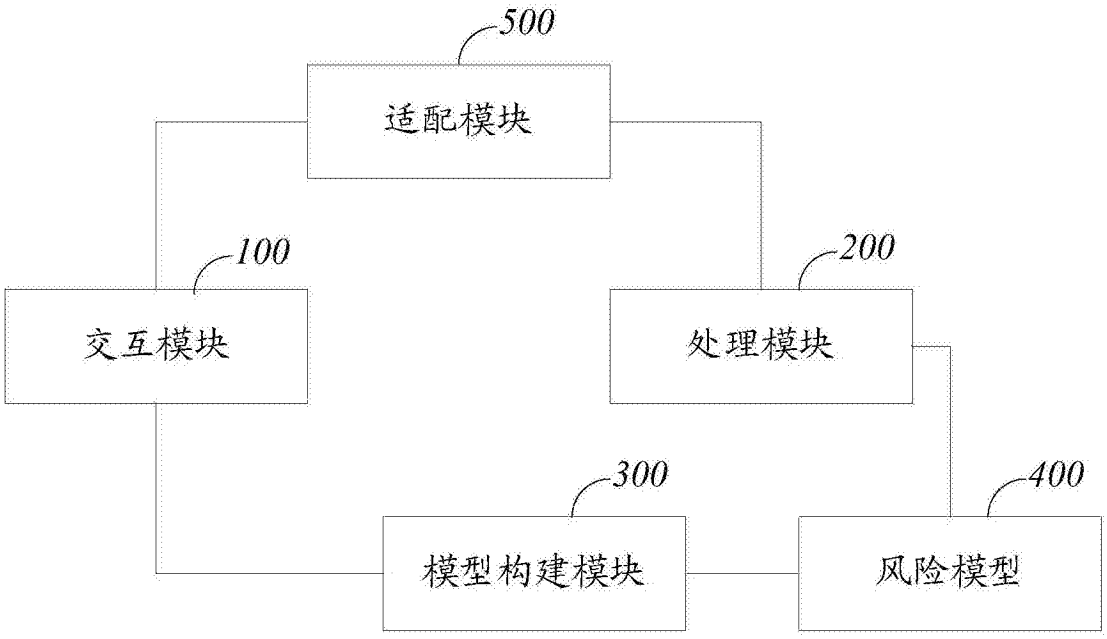


图 3