(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 111784348 A
(43)申请公布日 2020.10.16

(21)申请号 202010507603.6

(22)申请日 2016.04.26

(62)分案原申请数据
201610266814.9 2016.04.26

(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 洪满伙

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 周嗣勇

(51)Int.Cl.
G06Q 20/40(2012.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)

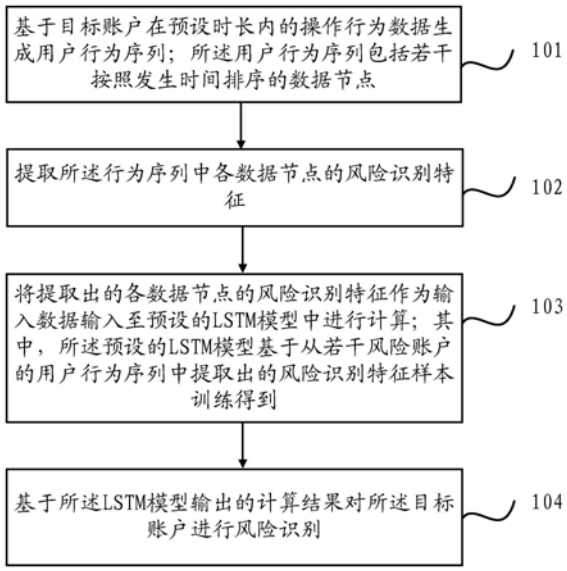
权利要求书2页 说明书14页 附图5页

(54)发明名称

账户风险识别方法及装置

(57)摘要

本申请提供一种账户风险识别方法及装置，其中的方法包括：基于目标账户在预设时长内的操作行为数据生成用户行为序列；所述用户行为序列包括若干按照发生时间排序的数据节点；提取所述行为序列中各数据节点的风险识别特征；将提取出的各数据节点的风险识别特征作为输入数据输入至预设的长短期记忆LSTM模型中进行计算；其中，所述预设的LSTM模型基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到；基于所述LSTM模型输出的计算结果对所述目标账户进行风险识别。本申请可以从整体上提升对目标账户进行风险评估的灵敏度和准确度。



CN 111784348 A

1.一种账户风险识别方法,该方法包括:

基于目标账户在预设时长内的操作行为数据生成用户行为序列;所述用户行为序列包括若干按照发生时间排序的数据节点;

提取所述行为序列中各数据节点的风险识别特征;

将所述各数据节点的风险识别特征作为输入数据,按照发生时间顺序依次输入至预设的LSTM模型进行计算,并将前一数据节点的计算结果与下一数据节点的风险识别特征进行加权求和后继续进行计算,直到所述各数据节点的风险识别特征在所述LSTM模型中均计算完成;其中,所述预设的LSTM模型为基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到的风险识别模型;

基于所述LSTM模型输出的计算结果对所述目标账户进行风险识别。

2.根据权利要求1所述的方法,所述基于目标账户在预设时长内的操作行为数据生成行为序列包括:

采集目标账户在预设时长内的操作行为数据;

基于预设时间周期将采集到的所述操作行为数据划分为若干数据集合;

将划分出的所述若干数据集合分别作为数据节点按照发生时间进行排序以生成所述行为序列。

3.根据权利要求1所述的方法,所述基于目标账户在预设时长内的操作行为数据生成行为序列包括:

采集目标账户的操作行为数据;

确定所述操作行为数据是否包含指定的关键行为;

当所述操作行为数据中包含指定的关键行为时,采集该目标账户在所述指定的关键行为的发生时间以前预设时长内产生的所有关键行为数据;

将采集到的所有关键行为数据分别作为数据节点按照发生时间进行排序以生成所述行为序列。

4.根据权利要求1所述的方法,所述数据节点包括若干按照发生时间排序的操作行为数据;

所述提取所述行为序列中各数据节点的风险识别特征包括:

提取与所述行为序列中各数据节点中的操作行为数据关联的风险评估信息,作为所述风险识别特征;其中,所述风险评估信息包括与所述目标账户相关的风险评估信息,以及与所述目标账户对应的业务对端账户相关的风险评估信息;或者

判定所述行为序列中各数据节点中的操作行为数据是否具有设定的风险特征,并对判定结果进行编码,将编码得到的字符串作为所述风险识别特征。

5.根据权利要求1所述的方法,所述方法还包括:

在指定的数据节点或者在检测到指定的关键行为时,输出所述LSTM模型的计算结果。

6.根据权利要求1所述的方法,搭载所述LSTM模型的硬件处理器为GPU。

7.根据权利要求1所述的方法,所述用户行为序列中已发生的数据节点的风险识别特征在所述风险识别模型中进行离线计算,所述离线计算的结果与所述用户行为序列中最新的数据节点的风险识别特征在所述风险识别模型中进行实时计算。

8.一种账户风险识别装置,该装置包括:

生成模块，用于基于目标账户在预设时长内的操作行为数据生成用户行为序列；所述用户行为序列包括若干按照发生时间排序的数据节点；

提取模块，用于提取所述行为序列中各数据节点的风险识别特征；

计算模块，用于将所述各数据节点的风险识别特征作为输入数据，按照发生时间顺序依次输入至预设的LSTM模型进行计算，并将前一数据节点的计算结果与下一数据节点的风险识别特征进行加权求和后继续进行计算，直到所述各数据节点的风险识别特征在所述LSTM模型中均计算完成；其中，所述预设的LSTM模型为基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到的风险识别模型；

识别模块，用于基于所述LSTM模型输出的计算结果对所述目标账户进行风险识别。

9.根据权利要求8所述的装置，所述生成模块具体用于：

采集目标账户在预设时长内的操作行为数据；

基于预设时间周期将采集到的所述操作行为数据划分为若干数据集合；

将划分出的所述若干数据集合分别作为数据节点按照发生时间进行排序以生成所述行为序列。

10.根据权利要求8所述的装置，所述生成模块具体用于：

采集目标账户的操作行为数据；

确定所述操作行为数据是否包含指定的关键行为；

当所述操作行为数据中包含指定的关键行为时，采集该目标账户在所述指定的关键行为的发生时间以前预设时长内产生的所有关键行为数据；

将采集到的所有关键行为数据分别作为数据节点按照发生时间进行排序以生成所述行为序列。

11.根据权利要求8所述的装置，所述数据节点包括若干按照发生时间排序的操作行为数据；

所述提取模块具体用于：

提取与所述行为序列中各数据节点中的操作行为数据关联的风险评估信息，作为所述风险识别特征；其中，所述风险评估信息包括与所述目标账户相关的风险评估信息，以及与所述目标账户对应的业务对端账户相关的风险评估信息；或者

判定所述行为序列中各数据节点中的操作行为数据是否具有设定的风险特征，并对判定结果进行编码，将编码得到的字符串作为所述风险识别特征。

12.根据权利要求8所述的装置，所述装置还包括：

输出模块，用于在指定的数据节点或者在检测到指定的关键行为时，输出所述LSTM模型的计算结果。

13.根据权利要求8所述的装置，搭载所述LSTM模型的硬件处理器为GPU。

14.根据权利要求8所述的装置，所述用户行为序列中已发生的数据节点的风险识别特征在所述风险识别模型中进行离线计算，所述离线计算的结果与所述用户行为序列中最新的数据节点的风险识别特征在所述风险识别模型中进行实时计算。

账户风险识别方法及装置

技术领域

[0001] 本申请涉及通信领域，尤其涉及一种账户风险识别方法及装置。

背景技术

[0002] 在现有的交易风险防范体系中，已经广泛使用交易模型来防范风险。通过提供大量风险交易作为训练样本，并从这些风险交易中提取风险特征进行训练，来构建交易模型，然后使用构建完成的交易模型来对用户的交易账户进行风险预测和评估。然而，在现有的交易风险防范体系中，交易模型的训练阶段所使用到的特征变量通常均为一些离散的特征，已逐渐无法满足实际的交易风险防范需求。

发明内容

[0003] 本申请提出一种账户风险识别方法，该方法包括：

[0004] 基于目标账户在预设时长内的操作行为数据生成用户行为序列；所述用户行为序列包括若干按照发生时间排序的数据节点；

[0005] 提取所述行为序列中各数据节点的风险识别特征；

[0006] 将提取出的各数据节点的风险识别特征作为输入数据输入至预设的长短期记忆LSTM模型中进行计算；其中，所述预设的LSTM模型基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到；

[0007] 基于所述LSTM模型输出的计算结果对所述目标账户进行风险识别。

[0008] 可选的，所述基于目标账户在预设时长内的操作行为数据生成行为序列包括：

[0009] 采集目标账户在预设时长内的操作行为数据；

[0010] 基于预设时间周期将采集到的所述操作行为数据划分为若干数据集合；

[0011] 将划分出的所述若干数据集合分别作为数据节点按照发生时间进行排序以生成所述行为序列。

[0012] 可选的，所述基于目标账户在预设时长内的操作行为数据生成行为序列包括：

[0013] 采集目标账户的操作行为数据；

[0014] 确定所述操作行为数据是否包含指定的关键行为；

[0015] 当所述操作行为数据中包含指定的关键行为时，采集该目标账户在所述指定的关键行为的发生时间以前预设时长内产生的所有关键行为数据；

[0016] 将采集到的所有关键行为数据分别作为数据节点按照发生时间进行排序以生成所述行为序列。

[0017] 可选的，所述数据节点包括若干按照发生时间排序的操作行为数据；

[0018] 所述提取所述行为序列中各数据节点的风险识别特征包括：

[0019] 提取与所述行为序列中各数据节点中的操作行为数据关联的风险评估信息，作为所述风险识别特征；其中，所述风险评估信息包括与所述目标账户相关的风险评估信息，以及与所述目标账户对应的业务对端账户相关的风险评估信息；或者

