

一种支付风控方法及系统

技术领域

[01] 本说明书实施例涉及互联网应用技术领域，尤其涉及一种支付风控方法及系统。

背景技术

- 5 [02] 随着智能终端的发展和网络应用的普及，用户可以通过终端上安装的具有支付功能的应用客户端实现各种支付操作，例如，在乘坐巴士、地铁等公共交通工具时，可以使用电子钱包的客户端支付交通费用。但是，对于用户及支付机构，可能存在盗用账号、扣不到款等风险。

[03] 基于现有技术，需要一种针对电子支付公共交通费用场景的支付风控方案。

10 发明内容

[04] 针对上述技术问题，本说明书实施例提供一种支付风控方法及系统，技术方案如下：

[05] 根据本说明书实施例的第一方面，提供一种支付风控方法，该方法包括：

- 15 [06] 应用侧接收到进出站付款操作触发后，生成携带预设风控特征的付款图形码生成请求，并将该请求发送至风控侧；所述风控特征至少包括：付款账号特征、当前位置特征及进出站特征；

[07] 风控侧接收到应用侧发送的付款图形码生成请求后，根据该请求中的付款账号特征，获取预先存储的该账号的历史风控特征；

- 20 [08] 风控侧通过比较读取的历史风控特征与该请求中携带的风控特征，检测应用侧是否存在交易风险，并向应用侧返回风控检测结果；其中，检测交易风险的方法包括：根据进出站特征判断本次生成的付款图形码用于进站或出站；若为进站，则判断付款图形码生成请求的频率是否高于预设阈值，若是则确定存在交易风险；若为出站，则判断当前位置特征与历史风控特征中对应的进站位置特征是否符合预设位置关系条件，若否则确定存在交易风险；

[09] 应用侧接收到风控侧返回的不存在交易风险的结果后，生成并展示付款图形码。

- 25 [10] 根据本说明书实施例的第二方面，提供一种支付风控方法，应用于应用侧，该方法

包括:

[11]接收到进出站付款操作触发后,生成携带预设风控特征的付款图形码生成请求;

[12]将所述付款图形码生成请求发送至风控侧,以使风控侧根据该请求中携带的风控特征,检测应用侧是否存在交易风险并返回检测结果;

5 [13]其中,所述风控特征至少包括:付款账号特征、当前位置特征及进出站特征;

[14]接收到风控侧返回的不存在交易风险的结果后,生成并展示付款图形码。

[15]根据本说明书实施例的第三方面,提供一种支付风控方法,应用于风控侧,该方法包括:

10 [16]接收到应用侧发送的付款图形码生成请求后,根据该请求中的付款账号特征,获取预先存储的该账号的历史风控特征;

[17]通过比较读取的历史风控特征与该请求中携带的风控特征,检测应用侧是否存在交易风险,并向应用侧返回风控检测结果;

15 [18]其中,检测交易风险的方法包括:根据进出站特征判断本次生成的付款图形码用于进站或出站;若为进站,则判断付款图形码生成请求的频率是否高于预设阈值,若是则确定存在交易风险;若为出站,则判断当前位置特征与历史风控特征中对应的进站位置特征是否符合预设位置关系条件,若否则确定存在交易风险。

[19]根据本说明书实施例的第四方面,提供一种支付风控系统,该系统包括:应用侧及风控侧;

20 [20]应用侧接收到进出站付款操作触发后,生成携带预设风控特征的付款图形码生成请求,并将该请求发送至风控侧;所述风控特征至少包括:付款账号特征、当前位置特征及进出站特征;

[21]风控侧接收到应用侧发送的付款图形码生成请求后,根据该请求中的付款账号特征,获取预先存储的该账号的历史风控特征;

25 [22]风控侧通过比较读取的历史风控特征与该请求中携带的风控特征,检测应用侧是否存在交易风险,并向应用侧返回风控检测结果;其中,风控侧具体通过以下方式检测交易风险:根据进出站特征判断本次生成的付款图形码用于进站或出站;若为进站,则判断付款图形码生成请求的频率是否高于预设阈值,若是则确定存在交易风险;若为出站,则判断当前位置特征与历史风控特征中对应的进站位置特征是否符合预设位置关系条

