(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 106934606 A
(43)申请公布日 2017.07.07

(21)申请号 201511022956.2

(22)申请日 2015.12.30

(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 倪飞

(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 林祥

(51)Int.Cl.
G06Q 20/08(2012.01)
G06Q 20/34(2012.01)
G06Q 20/40(2012.01)

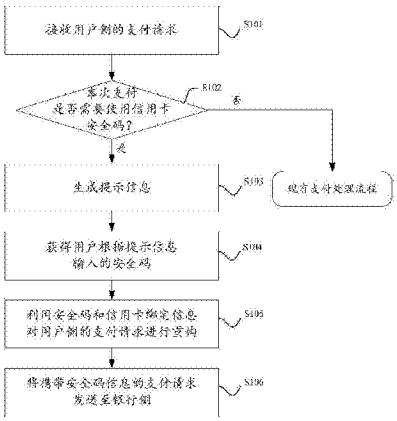
权利要求书2页 说明书8页 附图2页

(54)发明名称

一种信用卡支付请求处理方法及装置

(57)摘要

本申请公开了一种信用卡支付请求处理方法及装置。一种信用卡支付请求处理方法包括：接收用户侧的支付请求；在所述支付请求为基于已绑定信用卡的支付请求的情况下，判断本次支付是否需要使用信用卡安全码；如果是，则生成提示信息，以提示用户输入所述信用卡的安全码；获得用户根据所述提示信息输入的安全码；利用所获得的安全码和所述信用卡的绑定信息，对所述用户侧的支付请求进行重构，得到携带安全码信息的支付请求；将所述携带安全码信息的支付请求发送至银行侧。上述方案可以提高用户操作便捷性和输入成功率，降低第三方支付平台的支付失败率，减少系统资源的不必要消耗。



CN 106934606 A

1.一种信用卡支付请求处理方法，应用于第三方支付平台，其特征在于，该方法包括：

接收用户侧的支付请求；

在所述支付请求为基于已绑定信用卡的支付请求的情况下，判断本次支付是否需要使用信用卡安全码；

如果是，则生成提示信息，以提示用户输入所述信用卡的安全码；

获得用户根据所述提示信息输入的安全码；

利用所获得的安全码和所述信用卡的绑定信息，对所述用户侧的支付请求进行重构，得到携带安全码信息的支付请求；

将所述携带安全码信息的支付请求发送至银行侧。

2.根据权利要求1所述的方法，其特征在于，所述判断本次支付是否需要使用信用卡安全码，包括：

利用所述信用卡的绑定信息，对所述用户侧的支付请求进行重构；

将重构得到的支付请求发送至银行侧；

如果支付失败，则根据银行侧反馈的错误码判断支付失败原因是否包括缺少安全码，如果包括则确定本次支付需要使用信用卡安全码。

3.根据权利要求1所述的方法，其特征在于，所述判断本次支付是否需要使用信用卡安全码，包括：

根据所述用户侧的支付请求所对应的支付信息，判断本次支付是否与预先存储的信用卡安全码使用场景特征匹配，如果匹配则确定本次支付需要使用信用卡安全码。

4.根据权利要求3所述的方法，其特征在于，所述支付信息包括：

信用卡所属银行信息，和/或支付金额信息。

5.根据权利要求3所述的方法，其特征在于，所述方法还包括：

在判断结果为不匹配的情况下，利用所述信用卡的绑定信息，对所述用户侧的支付请求进行重构；

将重构得到的支付请求发送至银行侧；

如果支付失败，则根据银行侧反馈的错误码判断支付失败原因是否包括缺少安全码，如果包括则确定本次支付需要使用信用卡安全码。

6.根据权利要求5所述的方法，其特征在于，所述方法还包括：

根据银行侧反馈的错误码确定本次支付需要使用信用卡安全码后，对本次支付进行记录，所记录的内容用于生成信用卡安全码使用场景特征。

7.一种信用卡支付请求处理装置，应用于第三方支付平台，其特征在于，该装置包括：

支付请求接收模块，用于接收用户侧的支付请求；

判断模块，用于在所述支付请求为基于已绑定信用卡的支付请求的情况下，判断本次支付是否需要使用信用卡安全码；

提示模块，用于在判断本次支付需要使用信用卡安全码的情况下，则生成提示信息，以提示用户输入所述信用卡的安全码；

安全码获得模块，用于获得用户根据所述提示信息输入的安全码；

支付请求重构模块，用于利用所获得的安全码和所述信用卡的绑定信息，对所述用户侧的支付请求进行重构，得到携带安全码信息的支付请求；

支付请求发送模块，用于将所述携带安全码信息的支付请求发送至银行侧。

8.根据权利要求7所述的装置，其特征在于，所述判断模块，具体用于：

利用所述信用卡的绑定信息，对所述用户侧的支付请求进行重构；将重构得到的支付请求发送至银行侧；如果支付失败，则根据银行侧反馈的错误码判断支付失败原因是否包括缺少安全码，如果包括则确定本次支付需要使用信用卡安全码。