[0020] 判定所述行为序列中各数据节点中的操作行为数据是否具有设定的风险特征，并对判定结果进行编码，将编码得到的字符串作为所述风险识别特征。

[0021] 可选的，所述将提取出的各数据节点的风险识别特征作为输入数据输入至预设的LSTM模型中进行计算包括：

[0022] 将所述各数据节点的风险识别特征作为输入数据，按照发生时间顺序依次输入至所述LSTM模型进行计算，并将前一数据节点的计算结果与下一数据节点的风险识别特征进行加权求和后继续进行计算，直到所述各数据节点的风险识别特征在所述LSTM模型中均计算完成；

[0023] 其中，所述用户行为序列中已发生的数据节点的风险识别特征在所述风险识别模型中进行离线计算，所述离线计算的结果与所述用户行为序列中最新的数据节点的风险识别特征在所述风险识别模型中进行实时计算。

[0024] 可选的，所述方法还包括：

[0025] 在指定的数据节点或者在检测到指定的关键行为时，输出所述LSTM模型的计算结果。

[0026] 可选的，搭载所述LSTM模型的硬件处理器为GPU。

[0027] 本申请还提出一种账户风险识别装置，该装置包括：

[0028] 生成模块，用于基于目标账户在预设时长内的操作行为数据生成用户行为序列；所述用户行为序列包括若干按照发生时间排序的数据节点；

[0029] 提取模块，用于提取所述行为序列中各数据节点的风险识别特征；

[0030] 计算模块，用于将提取出的各数据节点的风险识别特征作为输入数据输入至预设的LSTM模型中进行计算；其中，所述预设的LSTM模型基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到；

[0031] 识别模块，用于基于所述LSTM模型输出的计算结果对所述目标账户进行风险识别。

[0032] 可选的，所述生成模块具体用于：

[0033] 采集目标账户在预设时长内的操作行为数据；

[0034] 基于预设时间周期将采集到的所述操作行为数据划分为若干数据集合；

[0035] 将划分出的所述若干数据集合分别作为数据节点按照发生时间进行排序以生成所述行为序列。

[0036] 可选的，所述生成模块具体用于：

[0037] 采集目标账户的操作行为数据；

[0038] 确定所述操作行为数据是否包含指定的关键行为；

[0039] 当所述操作行为数据中包含指定的关键行为时，采集该目标账户在所述指定的关键行为的发生时间以前预设时长内产生的所有关键行为数据；

[0040] 将采集到的所有关键行为数据分别作为数据节点按照发生时间进行排序以生成所述行为序列。

[0041] 可选的，所述数据节点包括若干按照发生时间排序的操作行为数据；

[0042] 所述提取模块具体用于：

[0043] 提取与所述行为序列中各数据节点中的操作行为数据关联的风险评估信息，作为

所述风险识别特征;其中,所述风险评估信息包括与所述目标账户相关的风险评估信息,以及与所述目标账户对应的业务对端账户相关的风险评估信息;或者

[0044] 判定所述行为序列中各数据节点中的操作行为数据是否具有设定的风险特征,并对判定结果进行编码,将编码得到的字符串作为所述风险识别特征。

[0045] 可选的,所述计算模块具体用于

[0046] 将所述各数据节点的风险识别特征作为输入数据,按照发生时间顺序依次输入至所述LSTM模型中进行计算,并将前一数据节点的计算结果与下一数据节点的风险识别特征进行加权求和后继续进行计算,直到所述各数据节点的风险识别特征在所述LSTM模型中均计算完成;

[0047] 其中,所述用户行为序列中已发生的数据节点的风险识别特征在所述风险识别模型中进行离线计算,所述离线计算的结果与所述用户行为序列中最新的数据节点的风险识别特征在所述风险识别模型中进行实时计算。

[0048] 可选的,所述装置还包括:

[0049] 输出模块,用于在指定的数据节点或者在检测到指定的关键行为时,输出所述LSTM模型的计算结果。

[0050] 可选的,搭载所述LSTM模型的硬件处理器为GPU。

[0051] 本申请中,通过基于目标账户在预设时长内的操作行为数据生成用户行为序列,并提取该行为序列中各数据节点的风险识别特征,将提取出的各数据节点的风险识别特征作为输入数据输入至基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到的LSTM模型中进行计算,然后基于该LSTM模型输出的计算结果对所述目标账户进行风险识别,实现了可以基于若干风险账户在预设时长内的行为序列来构建用于风险账户识别的LSTM模型,并通过构建的LSTM模型对从用户的行为序列中提取出的风险识别特征进行计算,来对目标账户进行风险评估;由于在构建LSTM模型以及使用LSTM模型时充分考虑了风险识别特征间的时序关系,构建模型以及使用模型时所输入的特征变量将不再是零散的特征变量,因此可以从整体上提升对目标账户进行风险评估的灵敏度和准确度。

附图说明

[0052] 图1是本申请一实施例提供的一种账户风险识别方法的流程图;

[0053] 图2是本申请一实施例提供的一种风险识别模型的架构图;

[0054] 图3是本申请一实施例提供的一种风险识别模型的架构图;

[0055] 图4是本申请一实施例提供的一种风险识别模型的架构图;

[0056] 图5是本申请一实施例提供的一种风险识别模型的架构图;

[0057] 图6是本申请一实施例提供的一种风险识别模型的架构图;

[0058] 图7是本申请一实施例提供的一种账户风险识别装置的逻辑框图;

[0059] 图8是本申请一实施例提供的承载所述一种账户风险识别装置的服务端的硬件结构图。

具体实施方式

[0060] 在现有的交易风险防范体系中,通常可以通过提供大量风险账户作为训练样本,

并从这些风险交易中提取风险特征作为特征变量进行训练，来构建用于对用户的交易账户进行风险预测和评估的交易模型。

[0061] 当使用交易模型对用户的交易账户进行风险预测和评估时，可以从用户发起的交易中提取与构建交易模型时所使用的风险特征维度相同的交易特征作为特征变量，然后输入至交易模型基于交易模型的算法进行计算，通过计算结果(通常为该交易为风险交易的概率值)对本次交易进行风险预测和评估。

[0062] 然而，现有交易风险防范体系中的交易模型，至少存在以下不足：

[0063] 第一，现有的交易模型通常具有实时性的要求，需要在用户确认付款至用户感知到交易付款成功的间隙(时间以毫秒记)作出实时响应，因此需要在交易模型中计算的特征变量数据往前追溯的时间不能太长，一旦过长，数量量过大可能就不能满足实时性的要求。

[0064] 第二，现有的交易模型在训练阶段以及使用阶段所使用的特征变量，并通常均为一些离散的特征(比如可以包括用户登录特征，当前交易特征，以及用户历史操作特征等)，并不能有效的反映不同时间点的特征变量之间的时序关系；例如，并不能有效的反映出用户几个月以前的登录、浏览及交易等环节的特征信息与当前登录、浏览、交易环节的特征信息之间的时序关系。

[0065] 因此，鉴于以上的不足，现有的交易模型在一些特殊的风险防范场景中，比如囤号风险，可能无法满足实际的风险防范需求。

[0066] 所谓囤号风险，是指非法用户在盗取用户的账户后，并不急于把该账户的资金迅速转走，而是通过小金额操作等多种手段(比如给正常用户进行小额度充值)进行长期尝试(比如可能长达数月)，以绕过交易模型的风险监控，并在绕过交易模型的风险监控后潜伏一段时间，然后再逐步提升转移资金的额度，使得被盗账号损失严重。

[0067] 囤号风险之所以防范难度较大，在于在线交易的数据处理量通常极大，盗号者前期小金额的试探性交易一旦未能被交易模型有效防范，那么这些小金额的试探性交易就会混入正常的用户交易中，随着正常的用户交易的数量不断增长，后续针对这些交易的识别难度就会增大，可能会造成对这类风险交易防范不及时而对用户的资金造成损失。

[0068] 可见，基于现有的交易模型针对囤号风险交易进行风险防范时，由于交易模型中计算处理的特征变量的追溯周期有限，并且所使用的特征变量为离散的特征，并不能有效的反映不同时间点的特征变量之间的时序关系的时序关系，因此对于盗号初期那些小金额的试探性交易无法进行及时识别，从而可能会导致对囤号风险交易防范不及时而对用户的资金造成损失。

[0069] 有鉴于此，本申请提出一种账户风险识别方法，通过基于目标账户在预设时长内的操作行为数据生成用户行为序列，并提取该行为序列中各数据节点的风险识别特征，将提取出的各数据节点的风险识别特征作为输入数据输入至基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到的LSTM模型中进行计算，然后基于该LSTM模型输出的计算结果对所述目标账户进行风险识别，实现了可以基于若干风险账户在预设时长内的行为序列来构建用于风险账户识别的LSTM模型，并通过构建的LSTM模型对从用户的行为序列中提取出的风险识别特征进行计算，来对目标账户进行风险评估；由于在构建LSTM模型以及使用LSTM模型时充分考虑了风险识别特征间的时序关系，构建模型以及使用模型时所输入的特征变量将不再是零散的特征变量，因此可以从整体上提升对目标账户进