件，若否则确定存在交易风险；

[23]应用侧接收到风控侧返回的不存在交易风险的结果后，生成并展示付款图形码。

[24]根据本说明书实施例的第五方面，提供一种支付风控装置，应用于应用侧设备，该装置包括：

5 [25]请求生成模块，用于接收到进出站付款操作触发后，生成携带预设风控特征的付款图形码生成请求；

[26]请求发送模块，用于将所述付款图形码生成请求发送至风控侧，以使风控侧根据该请求中携带的风控特征，检测应用侧是否存在交易风险并返回检测结果；

[27]其中，所述风控特征至少包括：付款账号特征、当前位置特征及进出站特征；

10 [28]图形码生成模块，用于接收到风控侧返回的不存在交易风险的结果后，生成并展示付款图形码。

[29]根据本说明书实施例的第六方面，提供一种支付风控装置，应用于风控侧设备，该装置包括：

15 [30]特征获取模块，用于接收到应用侧发送的付款图形码生成请求后，根据该请求中的付款账号特征，获取预先存储的该账号的历史风控特征；

[31]风险检测模块，用于通过比较读取的历史风控特征与该请求中携带的风控特征，检测应用侧是否存在交易风险，并向应用侧返回风控检测结果；

20 [32]其中，风险检测模块具体通过以下方式检测交易风险：根据进出站特征判断本次生成的付款图形码用于进站或出站；若为进站，则判断付款图形码生成请求的频率是否高于预设阈值，若是则确定存在交易风险；若为出站，则判断当前位置特征与历史风控特征中对应的进站位置特征是否符合预设位置关系条件，若否则确定存在交易风险。

[33]本说明书实施例所提供的技术方案，针对电子支付公共交通费用的场景，通过应用侧生成付款图形码之前，对应用侧进行交易风险检测，避免应用侧在存在交易风险的情况下，生成图形码进行公交费用的支付，提高了该场景中用户与支付机构的安全性。

25 [34]应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书实施例。

[35]此外，本说明书实施例中的任一实施例并不需要达到上述的全部效果。

附图说明

[36]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述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说明书实施例中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

- [37]图 1 是本说明书实施例的支付风控系统的结构示意图；
- [38]图 2 是本说明书实施例的支付风控方法的一种流程示意图；
- [39]图 3 是本说明书实施例的支付风控方法的另一种流程示意图；
- [40]图 4 是本说明书实施例的支付风控方法的又一种流程示意图；
- 10 [41]图 5 是本说明书实施例的业务开通阶段的流程示意图；
- [42]图 6 是本说明书实施例的付款图形码生成阶段的流程示意图；
- [43]图 7 是本说明书实施例的交易清算阶段的流程示意图；
- [44]图 8 是本说明书实施例的支付风控装置的一种结构示意图；
- [45]图 9 是本说明书实施例的支付风控装置的另一种结构示意图；
- 15 [46]图 10 是用于配置本说明书实施例装置的一种设备的结构示意图。

具体实施方式

[47]为了使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述，显然，所描述的实施例仅仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于保护的范围。

[48]在本说明书的实施例中，针对电子支付公共交通费用场景的支付风控流程，涉及应用侧与风控侧。

[49]应用侧部署于移动终端设备，如用户的智能手机、平板电脑等可以安装应用程序的移动终端设备，而应用侧则可以是安装于该设备的电子钱包客户端等应用程序，以使用户可以通过所携带的移动终端中的客户端，在外出时方便地支付公共交通费用。

[50]风控侧可以以云端风控侧的形式，部署于云端服务器、且与应用侧通过各种形式的

无线网络实现通信连接，云端服务器的具体形式，可以是特定的一台服务器或服务器集群等形式。

5 [51]此外，用户乘坐巴士、地铁、渡轮等公共交通工具时，交通工具的移动、或者处于封闭的车厢、地下等因素，可能会使得移动终端设备与云端服务器之间的网络连接质量较差，从而影响对支付过程的实时风险控制。

[52]因此，风控侧还可以以本机风控侧的形式，部署于应用侧所在的移动终端设备本地，且与应用侧通过终端内部的有限链路连接。如可以在电子钱包客户端内植入风控 SDK（Software Development Kit，软件开发工具包）。

10 [53]本说明书的方案，可以通过应用侧与云端风控侧实现，也可以通过应用侧与本机风控侧实现，当然还可以通过应用侧与本机风控侧及云端风控侧的结合实现，本说明书对此不做限定。