9.根据权利要求7所述的装置，其特征在于，所述判断模块，具体用于：

根据所述用户侧的支付请求所对应的支付信息，判断本次支付是否与预先存储的信用卡安全码使用场景特征匹配，如果匹配则确定本次支付需要使用信用卡安全码。

10.根据权利要求9所述的装置，其特征在于，所述支付信息包括：

信用卡所属银行信息，和/或支付金额信息。

11.根据权利要求9所述的装置，其特征在于，所述判断模块还用于：

在判断结果为不匹配的情况下，利用所述信用卡的绑定信息，对所述用户侧的支付请求进行重构；将重构得到的支付请求发送至银行侧；如果支付失败，则根据银行侧反馈的错误码判断支付失败原因是否包括缺少安全码，如果包括则确定本次支付需要使用信用卡安全码。

12.根据权利要求11所述的装置，其特征在于，所述装置还包括：

记录模块，用于在所述判断模块根据银行侧反馈的错误码确定本次支付需要使用信用卡安全码后，对本次支付进行记录，所记录的内容用于生成信用卡安全码使用场景特征。

一种信用卡支付请求处理方法及装置

技术领域

[0001] 本申请涉及第三方支付技术领域，尤其涉及一种信用卡支付请求处理方法及装置。

背景技术

[0002] 第三方支付是一种网络支付模式，这种模式是由具备信誉保障的独立机构采用与各大银行签约的方式，提供与银行支付结算系统接口的交易支持平台实现。第三方支付平台不仅降低了各类用户与银行之间的连接成本，而且能够有效地起到监管作用，已经成为目前主要的网络交易手段和信用中介。

[0003] 绑定银行卡是第三方支付平台用于提升用户支付体验的一种基本方式，在绑定过程中，用户需要将银行卡号码、姓名、身份证号码等基本信息提供给第三方支付平台，第三方支付平台验证无误后，将这些基本信息作为该银行卡的绑定信息进行保存。绑定完成后，用户进行网上交易时，只需要在第三方支付平台上选择已绑定的银行卡，第三方支付平台就会根据绑定信息自动与用户银行账户对接，从而避免了用户每次交易都输入银行卡号码等信息的麻烦。

[0004] 目前，主流的第三方支付平台不仅支持对借记卡的绑定，还能够支持对信用卡的绑定。与普通借记卡相比，信用卡具备一种特有的信息：信用卡安全码。该信息的作用与交易密码类似，都是用来确认用户身份的。在实际使用时，有些场景需要用户提供安全码才能完成支付，但是出于安全目的，第三方支付平台在对信用卡进行绑定时不会保存信用卡安全码。这样所导致的问题是：在需要提供安全码的支付场景，用户如果直接使用绑定的信用卡进行支付会出现错误。如果用户想要继续使用信用卡进行支付，只能按照使用新卡的方式，手动输入信用卡安全码以及卡号、姓名、身份证号等其他基本信息，不仅用户操作繁琐，误操作几率大大增加，对于第三方支付平台而言，支付失败所导致的重复处理也会带来额外的系统资源消耗。