行风险评估的灵敏度和准确度。

[0070] 下面通过具体实施例并结合具体的应用场景对本申请进行描述。

[0071] 请参考图1,图1是本申请一实施例提供的一种账户风险识别方法,应用于服务端,所述方法执行以下步骤:

[0072] 步骤101,基于目标账户在预设时长内的操作行为数据生成用户行为序列;所述用户行为序列包括若干按照发生时间排序的数据节点;

[0073] 步骤102,提取所述行为序列中各数据节点的风险识别特征;

[0074] 步骤103,将提取出的各数据节点的风险识别特征作为输入数据输入至预设的LSTM模型中进行计算;其中,所述预设的LSTM模型基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到;

[0075] 步骤104,基于所述LSTM模型输出的计算结果对所述目标账户进行风险识别。

[0076] 上述目标账户,可以包括用户的支付账户,用户可以通过在相应的支付客户端(比如支付APP)上登录目标账户来发起支付交易。

[0077] 上述服务端,可以包括面向用户的支付客户端提供服务,对用户登录客户端所使用的支付账号进行风险识别的服务器、服务器集群或者基于服务器集群构建的云平台。

[0078] 上述操作行为数据,可以包括用户在客户端上登录目标账户后执行的一系列与交易相关的操作行为而产生的数据;例如,上述操作行为可以包括用户的登录、绑定手机、修改密码、绑定银行卡、充值、交易创建以及付款等用户在执行交易的过程中各环节的操作行为,客户端在检测到上述操作行为后,可以将客户端在执行上述操作行为产生的数据上传至服务端,由服务端在本地的数据库中作为事件进行保存。

[0079] 在本例中,可以预先提供大量已标定出的风险账户,并针对这些风险账户在预设时长内的用户操作行为数据生成用户行为序列,然后从生成的这些用户行为序列中提取风险识别特征作为训练样本进行深度学习训练,来构建LSTM(Long-Short Term Memory,长短期记忆)模型。

[0080] 当上述LSTM模型构建完成后,在基于该LSTM模型对目标账户进行风险识别时,可以按照相同的方式,针对目标账户在预设时长内的用户操作行为数据生成用户行为序列,从生成的该用户行为序列中提取风险识别特征作为特征变量,并将提取出的特征变量作为输入数据输入至该LSTM模型中进行计算,然后基于计算结果来对该目标账户进行风险识别。

[0081] 由于在构建LSTM模型以及使用LSTM模型时所使用的特征变量均为基于用户行为序列提取出的风险识别特征,充分考虑了不同时间点上特征变量之间的时序关系,因此在构建模型以及使用模型时输入的特征变量将不再是零散的特征,从而可以从整体上提升对目标账户进行风险评估的灵敏度和准确度。

[0082] 以下结合服务端对目标账户发起的交易进行风险识别的应用场景对本申请的技术方案进行详细描述。

[0083] 请参见图2,图2为本例示出的一种LSTM模型的架构图。

[0084] 本例中示出的该LSTM模型,是一种基于LSTM网络搭建的,可以在模型中对具有时序关系的连续的特征样本进行记忆的深度学习模型,在实际应用中,可以作为风险识别模型对用户的目标账户进行风险识别。

[0085] 请继续参见图2,在本例中,该LSTM模型为一种三层模型,可以包括输入层、记忆层(也称为隐藏层)和输出层。

[0086] 需要说明的是,在实际应用中,该LSTM模型的层数并不限定为三层,本领域技术人员可以根据实际的深度学习需求,在本例中示出的三层架构的基础上适当增加模型的层数。

[0087] 1)输入层

[0088] 上述输入层,用于接收从用户行为序列中提取到的风险识别特征,可以包括若干个数据节点,每一个数据点都可以作为输入层的一个数据输入源。

[0089] 其中,对于输入层来说,包含的数据节点的个数,以及各数据节点需要输入的风险识别特征,均可以由LSTM模型的设计者根据具体的风险评估需求来进行设计。

[0090] 一方面,上述输入层的数据节点的个数,通常取决于上述风险识别模型的时序设计。

[0091] 在示出的一种时序设计中,可以采用设定的时间周期来组织序列。

[0092] 上述模型的设计者可以为用户行为序列设定一个预设时长(比如3个月),此时上述用户行为序列可以基于该预设时长内的所有操作行为数据生成。同时,上述模型的设计者还可以设定一个用于组织序列的时间周期(比如该时间周期可以为小时、天、周或者月),然后基于设定的该时间周期对上述预设时长内的操作行为数据进行划分,得到若干数据集合(每一个时间周期产生的操作行为数据为一个数据集合),并按照发生时间将各数据集合作为数据节点进行排序,以生成用户行为序列。

[0093] 此时生成的用户行为序列包括按照发生时间排序的若干数据节点,每一个数据节点中包括若干按照发生时间排序的操作行为数据。其中,不同的数据节点中包含的操作行为数据可以互不相同。

[0094] 请参见图3,图3为本例中示出的一种按天组织时序的LSTM模型的架构图。

[0095] 假设模型的设计者设定的用户行为序列的长度为90天,设定的时间周期为按天组织序列,那么可以将用户在这90天内的操作行为数据按天划分为90个数据节点,此时每一天的操作行为数据都为输入层的一个输入源。

[0096] 在示出的一种时序设计中,可以采用设定的关键行为来组织序列。

[0097] 上述模型的设计者可以设定若干关键行为,其中上述关键行为可以包括日常交易过程中可以用于对交易风险进行评估的操作行为;例如,上述关键行为可以包括在日常交易过程中的“登录”、“修改密码”、“创建交易”以及“支付”等操作行为。

[0098] 同时,上述模型的设计者,还可以为用户行为序列设定一个预设时长,在组织序列时,可以读取预设时长内的所有关键行为数据,然后将读取到的所有关键行为数据分别作为一个数据节点,按照发生时间对所有数据节点进行排序,以生成用户行为序列。此时生成的用户行为序列仍然包括按照发生时间排序的若干数据节点,每一个数据节点中包括若干按照发生时间排序的关键行为数据。

[0099] 其中,需要说明的是,对于风险识别模型来说,通常都会具有实时的响应用户的关键操作行为的需求;例如,当利用风险识别模型对用户通过目标账户发起的交易进行风险识别时,模型可以在用户发起的这笔交易最终的支付环节来进行响应,实时的对本次交易进行风险评估。

[0100] 因此，上述LSTM模型的设计者，在基于设定的关键行为来设计时点特征组织序列时，可以从设定的若干关键行为中指定一个关键行为(例如可以将支付这种操作行为指定为关键行为)，该指定的该关键行为即为模型的响应节点，模型会在检测到该指定的关键行为时，输出最终的计算结果。

[0101] 当从设定的若干关键行为中指定出关键行为后，在基于关键行为组织时序时，可以采集目标账户在该指定的关键行为的发生时间以前预设时长内的产生的所有关键行为数据，并将采集到的所有关键行为数据分别作为数据节点，按照发生时间进行排序，以生成上述用户行为序列。

[0102] 请参见图4，图4为本例中示出的一种基于关键行为组织时序的LSTM模型的架构图。

[0103] 假设模型的设计者设定的用户行为序列的长度为90天，设定的关键行为“登录”、“修改密码”、“创建交易”以及“支付”等日常交易过程中的关键行为，其中关键行为“支付”为指定的关键行为，作为模型的响应节点，那么可以采集“支付”这一关键行为的发生时间以前90天内，用户的目标账户产生的所有关键行为数据，此时采集到的每一个关键行为数据均为一个独立的数据节点，每一个关键行为数据都为输入层的一个输入源。

[0104] 当然，在实际应用中，除了以上描述的时序设计，也可以基于其它策略来设计时序，在本例中不在进行一一详述。

[0105] 另一方面，当完成时序设计，确定出上述LSTM模型输入层的数据节点的个数后，则可以进一步确定每一个数据节点上需要输入的风险识别特征。

[0106] 其中，上述输入层上各数据节点需要输入的风险识别特征，通常取决于上述LSTM模型的时点特征设计。

[0107] 在示出的一种时点特征设计中，可以将与各数据节点中的操作行为数据关联的风险评估信息作为当前数据节点的风险识别特征。

[0108] 其中，上述风险评估信息可以包括与目标账户相关的风险评估信息，以及与上述目标账户对应的交易对端账户相关的风险评估信息。

[0109] 例如，在现有的风险防范体系中，对于目标账户的用户行为序列中的每一次用户操作行为(尤其是一些关键行为)，都会由服务端来分别进行风险评估。在针对用户操作行为进行风险评估时，通常不仅需要对该目标账户进行风险评估，同时也需要基于账户关系针对该目标账户的关联账户进行风险评估，当目标账户所属的交易本端与目标账户对应的交易对端账户所属的交易对端任意一方存在交易风险时，都会由服务端将当前的用户操作行为判断为风险操作。

[0110] 因此，服务端在针对用户操作行为进行风险评估时，可以针对该目标账户的交易本端以及与该目标账户对应的交易对端账户所属的交易对端分别进行风险评估，以得到与目标账户相关的风险评估信息，以及与上述目标账户对应的交易对端账户相关的风险评估信息。

[0111] 在实际应用中，上述风险评估信息具体可以是服务端在进行风险评估后得到的风险评分。服务端在针对目标账户的用户行为序列中的用户操作行为进行风险评估时，可以基于预设的风险评估策略从不同维度来分别进行风险评估。其中，服务端上的上述风险评估策略，可以根据实际的风险评估需求进行制定，在本例中不再详述，本领域技术人员在将