[54]本说明书实施例对应的系统架构示意图，如图 1 所示，包括应用侧设备 10 和风控侧设备 20。其中，如上面所述，应用侧设备可以是用户所携带的智能手机、平板电脑等移动终端设备，风控侧设备可以是上述的云端服务器、或应用侧所在的移动终端设备。

15 [55]图 2 为本说明书实施例提供的支付风控方法的交互流程图，具体可以包括以下步骤：

[56]S201，应用侧接收到进出站付款操作触发后，生成携带预设风控特征的付款图形码生成请求，并将该请求发送至风控侧；所述风控特征至少包括：付款账号特征、当前位置特征及进出站特征；

20 [57]应用本支付风控方案的公共交通费用支付场景中，用户进出站时均需要在应用侧进行进出站付款操作。例如，用户通过地铁的进站、出站闸机时，或用户上、下公交车或渡轮时，可以打开手机（应用侧设备）中安装的电子钱包客户端（应用侧），通过点击客户端提供的按钮等操作，进行进出站付款操作。

25 [58]应用侧接收到进出站付款操作触发后，可以展示付款图形码进行费用支付，一般付款图形码可以由应用侧或风控侧生成，由于本说明书的方案应用的场景中，可能存在应用侧设备网络信号较差，无法通过无线网络与云端风控侧进行数据传输的情况，因此本说明书的方案中，由应用侧生成并展示付款图形码，并在生成图形码之前对应用侧是否存在交易风险进行风险检测，从而确保支付过程的安全性。

[59]当然，也可以通过读码设备，对读取到的付款图形码是否正确、是否已重复使用、是否过期等做进一步的检测，这里不做详细描述。

[60]因此，应用侧接收到进出站付款操作触发后，生成携带预设风控特征的付款图形码生成请求，并进一步地将该请求发送至风控侧。

[61]本说明书实施例中，在风控侧包括云端风控侧和本机风控侧的情况下，优先使用性能更优的云端风控侧进行本次支付风控，但在应用侧与云端风控侧无线网络连接质量较差，因而不适合使用云端风控侧时，优先使用通过有线链路进行通讯，因而数据传输更稳定的本机风控侧进行本次支付风控。

[62]具体地，在应用侧进行发送之前，首先判断所在的移动终端当前的网络信号是否达到预设强度，若是则表明当前网络信号较好，可以将付款图形码生成请求通过无线网络发送至云端风控侧；若否则表明当前网络信号不好，不适宜向云端风控侧发送数据，可以将付款图形码生成请求通过有线链路发送至本机风控侧。

[63]S202，风控侧接收到应用侧发送的付款图形码生成请求后，根据该请求中的付款账号特征，获取预先存储的该账号的历史风控特征；

[64]S203，风控侧通过比较读取的历史风控特征与该请求中携带的风控特征，检测应用侧是否存在交易风险，并向应用侧返回风控检测结果；

[65]为了便于描述，将 S202 与 S203 结合进行说明。

[66]根据应用侧发来的请求中携带的各项风控特征、与历史风控特征，具体可以通过多种方式检测应用侧是否存在交易风险。

[67]在本说明书实施例中，可以根据进出站特征判断本次生成的付款图形码用于进站或出站；若为进站，则判断付款图形码生成请求的频率是否高于预设阈值，若是，则表示通过该账号支付的进站频率过高，可能存在被盗账号、合谋共用账号等风险，因此可以确定存在交易风险。

[68]此外，还可以进一步确定本次请求的时间、及历史各次请求的时间，结合当前位置特征及历史各次请求的位置特征，判断各次进站的位置变动是否合理，例如是否频繁变动、或在较短的时间内变动距离较大、等，从而判断是否存在被盗账号、合谋共用账号等风险。

[69]若为出站，则判断当前位置特征与历史风控特征中对应的进站位置特征是否符合预设位置关系条件，若否则确定存在交易风险。例如，可以确定进站时间与位置、本次出站的时间与位置、以及所使用公共交通工具的行驶速度与路线等信息，判断出站的时间与位置是否合理，从而判断是否存在盗账号以及合谋等风险。

[70]在本说明书的另一实施例中，还可以获取预先存储的黑名单，黑名单记录了存在交易风险的对象，可以为付款账号、付款账号绑定的用户信息（如姓名、证件号码、手机号、银行卡号、等等）、和/或应用侧所在移动终端的设备信息（如手机识别码、当前使用的无线热点、等等），风控侧可以根据所述付款图形码生成请求中的风控特征，确定所述黑名单中记录的是否包括该请求对应的对象。