发明内容

[0005] 针对上述技术问题，本申请提供一种信用卡支付请求处理方法及装置，技术方案如下：

[0006] 根据本申请的第一方面，提供一种信用卡支付请求处理方法，应用于第三方支付平台，该方法包括：

[0007] 接收用户侧的支付请求；

[0008] 在所述支付请求为基于已绑定信用卡的支付请求的情况下，判断本次支付是否需要使用信用卡安全码；

[0009] 如果是，则生成提示信息，以提示用户输入所述信用卡的安全码；

[0010] 获得用户根据所述提示信息输入的安全码；

[0011] 利用所获得的安全码和所述信用卡的绑定信息，对所述用户侧的支付请求进行重

构，得到携带安全码信息的支付请求；

[0012] 将所述携带安全码信息的支付请求发送至银行侧。

[0013] 根据本申请的第二方面，提供一种信用卡支付请求处理装置，应用于第三方支付平台，该装置包括：

[0014] 支付请求接收模块，用于接收用户侧的支付请求；

[0015] 判断模块，用于在所述支付请求为基于已绑定信用卡的支付请求的情况下，判断本次支付是否需要使用信用卡安全码；

[0016] 提示模块，用于在判断本次支付需要使用信用卡安全码的情况下，则生成提示信息，以提示用户输入所述信用卡的安全码；

[0017] 安全码获得模块，用于获得用户根据所述提示信息输入的安全码；

[0018] 支付请求重构模块，用于利用所获得的安全码和所述信用卡的绑定信息，对所述用户侧的支付请求进行重构，得到携带安全码信息的支付请求；

[0019] 支付请求发送模块，用于将所述携带安全码信息的支付请求发送至银行侧。

[0020] 应用本申请所提供的技术方案，第三方支付平台可以在需要提供信用卡安全码的支付场景下，仅要求用户补充输入安全码即可完成支付，避免用户手动输入已绑定过的其他基本信息，从而提高用户操作便捷性和输入成功率。对于第三方支付平台而言，则可以有效降低支付失败率，减少系统资源的不必要消耗。

[0021] 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，并不能限制本申请。

附图说明

[0022] 为了更清楚地说明本申请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申请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。

[0023] 图1是本申请的第三方支付平台交互架构示意图；

[0024] 图2是本申请的信用卡支付请求处理方法的流程示意图；

[0025] 图3是本申请的信用卡安全码使用判断方法的流程示意图；

[0026] 图4是本申请的信用卡支付请求处理装置的第一种结构示意图；

[0027] 图5是本申请的信用卡支付请求处理装置的第二种结构示意图。

具体实施方式

[0028] 信用卡安全码是打印在信用卡卡签名区的一串数字，它由卡号、有效期和服务约束代码经过发卡机构的编码规则和加密算法生成，一般为3位或4位，用于非现场交易时核对用户身份。不同发卡机构对信用卡安全码的叫法不同，例如VISA卡的安全码叫做CVV2(Card Verification Value 2)，MasterCard的安全码叫做CVC2(Card Validation Code 2)，但是本质作用是相同的。

[0029] 信用卡安全码在国际上应用相对广泛，目前国内的一些银行也开始支持该服务，信用卡用户仅凭安全码就可以利用电话或网络完成支付，因此安全码也被认为是信用卡的

“第二支付密码”，属于用户的隐私信息，第三方支付平台在绑定信用卡时不要求用户提供信用卡安全码，也不会对信用卡安全码进行保存。如果遇到需要使用信用卡安全码的情形，则已存储的信用卡绑定信息失效，现有的解决方案是引导用户使用其他资金账户(例如已绑定的借记卡)完成支付，或者引导用户以新卡(非绑定)的方式来使用信用卡。

[0030] 针对上述问题，本申请提供如下技术方案：

[0031] 第三方支付平台接收到基于已绑定信用卡的支付请求后，首先判断本次支付是否需要提供信用卡安全码，如果需要则提示用户补充输入安全码，然后利用户补充输入的安全码和已存储的信用卡绑定信息重新构建支付请求发送至银行侧。这种方式可以让让在不需要手动输入其他信用卡基本信息的情况下，继续使用已绑定的信用卡完成支付，从而提高用户操作便捷性和输入成功率。对于第三方支付平台而言，则可以有效降低支付失败率，减少系统资源的不必要消耗。

[0032] 为了使本领域技术人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于本申请保护的范围。

[0033] 在一个包含第三方支付的过程中，涉及的主体包括付款方、第三方支付平台、银行和收款方。本申请方案基于第三方支付平台实现，第三方支付平台的在支付过程中的作用是：根据付款方发起的支付请求，进一步向被绑定银行卡的所属银行发起支付请求，请求银行从付款方账户中转移支付费用至收款方账户。参见图1所示，在本申请方案中，第三方支付平台20实际涉及的交互主体包括付款方用户侧设备10和银行侧设备30，其中用户侧设备可以是PC机、手机、平板电脑等，第三方支付平台20和银行侧设备30则一般是服务器的形式，设备之间可通过各种形式的网络实现通信连接。为描述方便，在本申请后文中将分别以“用户侧”和“银行侧”对方案进行说明。

[0034] 图2所示，为本申请提供的信用卡支付请求处理方法的流程图，该方法可以包括以下步骤：

[0035] S101，接收用户侧的支付请求；

[0036] 付款方用户需要向收款方支付费用时，在个人设备上通过浏览器或专用客户端应用登录到第三方支付平台，选择已一张已在平台绑定的银行卡并确认支付后，用户设备向第三方支付平台发送支付请求，除了用户标识、被绑定银行卡标识之外，该支付请求中至少还应该携带支付费用信息和收款方信息。