本申请的技术方案付诸实施时，可以参考相关技术中的记载。

[0112] 请参见图5，图5为本例中示出的一种将风险评分作为时点特征的LSTM模型的架构图。

[0113] 在图5示出的模型架构中，服务端在针对目标账户的用户行为序列中的用户操作行为进行风险评估时，可以分别基于账户、所在设备、所在设备的网络环境等多个维度针对目标账户和上述交易对端账户分别进行风险评估，得到目标账户的评分、目标账户的设备评分、目标账户的环境评分、交易对端账户的评分、交易对端账户的设备评分以及交易对端账户的环境评分。

[0114] 例如，服务端在基于预设的风险评估策略针对账户进行评分时，可以综合考虑当前账户是否异地登录、是否频繁登录等多种因素进行综合评分，如果出现异地登录、频繁登录则相应的降低评分；在针对设备进行评分时，可以综合考虑该设备的使用用户是否较多等因素，如果该设备的使用用户较多，比如网吧中的PC设备，则可以判定该设备安全风险较大，可以相应的降低评分；在针对环境进行评分时，可以综合考虑当前网络环境中的IP地址、安全扫描结果等因素进行综合评分，如果当前网络环境中的IP地址为防火墙管控的黑名单中IP地址，或者当前网络环境安全扫描结果较差，则可以相应的降低评分。

[0115] 当然，除了以上描述的服务端可以基于账户、所在设备、所在设备的网络环境等多个维度针对目标账户和上述交易对端账户分别进行风险评估以外，在实际应用中也可以通过其它维度针对目标账户和上述交易对端账户进行评分，在本例中不再进行一一详述，本领域技术人员在将本申请的技术方案付诸实施时，可以参考相关技术中的记载。

[0116] 在示出的另一种时点特征设计中，可以判定各数据节点中的操作行为数据是否具有设定的风险特征，并对判定结果进行编码，然后将编码得到的字符串作为各数据节点的风险识别特征。

[0117] 在本例中，在针对各数据节点进行时点特征设计时，可以针对各数据节点分别设定若干组风险特征，其中上述风险特征可以包括能够用于对各数据节点中的操作行为进行风险评估的特征；例如，在实现时，上述风险特征可以包括交易次数是否达到N次、是否异地登录、是否频繁登录、是否修改密码等交易特征。

[0118] 当为各数据节点设定了若干组风险特征后，可以判定各数据节点中的操作行为数据是否具有设定的风险特征，然后对判定结果进行编码；例如，可以采用0、1编码的方式，具有某种设定的风险特征则编码为1，不具有某种设定的风险特征则编码为0，最终编码完成得到一个由0和1组成的字符串。当编码完成后，可以将编码完成的字符串作为当前数据节点需要输入的风险识别特征。当然，如果任一数据节点中的操作行为数据均不具有设定的风险特征，此时该数据节点的风险识别特征可以为空值。

[0119] 其中，需要说明的是，在为各数据节点设置风险特征时，可以为各数据节点设置统一的风险特征，也可以针对不同的数据节点分别设置不同的风险特征。

[0120] 例如，在如图3所示出的基于预设时间周期来组织时序的模型架构中，各数据节点中可能会包含相同的操作行为，因此在这种情况下，可以针对各数据节点分别设置统一的风险特征；比如，该风险特征可以是当天的交易次数是否达到N次等交易特征。

[0121] 又如，在如图4所示出的基于关键行为组织时序的模型架构中，由于不同的数据节点包含的关键行为特征均不相同，因此在这种情况下，可以针对各数据节点对应的关键行

为的特点分别设置不同的风险特征;例如,对于与登录该关键行为对应的数据节点,为该数据节点设定的风险特征可以包括是否异地操作、是否频繁登录、密码是否过于简单、是否修改密码等风险特征。而对于与其它关键行为对应的数据节点,也可以结合当前数据节点对应的关键行为的特点,来相应设置风险特征,在本例中不再进行一一详述,本领域技术人员在将本申请的技术方案付诸实施时,可以参考相关技术中的记载。

[0122] 请参见图6,图6为本例中示出的一种将上述编码得到的字符串作为各数据节点的风险识别特征的LSTM模型的架构图。

[0123] 在图6示出的模型架构中,为输入层各数据节点设置了统一的四组风险特征,在确定各数据节点需要输入的风险识别特征时,可以采用0、1编码的方式,具有某种设定的风险特征则编码为1,不具有某种设定的风险特征则编码为0,然后将编码完成的字符串作为当前数据节点需要输入的风险识别特征。

[0124] 当然,在实际应用中,在针对模型设计时点特征时,也可以对以上描述的两种时点特征设计方案进行有机结合;比如,可以将风险评估评分作为一种风险特征,与设定的风险特征进行组合编码(组合顺序可以基于实际需求进行调整),然后将编码得到的字符串作为风险识别特征。

[0125] 2)记忆层

[0126] 上述记忆层,用于调用LSTM模型中的算法对输入层上各数据节点的风险识别特征进行计算。

[0127] 请继续参见图2,记忆层在进行计算时,可以按照发生时间顺序,对输入层上各数据节点的风险识别特征依次进行计算,并采用递归计算的方式,将前一数据节点的计算结果与下一数据节点输入的风险识别特征进行加权求和后继续进行计算,直到各数据节点的风险识别特征在所述LSTM模型中均计算完成。

[0128] 例如,记忆层可以按照发生时间的先后顺序,首先对发生时间最早的数据节点进行计算,当计算完成后将计算结果与下一个数据节点输入的风险识别特征进行加权求和继续进行计算,以此递归,直到所述数据节点的风险识别特征均计算完成。

[0129] 可见,通过这种方式,可以通过递归的方式,将用户行为序列中的各数据节点的风险识别特征按照发生时间在模型中完成记忆,从而可以对用户行为序列中的历史操作行为数据与最新的操作行为数据在模型中进行融合,由模型综合的完成风险评估。

[0130] 其中,记忆层在将前一数据节点的计算结果与后一数据节点的风险识别特征进行加权求和时,还可以通过设定加权比例,对前一数据节点计算结果中的部分信息进行筛除,以降低计算的数据处理量。

[0131] 在例中,由于用户行为序列中各数据节点可能携带大量的特征信息,而模型在处理较长的用户行为序列,可能会存在处理耗时较长而无法满足模型实时性需求的问题。

[0132] 一方面,为了满足模型实时性需求,记忆层在针对各数据节点的风险识别特征进行计算时,可以采用离线计算和实时计算相结合的方式。

[0133] 在示出的一种实施方式中,记忆层可以提前对用户行为序列中已发生的数据节点的风险识别特征在模型中进行离线预计算,当模型接收到了最新的数据节点,需要进行风险评估时,再将离线计算的结果实时导入线上生产系统,将上述离线计算结果与该用户行为序列中最新的数据节点的风险识别特征一起进行实时计算。

[0134] 通过这种方式，可以避免针对所有数据节点的风险识别特征均进行实时计算时，可能导致的处理耗时较长而无法满足模型实时性需求的问题。

[0135] 另一方面，为了满足模型实时性需求，可以使用高性能的硬件来承载模型，提升计算速度。

[0136] 在示出的一种实施方式中，服务端可以在其硬件架构中设置GPU(Graphics Processing Unit，图形处理器)，将GPU作为承载上述LSTM模型的处理硬件(即使用图形处理器来处理数据)，从而可以利用GPU的高性能的处理能力来完成记忆层的计算，提升整体的计算速度。

[0137] 3)输出层

[0138] 上述输出层，用于基于记忆层针对用户行为序列中各数据节点的计算结果，做出综合的风险评估，并在指定的数据节点或者检测到指定的关键行为时对风险评估结果进行输出。

[0139] 例如，在如图3所示出的基于预设时间周期来组织时序的LSTM模型架构中，可以在用户行为序列中指定一个模型的输出节点，比如将用户行为序列中最新的数据节点(即当天的数据节点)设定为模型的输出节点，从而模型可以在接收到当天的数据节点时进行响应，触发对目标账户进行风险评估，并将风险评估结果输出。

[0140] 或者，也可以在用户行为序列中最新的数据节点中指定关键行为，当在最新的数据节点中的操作行为数据中检测到关键行为时进行响应，触发对目标账户进行风险评估，并将风险评估结果输出。

[0141] 例如，上述指定关键行为可以是支付行为，当在当天的数据节点中的操作行为数据中检测到了用户的支付行为时，LSTM模型可以实时的进行响应，输出风险评估结果。

[0142] 又如，在如图4所示出的基于关键行为组织时序的模型架构中，由于不同的数据节点包含的关键行为特征均不相同，因此在这种情况下，可以所有数据节点对应的关键行为中指定一个关键行为，并将与该指定的关键行为对应的数据节点作为模型输出的节点。当检测到了该指定的关键行为时，LSTM模型可以实时的进行响应，输出风险评估结果；比如，上述指定关键行为可以是支付行为，上述LSRM模型输出计算结果的节点可以是与支付这一关键行为对应的数据节点，当在用户的操作行为数据中检测到了用户的支付行为时，LSTM模型可以实时的进行响应，向用户输出风险评估结果。

[0143] 以下结合图2示出的模型架构对LSTM模型的训练以及应用过程分别进行描述。

[0144] 一、模型训练

[0145] 在本例中，在基于图2示出的模型架构来训练LSTM模型时，可以预先准备大量已被标定出的风险账户，并针对这些风险账户在预设时长内的用户操作行为数据生成用户行为序列。