[71]在本说明书的又一实施例中，还可以获取该付款账号的历史支付记录，并根据历史支付记录判断该账号是否存在风险，从而确定应用侧当前是否存在交易风险。例如，是否存在为支付的款项、支付的金额是否正确、是否存在支付金额与余额变动不符的情况、等等。

10 [72]风控侧接收到应用侧发送的付款图形码生成请求后，还可以使用所述付款图形码生成请求中携带的风控特征，更新对应付款账号的历史风控特征，以便后续根据所更新的历史风控特征，进行交易风险检测。

[73]并且云端风控侧与本机风控侧可以互相进行数据同步，以及时更新本地存储的历史记录。

15 [74]S204，应用侧接收到风控侧返回的不存在交易风险的结果后，生成并展示付款图形码。

[75]应用侧在接收到风控侧返回的不存在交易风险的结果后，才可以生成付款图形码。本说明书实施例中，风控侧返回的结果中还可以包括特定的许可标识，应用侧生成的付款图形码中包括该标识，从而使后续读码设备进一步检测时，可以判断该图形码是否为风控侧确定不存在交易风险的情况下生成的。

20

[76]此外，除了应用侧生成与展示付款码的过程中，进行实时风险控制，本说明书实施例中，应用侧与风控侧之间，还可以进行异步数据积累，从而对用户开通进出站付款业务的数据、及交易清算的数据，进行非实时的风险控制，从而实现在整个支付过程对应用侧进行支付风控。

25 [77]为了更清楚地说明本说明书实施例的支付风控方案，下面分别再从单侧的角度，对应用侧与风控侧执行的支付风控方法进行说明：

[78]图3所示为应用侧所执行的支付风控方法流程图，具体可以包括以下步骤：

[79]S301，接收到进出站付款操作触发后，生成携带预设风控特征的付款图形码生成请求；

[80]S302, 将所述付款图形码生成请求发送至风控侧, 以使风控侧根据该请求中携带的风控特征, 检测应用侧是否存在交易风险并返回检测结果;

[81]其中, 所述风控特征至少包括: 付款账号特征、当前位置特征及进出站特征;

[82]S303, 接收到风控侧返回的不存在交易风险的结果后, 生成并展示付款图形码。

5 [83]图 4 所示为风控侧所执行的支付风控方法流程图, 具体可以包括以下步骤:

[84]S401, 接收到应用侧发送的付款图形码生成请求后, 根据该请求中的付款账号特征, 获取预先存储的该账号的历史风控特征;

[85]S402, 通过比较读取的历史风控特征与该请求中携带的风控特征, 检测应用侧是否存在交易风险, 并向应用侧返回风控检测结果;

10 [86]其中, 检测交易风险的方法包括: 根据进出站特征判断本次生成的付款图形码用于进站或出站; 若为进站, 则判断付款图形码生成请求的频率是否高于预设阈值, 若是则确定存在交易风险; 若为出站, 则判断当前位置特征与历史风控特征中对应的进站位置特征是否符合预设位置关系条件, 若否则确定存在交易风险。

[87]关于 与 的单侧执行方法细节, 可以参见前面实施例的描述, 这里不再赘述。

15 [88]下面结合一个更为具体的实例, 对本说明书提供的支付风控方法进行说明。

[89]针对电子支付公共交通费用场景的支付风控流程, 可以分为三个阶段: 业务开通阶段、付款图形码生成阶段、及交易清算阶段。

20 [90]以支付乘坐地铁费用为例, 风控侧进行风险控制时, 需要的输入数据可以包括: 应用侧设备信息, 当前位置信息, 交易账号, 该账号的余额变动情况、支付历史, 以及风控侧的黑名单, 等等。根据上述输入数据, 基于是否在黑名单中、地理位置变动情况、付款频率、余额变动情况、等等检测条件, 检测是否存在盗账户、扣不到款、合谋等风险。

[91]下面分别从这三个阶段, 描述具体实现过程。

[92]一、业务开通阶段

25 [93]如图 5 所示为业务开通阶段的流程示意图。

[94]用户在手机中安装电子钱包客户端后, 通过同意协议条款、输入密码验证身份后, 客户端(应用侧)即向风控侧发送开通进出站付款业务的请求, 风控侧可以包括电子钱