[0037] S102，判断本次支付是否需要使用信用卡安全码；如果是则执行S103，否则转入现有的正常支付处理流程。

[0038] 本申请方案仅针对用户使用已绑定信用卡进行支付的场景提出，第三方支付平台接收到用户侧的支付请求后，首先判断该支付请求是否基于已绑定信用卡，如果是则进一步判断本次支付是否需要使用信用卡安全码，否则转入其他支付渠道的处理流程。

[0039] 关于如何判断本次支付是否需要使用信用卡安全码，本申请提供以下两种方案：

[0040] 方案1，根据银行侧的反馈消息判断：

[0041] 步骤a)重构支付请求；

[0042] 第三方支付平台首先根据支付请求中所指定的信用卡标识，获取该信用卡的绑定

信息，然后根据所获取的绑定信息，对用户侧的发来的支付请求进行重构。

[0043] 重构过程中，除了原支付请求中携带的支付费用信息和收款方信息之外，还要在支付请求中进一步添加信用卡号码，用户姓名、用户身份证号码、用户手机号码、信用卡有效期等绑定信息。需要说明的是，实际支付时，不同银行所要求提供的具体信息可能有所区别。但是除信用卡安全码之外，第三方支付平台对支付所需要的一般必要信息都可以进行存储，本申请对重构支付请求时所添加的绑定信息的具体内容也并不需要进行限定。

[0044] 步骤b)将重构得到的支付请求发送至银行侧；

[0045] 步骤c)根据银行侧的反馈消息，判断本次支付是否需要使用信用卡安全码。

[0046] 首先，由于重构的支付请求中已经包含了支付所需的一般必要信息，因此本次支付是有可能一次性成功的，这种情况下，本次支付处理实际已经完成，第三方支付平台可以直接向用户反馈支付成功信息。

[0047] 如果支付失败，则第三方支付平台需要进一步确定导致支付失败的原因。具体而言，在支付失败之后，银行侧向第三方支付平台反馈支付失败消息时会进一步提供错误码，第三方支付平台可以根据错误码来判断失败原因，并根据失败原因做出相应的处理：

[0048] 如果是由于缺少信用卡安全码而导致支付失败，则确定本次支付需要使用信用卡安全码，继续执行本申请方案的后续失败处理流程；

[0049] 如果是由于其他原因(例如账户余额不足、账户被冻结等)而导致支付失败，则按照现有技术的方案执行正常的失败处理流程。

[0050] 这里还存在一种可能出现的特殊情况是：失败原因既包括“缺少信用卡安全码”，也包括其他原因，此时可能需要根据具体情况判断是否继续执行本申请方案的失败处理流程，当然也可以是按照一定的优先级顺序执行不同原因所对应的失败处理流程，或者同时执行本申请方案的失败处理流程与其他原因所对应的失败处理流程。例如，一种可用的处理方案是：先确定各种原因的严重级别，然后根据失败原因的严重程度，优先执行较严重原因所对应的失败处理流程。当然，实际应用中的业务逻辑可能更为复杂，本实施例所提供的方案仅用于示意性说明，本领域技术人员可根据实际的业务需求灵活制订具体的处理方案。

[0051] 方案2，本地自主判断：

[0052] 在实际的业务处理过程中，“支付是否需要信用卡安全码”并不是一个随机事件，而是根据一些客观存在的规则所决定的，如果能够把这些规则模型化并且存储在第三方支付平台，那么第三方支付平台在接收到基于已绑定信用卡的支付请求后，就可以根据本次请求的具体情况，直接在本地判断出本次支付是否需要使用信用卡安全码。

[0053] 就目前而言，一笔支付是否需要信用卡安全码主要取决于各家银行的不同政策，而作为银行签约方的第三方支付平台，完全可以搜集到这些政策的内容，并将进一步这些政策的内容模型化，形成一系列的信用卡安全码使用场景特征，例如：

[0054] 银行A，任何情况都需要提供信用卡安全码；

[0055] 银行B，支付额度大于等于200元人民币时需要提供信用卡安全码；

[0056] 银行C，使用外币结算时需要提供信用卡安全码；

[0057] ……

[0058] 当然，以上规则仅用于示意性说明，具体的银行政策内容可能更为复杂，而且“支

付是否需要信用卡安全码”也有可能存在银行方面之外的影响因素，但是可以理解的是：只要有确定的规则，就能够建立起相应的规则模型。

[0059] 第三方支付平台根据各银行政策建立相应的规则模型，接收到基于信用卡的支付请求后，从支付请求中提取相关的支付信息，例如信用卡所属银行、支付额度、支付币种等等，然后判断这些信息是否与预存的信用卡安全码使用场景特征相匹配，如果匹配则确定本次支付需要使用信用卡安全码。