[0146] 例如，当上述LSTM模型采用设定的时间周期来组织序列，则可以采集各风险账户在预设时长内的所有操作行为数据，并基于设定的时间周期将采集到的操作行为数据划分为若干个数据集合，然后将划分出的数据集合分别作为数据节点按照时间发生顺序生成用户行为数列；比如，假设设定的时间周期为按天组织序列，设定的预设时长为90天，则可以针对各风险账户在90天内所有用户操作行为按天进行数据划分，划分为90个数据集合，此时每一天的操作行为数据都将作为模型输入层的一个输入源。

[0147] 又如，当上述LSTM模型采用设定的关键行为来组织序列，则可以为各风险账户设定若干关键行为，并在这些关键行为中指定一个关键行为作为模型的响应节点，然后可以采集各风险账户的所有操作行为数据，并确定采集到的操作行为数据中是否包含指定的关键行为；如果包含指定的关键行为，则可以采集在该指定的关键行为发生的时间之前预设时长内各风险账户产生的所有关键行为数据，并将采集到的所有关键行为数据分别作为数据节点按照发生时间排序生成用户行为序列。比如，假设设定的预设时长为90天，设定的关键行为包括登录、修改密码、创建交易以及支付等操作行为，指定的关键行为为“支付”，当确定各风险账户的操作行为数据中包含“支付”行为时，则可以采集该“支付”行为的发生时刻之前90天内各风险账户产生的所有关键行为数据作为数据节点按照发生时刻进行排序生成用户行为序列。

[0148] 当针对这些风险账户在预设时长内的用户操作行为数据生成了用户行为序列后，可以从生成的这些用户行为序列中提取风险识别特征，以作为训练样本进行训练来构建LSTM模型。

[0149] 其中，如果上述LSTM模型将与各数据节点中的操作行为数据关联的风险评估信息作为时点特征，则可以提取与已经生成的用户行为序列中各数据节点中的操作行为数据关联的风险评估信息，作为数据节点的风险识别特征。

[0150] 如果上述模型将通过判定各数据节点中的操作行为数据是否具有设定的风险特征的判定结果的编码结果作为时点特征，则可以针对已经生成的用户行为序列中各数据节点中的操作行为数据进行是否具有设定的风险特征的判定，然后对判定结果进行编码(比如可以进行0、1编码)，并将编码得到的字符串作为数据节点的风险识别特征。

[0151] 在本例中，当从为各风险账户生成的这些用户行为序列中提取出风险识别特征后，可以将提取出的风险识别特征作为训练样本基于LSTM算法进行深度学习训练，来构建上述LSTM模型。

[0152] 其中，针对上述训练样本进行训练来构建图2所示出的LSTM模型的过程，以及对训练完成的LSTM模型的预测性能进行评估(比如可以通过AUC、PR曲线来评估模型的性能)的过程，在本例中不再进行详述，本领域技术人员在将本申请的技术方案付诸实施时，可以参考相关技术中的记载。

[0153] 另外，需要说明的是，在构建上述LSTM模型时所使用的风险账户的类型，取决于在构建上述模型时的深度学习目标；例如，当需要基于上述LSTM模型来针对交易过程中的囤号风险进行风险评估，此时在构建上述模型时的深度学习目标则为囤号风险交易的概率，在这种情况下，在构建上述LSTM模型时则可以使用大量已被标定为存在囤号风险的风险账户作为训练样本进行深度学习；相似的，当需要基于上述风险评估模型来针对整个交易的风险进行评估，那么在构建上述LSTM模型时则可以使用大量已被标定为存在交易风险的风险账户(不限于存在囤号风险的账户)作为训练样本进行深度学习。

[0154] 二、模型使用

[0155] 当上述LSTM模型构建完成，服务端可以基于构建完成的该LSTM模型对目标账户进行风险识别。

[0156] 在本例中，服务端首先可以采集目标账户在预设时长内的操作行为数据来生成用户行为序列。

[0157] 一方面，当上述模型采用设定的时间周期来组织序列，服务端可以采集目标账户在预设时长内的所有操作行为数据，然后基于设定的时间周期将采集到的操作行为数据划分为若干个数据集合，然后将划分出的数据集合分别作为数据节点按照时间发生顺序生成用户行为数列。

[0158] 另一方面，当上述模型采用设定的关键行为来组织序列，则可以为目标账户设定若干关键行为，并在这些关键行为中指定一个关键行为作为模型的响应节点，然后可以采集目标账户的所有操作行为数据，并确定采集到的操作行为数据中是否包含指定的关键行为；如果包含指定的关键行为，则可以采集该指定的关键行为的发生时间之前预设时长内该目标账户产生的所有关键行为数据，并将采集到的所有关键行为数据分别作为数据节点按照发生时间排序生成用户行为序列。

[0159] 其中，生成的用户行为序列可以包括若干按照发生时间排序的数据节点；在数据节点中可以包括若干按照发生时间排序的操作行为数据。

[0160] 在本例中，当服务端为目标账户生成用户行为序列后，可以提取该用户行为序列中各数据节点的风险识别特征。

[0161] 一方面，当上述LSTM模型将与各数据节点中的操作行为数据关联的风险评估信息作为时点特征时，服务端可以提取与已经生成的用户行为序列中各数据节点中的操作行为数据关联的风险评估信息，作为数据节点的风险识别特征。

[0162] 另一方面，当上述模型将通过判定各数据节点中的操作行为数据是否具有设定的风险特征的判定结果的编码结果作为时点特征时，则可以对判定结果进行编码，然后将编码得到的字符串作为各数据节点的风险识别特征。

[0163] 在本例中，当服务端提取出目标账户的用户行为序列中各数据节点的风险识别特征后，可以将提取出的各数据节点的风险识别特征作为输入数据，按照发生时间的顺序依次输入至上述LSTM模型的输入层，然后由上述LSTM模型的记忆层进行计算。

[0164] 其中，记忆层在针对各数据节点的风险识别特征进行计算时，可以按照发生时间顺序，对输入层上各数据节点的风险识别特征依次进行计算，并采用递归计算的方式，将前一数据节点的计算结果与下一数据节点输入的风险识别特征进行加权求和后继续进行计算，直到各数据节点的风险识别特征在所述LSTM模型中均计算完成。

[0165] 同时，记忆层还可以采用离线计算和实时计算相结合的方式，对于用户行为序列中已经发生的数据节点的风险识别特征，可以进行离线预计算，当LSTM模型接收到了用户行为序列中最新的数据节点，需要进行风险评估时，再将离线计算结果实时导入线上生产系统，将上述离线计算结果与该最新的数据节点的风险识别特征一起进行实时计算。

[0166] 当计算完成后，LSTM模型可以在指定的数据节点或者检测到指定的关键行为时，通过输出层将计算结果输出，后续系统可以通过解析该计算结果，针对目标账户进行风险识别，然后根据风险识别结果来针对目标账户执行相应的安全防护策略。

[0167] 例如，假设指定的关键行为为支付行为时，当使用目标账户的用户进行支付操作时，上述LSTM模型可以做出响应，对目标账户进行风险评估计算并输出计算结果，此时支付系统可以基于输出的计算结果来判定该笔交易是否为风险交易，比如输出的计算结果具体为该笔交易为风险交易的概率值，支付系统可以将该概率值是否大于预设阈值，来确定该笔交易是否为风险交易。如果支付系统基于计算结果判定该笔交易为风险交易，则可以针

对该目标账户进行支付限制操作,阻断该笔支付以防止对用户资金造成损失。

[0168] 通过以上实施例可知,本申请通过基于目标账户在预设时长内的操作行为数据生成用户行为序列,并提取该行为序列中各数据节点的风险识别特征,将提取出的各数据节点的风险识别特征作为输入数据输入至预设的基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到的LSTM模型中进行计算,然后基于该LSTM模型输出的计算结果对所述目标账户进行风险识别,实现了可以基于用于在预设时长内的行为序列来构建用于风险账户识别的LSTM模型,并通过构建的LSTM模型对从用户的行为序列中提取出的风险识别特征进行计算,来对目标账户进行风险评估。

[0169] 另外,由于在构建LSTM模型以及使用LSTM模型时充分考虑了风险识别特征间的时序关系,因此可以对用户在一定时长内的历史操作行为信息在模型中进行记忆,将用户的历史操作行为信息与最新发生的操作行为信息进行融合,共同对目标账户进行风险评估,因此对于诸如囤号风险交易盗号初期那些小金额的试探性交易也能够及时识别,从而可以解决相关技术中,由于模型使用到的特征变量为零散的特征变量,并未反映特征变量的时序关系,而导致的诸如囤号风险交易盗号初期那些小金额的试探性交易无法进行及时识别的问题,可以从整体上提升对目标账户进行风险评估的灵敏度和准确度。

[0170] 与上述方法实施例相对应,本申请还提供了装置的实施例。

[0171] 请参见图7,本申请提出一种账户风险识别装置70,应用于服务端;其中,请参见图8,作为承载所述账户风险识别装置70的服务端所涉及的硬件架构中,通常包括CPU、内存、非易失性存储器、网络接口以及内部总线等;以软件实现为例,所述账户风险识别装置70通常可以理解为加载在内存中的计算机程序,通过CPU运行之后形成的软硬件相结合的逻辑装置,所述装置70包括:

[0172] 生成模块701,用于基于目标账户在预设时长内的操作行为数据生成用户行为序列;所述用户行为序列包括若干按照发生时间排序的数据节点;

[0173] 提取模块702,用于提取所述行为序列中各数据节点的风险识别特征;