包的后台服务器与风控引擎，该请求首先发送至后台服务器。

- [95]后台服务器收到该请求后，可以基于预设的规则，对该请求进行较为简单的检测，从而确定是否允许本次的开通请求，并向客户端返回结果。所述预设的规则，可以包括风险检测规则，如该账户的信用值是否达标等，也可以包括其他商业规则，如该账户对应用户的个人信息是否符合条件等。

[96]后台服务器还需将业务开通请求及处理结果，发送至风控引擎，从而使风控引擎获取上述输入数据，并基于上述检测条件，检测是否存在盗账户、扣不到款、合谋等风险，这一过程可以是非实时进行的。

[97]二、付款图形码生成阶段

- 10 [98]如图 6 所示为付款图形码生成阶段的流程示意图。

[99]用户在电子钱包的客户端中点击相应按钮，从而使客户端接收到进出站付款操作触发，向后台服务器发送付款图形码生成请求，后台服务器将该请求转发至风控引擎，以使风控引擎获取上述输入数据，并基于上述检测条件，检测是否存在盗账户、扣不到款、合谋等风险。此外，后台服务器也可以基于预设规则进行较为简单的风险检测。

- 15 [100] 风控引擎将检测结果返回至后台服务器，后台服务器结合本端进行的风险检测，综合做出是否允许生成付款图形码的决定，发送至客户端，客户端接收到不存在交易风险、可以生成付款图形码的结果后，生成并展示用于进出地铁站闸机的付款图形码。后台服务器还需将综合处理结果发送至风控引擎，以用于更新所记录的相关数据，这一过程可以是非实时进行的。

- 20 [101] 三、交易清算阶段

[102] 如图 7 所示为交易清算阶段的流程示意图。

[103] 交易服务器可以以实时或非实时的形式，将交易数据发送至风控引擎，从而是风控引擎根据交易数据及预先异步积累的数据，基于上述检测条件，检测是否存在盗账户、扣不到款、合谋等风险。

- 25 [104] 可见，应用上述方案，针对电子支付公共交通费用的场景，通过应用侧生成付款图形码之前，对应用侧进行实时的交易风险检测，避免应用侧在存在交易风险的情况下，生成图形码进行公交费用的支付，提高了该场景中用户与支付机构的安全性。

[105] 此外，针对使用公共交通工具的场景中，网络连接质量不稳定的情况，风控侧

可以部署于应用侧所在的移动终端设备中，并与应用侧通过有线链路连接，并且在业务开通与交易清算阶段，通过异步数据积累进行风险控制，从而在不影响用户正常使用的前提下，更及时地进行交易风险检测，提供更优质的支付风控服务。

5 [106] 值得注意的是，本说明书提供的方案，还可以应用于风控赋能场景，即将已有的风控引擎或风控 SDK，直接与需要进行风控的电子钱包对接，在业务申请、生成付款图形码与交易清算三个节点，进行风险控制，在电子钱包自身的系统不需要做重大改造的前提下，使电子钱包获得风控能力，而不需要重新进行风控引擎的研发，从而提高了人力、物力等资源的利用效率。

10 [107] 相应于上述方法实施例，本说明书实施例还提供一种支付风控装置，应用于应用侧设备，参见图 8 所示，该装置可以包括：

[108] 请求生成模块 110，用于接收到进出站付款操作触发后，生成携带预设风控特征的付款图形码生成请求；

[109] 请求发送模块 120，用于将所述付款图形码生成请求发送至风控侧，以使风控侧根据该请求中携带的风控特征，检测应用侧是否存在交易风险并返回检测结果；

15 [110] 其中，所述风控特征至少包括：付款账号特征、当前位置特征及进出站特征；

[111] 图形码生成模块 130，用于接收到风控侧返回的不存在交易风险的结果后，生成并展示付款图形码。

[112] 本说明书实施例还提供一种支付风控装置，应用于风控侧设备，参见图 9 所示，该装置可以包括：

20 [113] 特征获取模块 210，用于接收到应用侧发送的付款图形码生成请求后，根据该请求中的付款账号特征，获取预先存储的该账号的历史风控特征；

[114] 风险检测模块 220，用于通过比较读取的历史风控特征与该请求中携带的风控特征，检测应用侧是否存在交易风险，并向应用侧返回风控检测结果；

25 [115] 其中，风险检测模块 220 具体通过以下方式检测交易风险：根据进出站特征判断本次生成的付款图形码用于进站或出站；若为进站，则判断付款图形码生成请求的频率是否高于预设阈值，若是则确定存在交易风险；若为出站，则判断当前位置特征与历史风控特征中对应的进站位置特征是否符合预设位置关系条件，若否则确定存在交易风险。