[0174] 计算模块703,用于将提取出的各数据节点的风险识别特征作为输入数据输入至预设的LSTM模型中进行计算;其中,所述预设的LSTM模型基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到;

[0175] 识别模块704,用于基于所述LSTM模型输出的计算结果对所述目标账户进行风险识别。

[0176] 在本例中,所述生成模块701具体用于:

[0177] 采集目标账户在预设时长内的操作行为数据;

[0178] 基于预设时间周期将采集到的所述操作行为数据划分为若干数据集合;

[0179] 将划分出的所述若干数据集合分别作为数据节点按照发生时间进行排序以生成所述行为序列。

[0180] 在本例中,所述生成模块701具体用于:

[0181] 采集目标账户的操作行为数据;

[0182] 确定所述操作行为数据是否包含指定的关键行为;

[0183] 当所述操作行为数据中包含指定的关键行为时,采集该目标账户在所述指定的关键行为的发生时间以前预设时长内产生的所有关键行为数据;

[0184] 将采集到的所有关键行为数据分别作为数据节点按照发生时间进行排序以生成所述行为序列。

[0185] 在本例中,所述数据节点包括若干按照发生时间排序的操作行为数据;

[0186] 所述提取模块702具体用于:

[0187] 提取与所述行为序列中各数据节点中的操作行为数据关联的风险评估信息,作为所述风险识别特征;其中,所述风险评估信息包括与所述目标账户相关的风险评估信息,以及与所述目标账户对应的业务对端账户相关的风险评估信息;或者

[0188] 判定所述行为序列中各数据节点中的操作行为数据是否具有设定的风险特征,并对判定结果进行编码,将编码得到的字符串作为所述风险识别特征。

[0189] 在本例中,所述计算模块703具体用于

[0190] 将所述各数据节点的风险识别特征作为输入数据,按照发生时间顺序依次输入至所述LSTM模型中进行计算,并将前一数据节点的计算结果与下一数据节点的风险识别特征进行加权求和后继续进行计算,直到所述各数据节点的风险识别特征在所述LSTM模型中均计算完成;

[0191] 其中,所述用户行为序列中已发生的数据节点的风险识别特征在所述风险识别模型中进行离线计算,所述离线计算的结果与所述用户行为序列中最新的数据节点的风险识别特征在所述风险识别模型中进行实时计算。

[0192] 在本例中,所述装置70还包括:

[0193] 输出模块705,用于在指定的数据节点或者在检测到指定的关键行为时,输出所述LSTM模型的计算结果。

[0194] 在本例中,搭载所述LSTM模型的硬件处理器为GPU。

[0195] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的,本申请的真正范围和精神由下面的权利要求指出。

[0196] 应当理解的是,本申请并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

[0197] 以上所述仅为本申请的较佳实施例而已,并不用以限制本申请,凡在本申请的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本申请保护的范围之内。

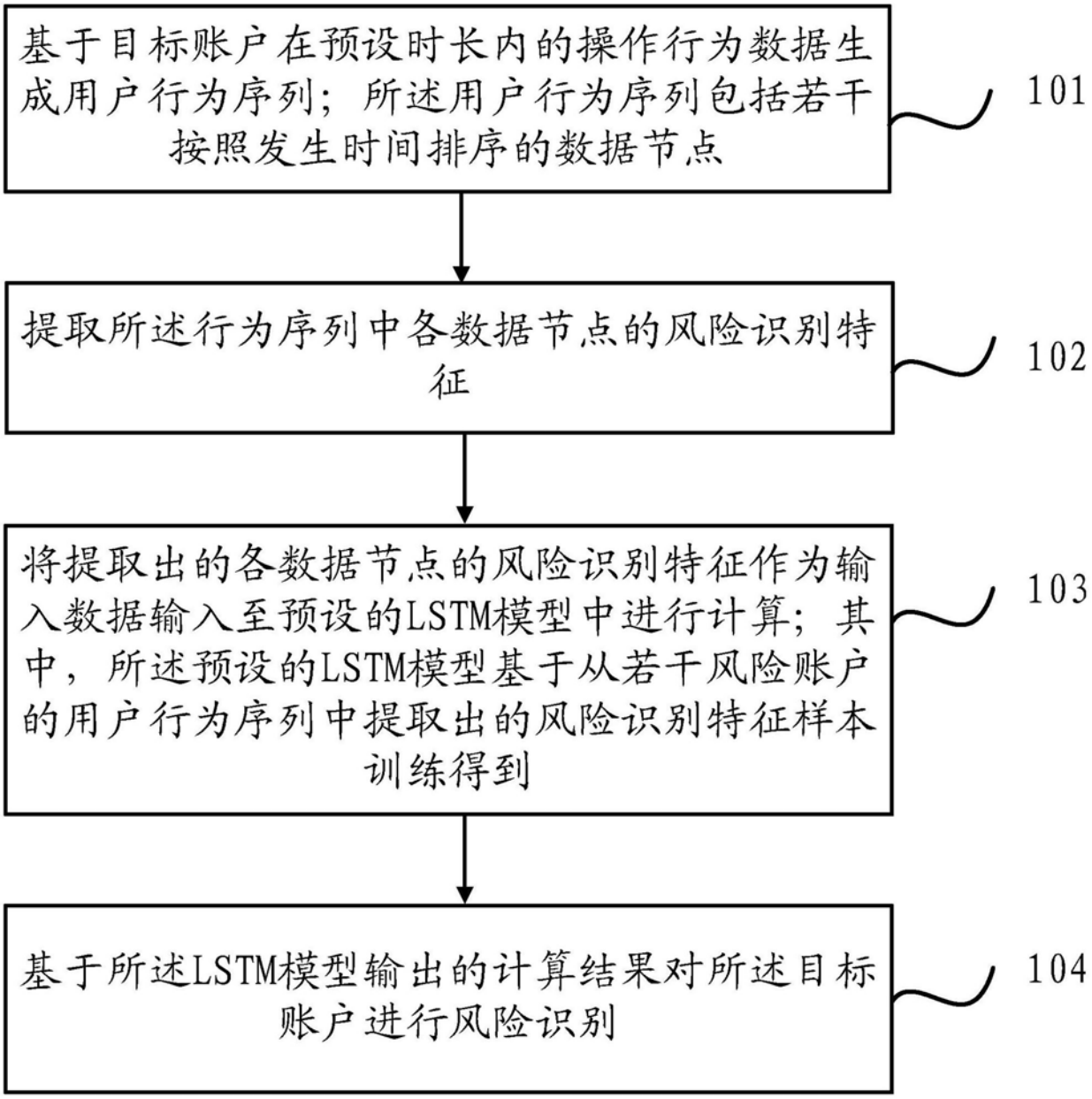

基于目标账户在预设时长内的操作行为数据生成用户行为序列；所述用户行为序列包括若干按照发生时间排序的数据节点
101
提取所述行为序列中各数据节点的风险识别特征
102
将提取出的各数据节点的风险识别特征作为输入数据输入至预设的LSTM模型中进行计算；其中，所述预设的LSTM模型基于从若干风险账户的用户行为序列中提取出的风险识别特征样本训练得到
103
基于所述LSTM模型输出的计算结果对所述目标账户进行风险识别
104

图1

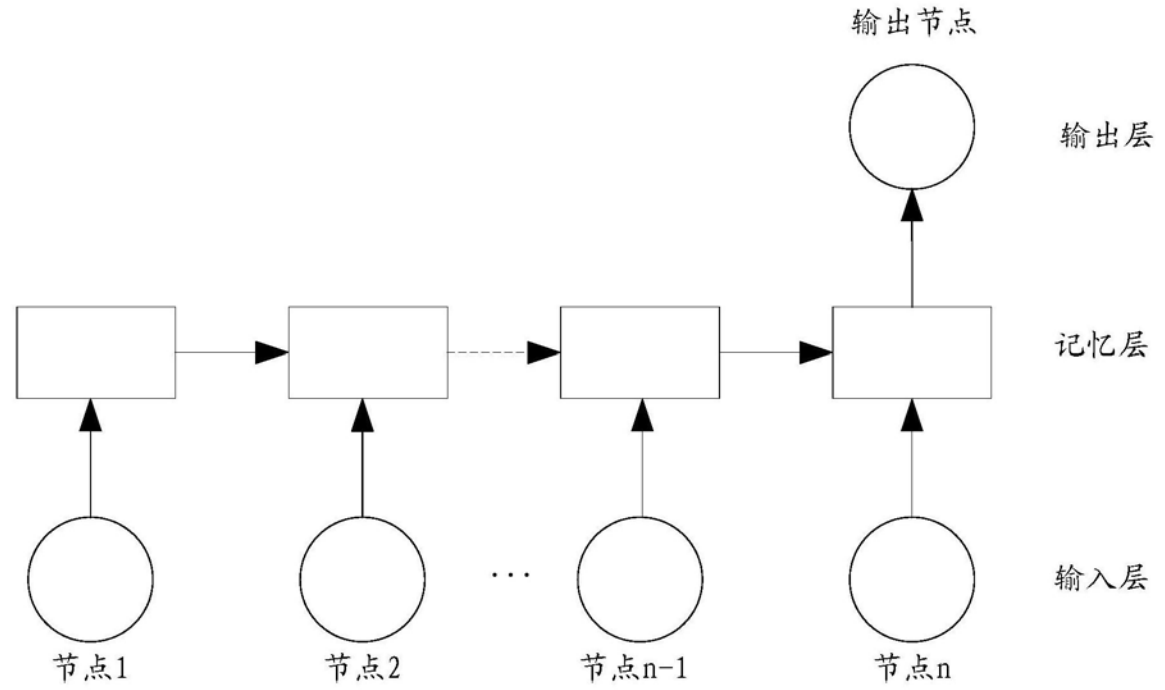

输出节点
输出层
记忆层
输入层
节点1
节点2
节点n-1
节点n

图2

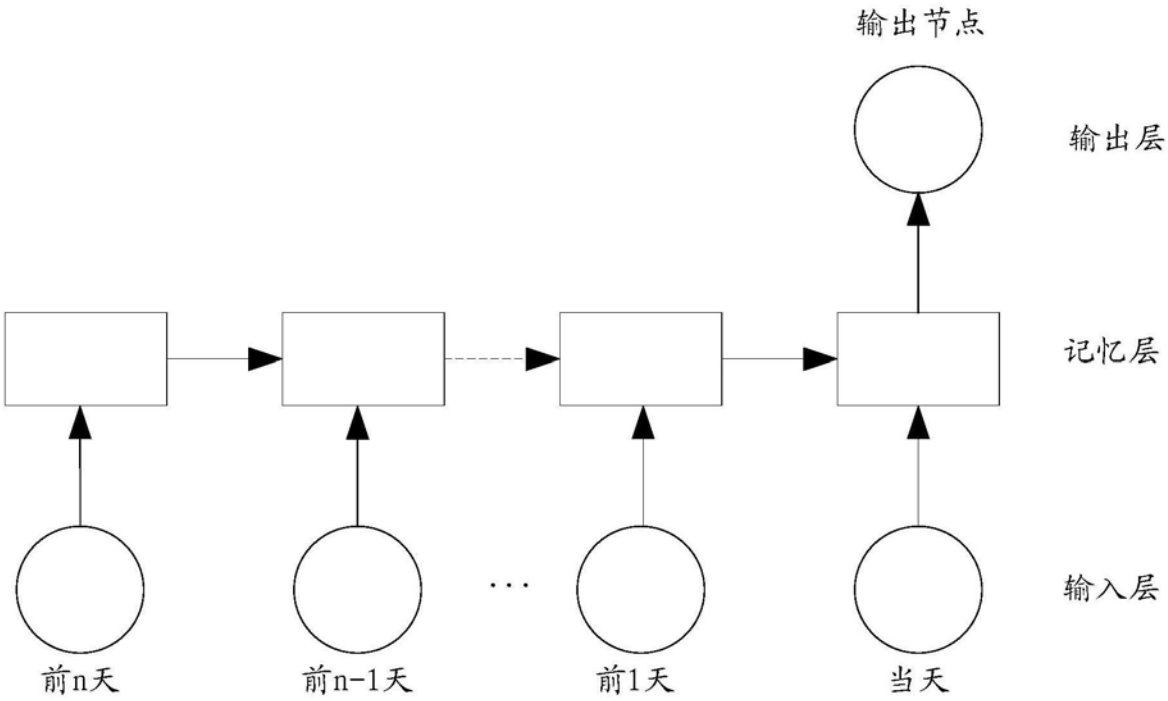

输出节点
输出层
记忆层
输入层
前n天
前n-1天
前1天
当天

图3

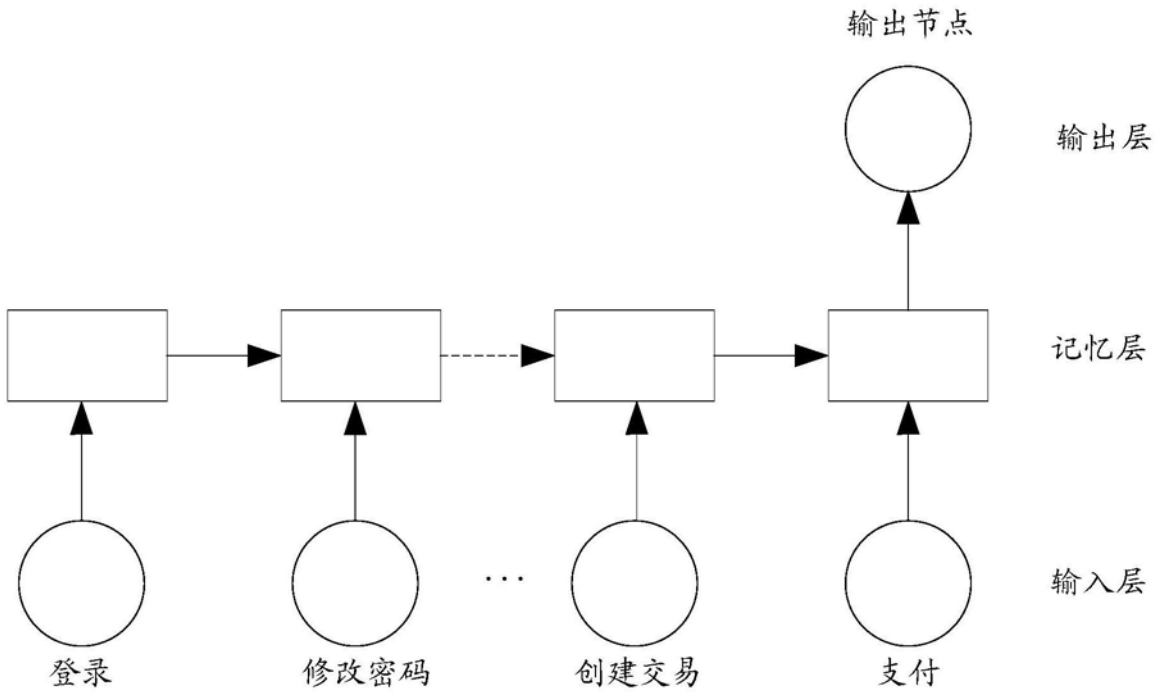

输出节点
输出层
记忆层
输入层
登录
修改密码
创建交易
支付

图4

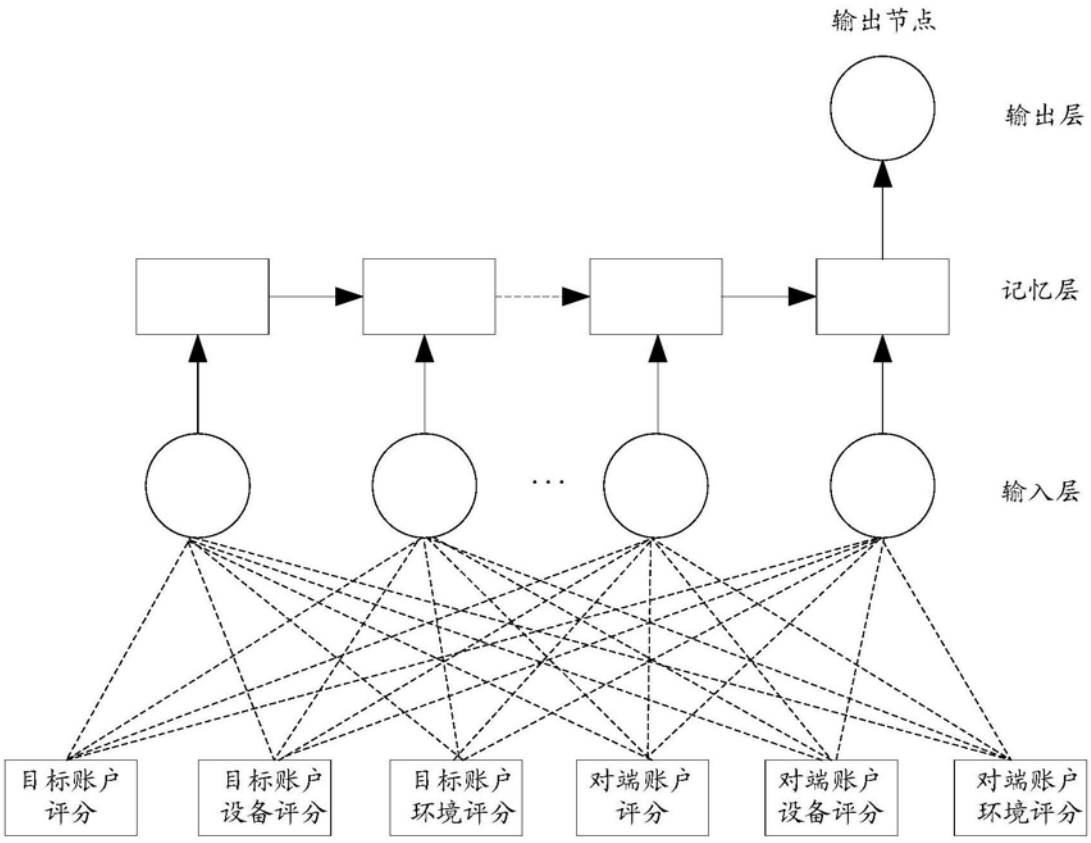

输出节点
输出层
记忆层
输入层
目标账户评分
目标账户设备评分
目标账户环境评分
对端账户评分