[116] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[117] 本说明书实施例还提供一种计算机设备，其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现前述的支付风控方法。该方法至少包括：

[118] 一种支付风控方法，该方法包括：

[119] 应用侧接收到进出站付款操作触发后，生成携带预设风控特征的付款图形码生成请求，并将该请求发送至风控侧；所述风控特征至少包括：付款账号特征、当前位置特征及进出站特征；

10 [120] 风控侧接收到应用侧发送的付款图形码生成请求后，根据该请求中的付款账号特征，获取预先存储的该账号的历史风控特征；

[121] 风控侧通过比较读取的历史风控特征与该请求中携带的风控特征，检测应用侧是否存在交易风险，并向应用侧返回风控检测结果；其中，检测交易风险的方法包括：根据进出站特征判断本次生成的付款图形码用于进站或出站；若为进站，则判断付款图形码生成请求的频率是否高于预设阈值，若是则确定存在交易风险；若为出站，则判断当前位置特征与历史风控特征中对应的进站位置特征是否符合预设位置关系条件，若否则确定存在交易风险；

[122] 应用侧接收到风控侧返回的不存在交易风险的结果后，生成并展示付款图形码。

20 [123] 图 10 示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 和总线 1050。其中处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040 通过总线 1050 实现彼此之间在设备内部的通信连接。

[124] 处理器 1010 可以采用通用的 CPU（Central Processing Unit，中央处理器）、微处理器、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[125] 存储器 1020 可以采用 ROM（Read Only Memory，只读存储器）、RAM（Random Access Memory，随机存取存储器）、静态存储设备，动态存储设备等形式实现。存储器 1020 可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施

例所提供的技术方案时,相关的程序代码保存在存储器 1020 中,并由处理器 1010 来调用执行。

[126] 输入/输出接口 1030 用于连接输入/输出模块,以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中(图中未示出),也可以外接于设备以提供相应功能。

5 其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等,输出设备可以包括显示器、扬声器、振动器、指示灯等。

[127] 通信接口 1040 用于连接通信模块(图中未示出),以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式(例如 USB、网线等)实现通信,也可以通过无线方式(例如移动网络、WIFI、蓝牙等)实现通信。

10 [128] 总线 1050 包括一通路,在设备的各个组件(例如处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040)之间传输信息。

[129] 需要说明的是,尽管上述设备仅示出了处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 以及总线 1050,但是在具体实施过程中,该设备还可以包括实现正常运行所必需的其他组件。此外,本领域的技术人员可以理解的是,上述设备中也可以仅包含实现本说明书实施例方案所必需的组件,而不必包含图中所示的全部组件。

15 [130] 本说明书实施例还提供一种计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现前述的支付风控方法。该方法至少包括:

[131] 一种支付风控方法,该方法包括:

20 [132] 应用侧接收到进出站付款操作触发后,生成携带预设风控特征的付款图形码生成请求,并将该请求发送至风控侧;所述风控特征至少包括:付款账号特征、当前位置特征及进出站特征;

[133] 风控侧接收到应用侧发送的付款图形码生成请求后,根据该请求中的付款账号特征,获取预先存储的该账号的历史风控特征;

25 [134] 风控侧通过比较读取的历史风控特征与该请求中携带的风控特征,检测应用侧是否存在交易风险,并向应用侧返回风控检测结果;其中,检测交易风险的方法包括:根据进出站特征判断本次生成的付款图形码用于进站或出站;若为进站,则判断付款图形码生成请求的频率是否高于预设阈值,若是则确定存在交易风险;若为出站,则判断当前位置特征与历史风控特征中对应的进站位置特征是否符合预设位置关系条件,若否则确定存在交易风险;

[135] 应用侧接收到风控侧返回的不存在交易风险的结果后,生成并展示付款图形码。

[136] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[137] 通过以上的实施方式的描述可知,本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解,本说明书实施例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,该计算机软件产品可以存储在存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

[138] 上述实施例阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机,计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[139] 本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于装置实施例而言,由于其基本相似于方法实施例,所以描述得比较简单,相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的,其中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,在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也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例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[140] 以上所述仅是本说明书实施例的具体实施方式,应当指出,对于本技术领域的

普通技术人员来说，在不脱离本说明书实施例原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本说明书实施例的保护范围。