对端账户设备评分
对端账户环境评分

图5

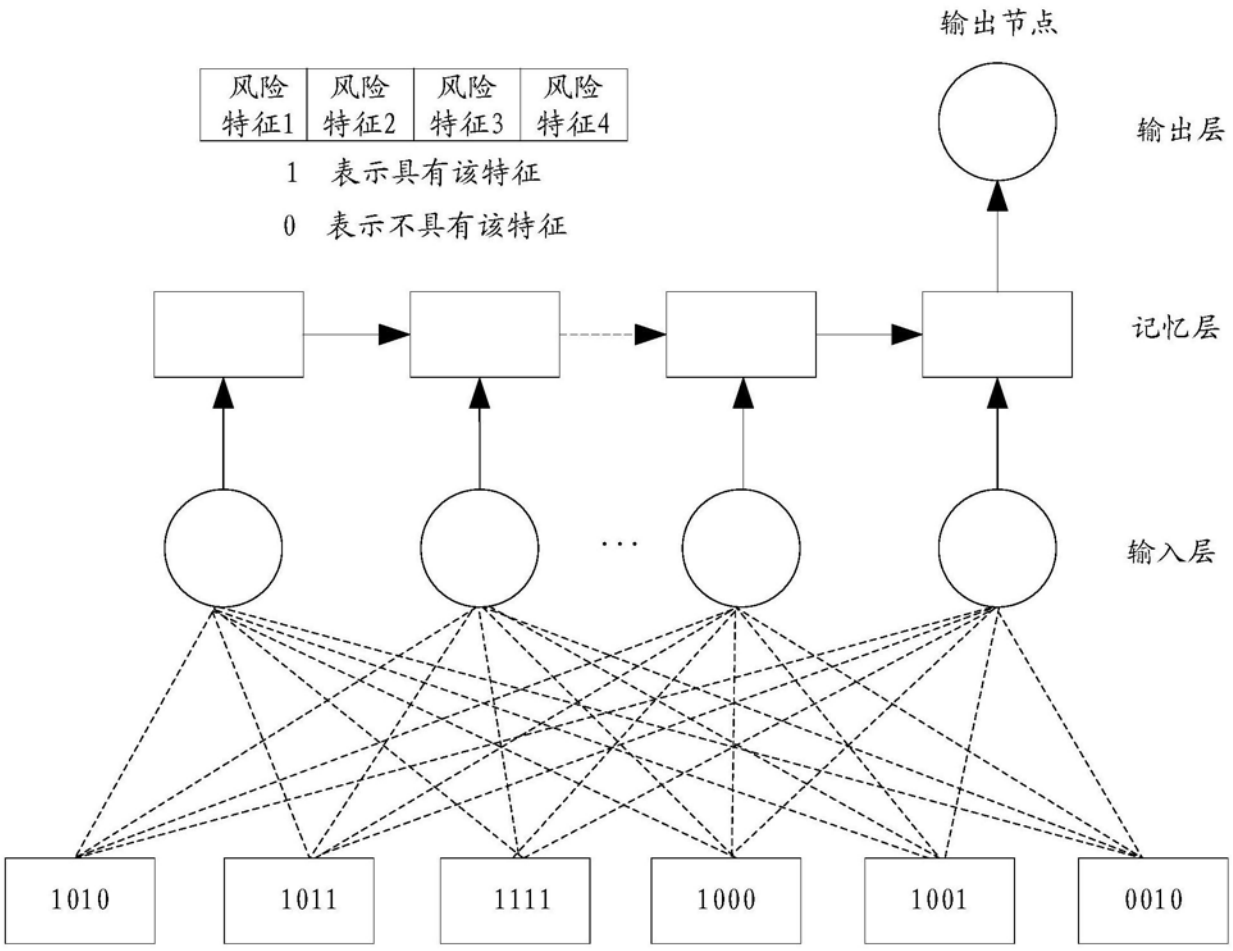

输出节点
风险特征1
风险特征2
风险特征3
风险特征4
1 表示具有该特征
0 表示不具有该特征
输出层
记忆层
输入层
1010
1011
1111
1000
1001
0010

图6

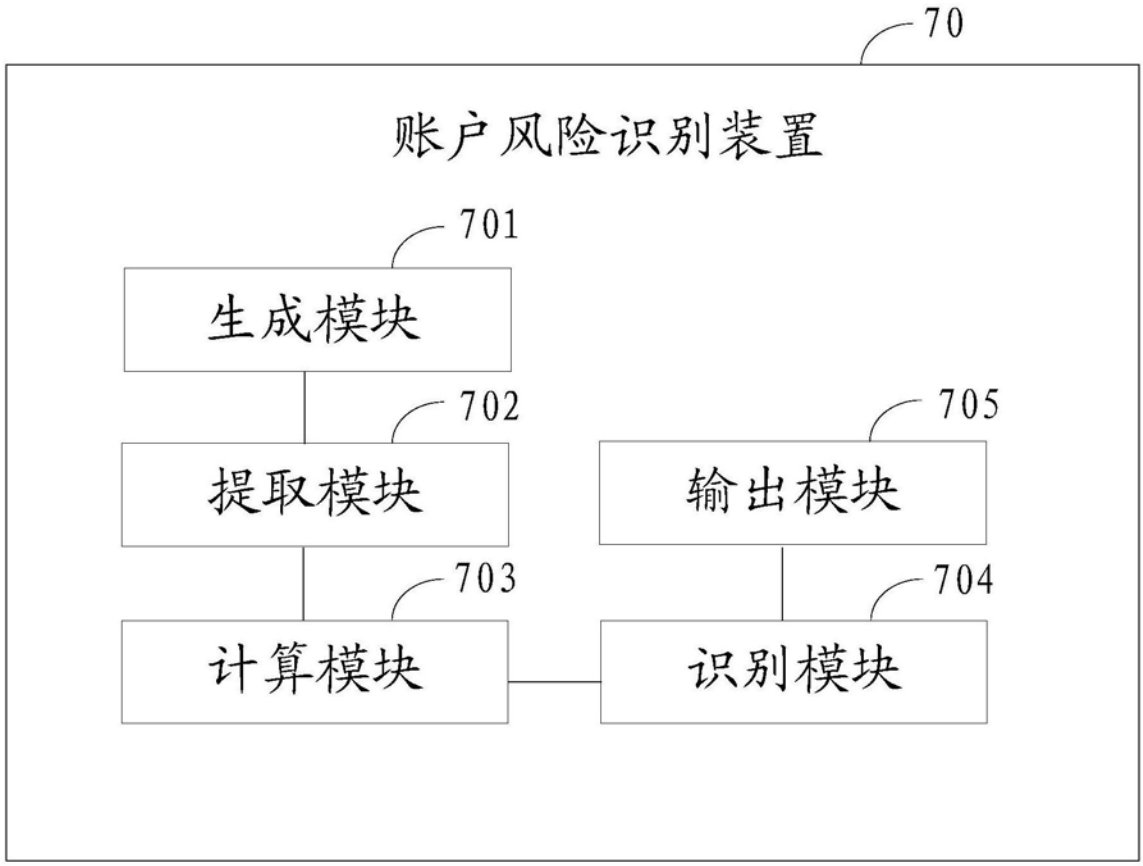

70
账户风险识别装置
701
生成模块
702
提取模块
703
计算模块
705
输出模块
704
识别模块

图7

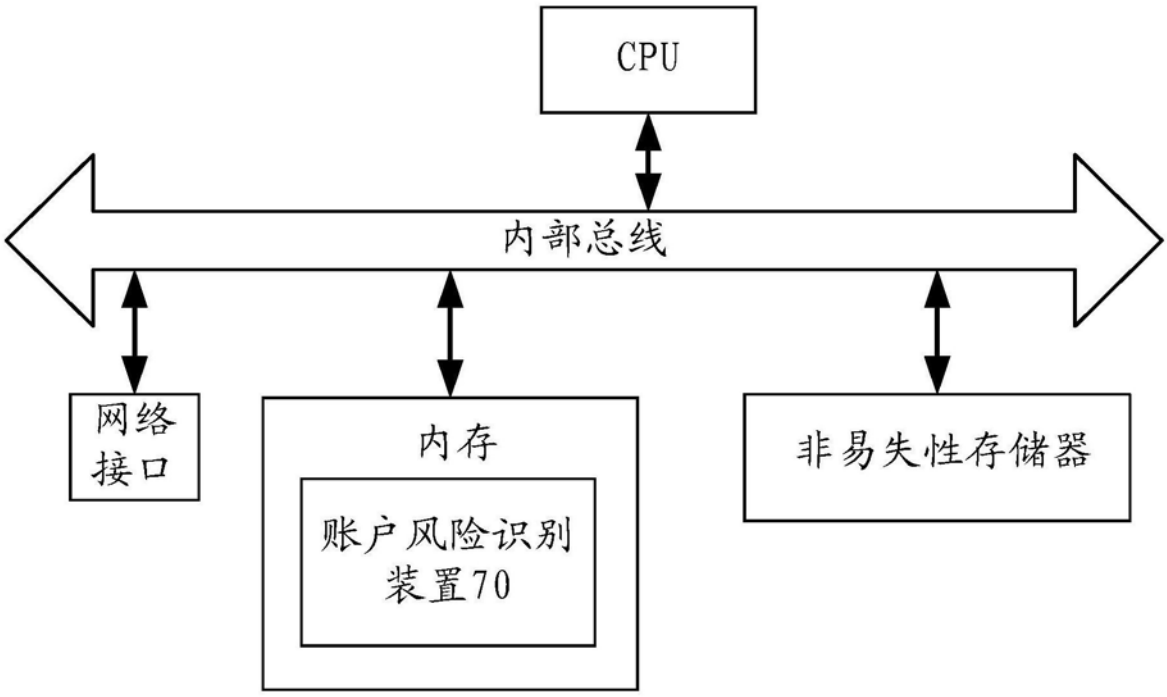

CPU
内部总线
网络接口
内存
账户风险识别装置70
非易失性存储器

图8