[0060] S103，生成提示信息，以提示用户输入所述信用卡的安全码；

[0061] 确定本次支付需要使用信用卡安全码后，第三方支付平台需要以某种方式告知用户：本次支付需要提供信用卡安全码。具体而言，第三方支付平台可以构建一个信用卡安全码输入界面，以网页或者客户端页面的形式展现在用户设备上，以提示用户补充输入信用卡安全码。在该界面中不需要用户重新填写其他在绑定时已经提供过的信息，例如姓名、身份证号码等等。当然，为了提高安全性，在该界面也可以进一步要求用户输入一些必要的认证信息，例如页面随机验证码、短信验证码等。此外，第三方支付平台也可以通过即时通信消息、短信等方式提示用户输入信用卡安全码，本申请对此并不需要进行限定。

[0062] S104，获得用户根据所述提示信息输入的安全码；

[0063] 用户根据第三方支付平台的提示补充输入安全码后，第三方支付平台获得该安全码，继续执行后续操作。

[0064] S105，利用所获得的安全码和所述信用卡的绑定信息，对用户侧的支付请求进行重构，得到携带安全码信息的支付请求；

[0065] 第三方支付平台根据用户补充输入的安全码和信用卡的绑定信息，对用户侧的发来的支付请求进行重构。

[0066] 重构过程中，除了原支付请求中携带的支付费用信息和收款方信息之外，还要在支付请求中进一步添加安全码、以及信用卡号码，用户姓名、用户身份证号码、用户手机号码、信用卡有效期等绑定信息。实际支付时，不同银行所要求提供的具体信息可能有所区别，除信用卡安全码之外，本申请对重构支付请求时所添加的绑定信息的具体内容不需要进行限定。

[0067] 需要说明的是，S102方案1中的重构支付请求与本步骤中的重构支付请求没有必然联系，两者的区别也很明显：

[0068] 前者仅利用“绑定信息”进行重构，重构结果中不携带安全码；

[0069] 后者利用“绑定信息”和“安全码”进行重构，重构结果中携带安全码。

[0070] S106，将携带安全码信息的支付请求发送至银行侧。

[0071] 第三方支付平台将携带安全码信息的支付请求发送到银行侧后，如果没有其他问题，那么本次支付将会直接成功，第三方支付平台可以直接向用户反馈支付成功信息。当然，这里也有可能由于其他非信用卡安全码的原因导致支付失败，这些与本申请方案无关，因此不再做进一步说明。

[0072] 在上面的实施例中，针对“如何判断本次支付是否需要使用信用卡安全码”，提供了“根据银行侧的反馈消息判断”和“本地自主判断”两种方案，其中第一种方案由于不需要本地数据的支持，因此实施门槛相对较低，而且由于是实时判断，因此能够保证判断的准确性，缺点在于但是需要增加至少一次第三方支付平台与银行侧的交互。第二种方案的优势

在于完全在第三方支付平台本地实现判断，但是要求积累足够的本地数据，并且可能会由于数据搜集不完全或更新不及时等客观因素，导致将实际需要使用安全码的情形误判为不需要使用安全码，进而转入现有的正常支付处理流程，而背景技术中所提到的问题仍然无法避免。

[0073] 针对以上两种方案的优缺点，本申请还提供一种改进的判断方案：首先利用本地方式进行判断，如果判断认为不需要使用信用卡安全码，再进一步利用银行侧反馈的方式进行判断。该方法的流程图可参见图3所示，具体步骤如下：

[0074] S102a，根据用户侧的支付请求所对应的支付信息，判断本次支付是否与预先存储的信用卡安全码使用场景特征匹配，如果匹配则转到S102b，如果不匹配则转到S102c；

[0075] S102b，确定本次支付需要使用信用卡安全码。

[0076] S102c，利用信用卡的绑定信息，对用户侧的支付请求进行重构，将重构得到的支付请求发送至银行侧；

[0077] S102d，如果支付失败，且根据银行侧反馈的错误码判断支付失败原因包括缺少安全码，则转到S102b，否则转到S102e；

[0078] S102e，确定本次支付不需要使用信用卡安全码，具体情况可能是支付成功，或者其他原因导致支付失败，与本申请方案无关，这里不再进一步说明。

[0079] 上述步骤S102a-S102e的具体实现可以参见S102中相关部分的描述，本实施例中不再重复说明。应用上述判断方法，首先利用本地方式进行初步判断，根据本地数据中存储的“需要使用安全码”的场景特征匹配，能够筛选出本次支付“需要使用安全码”的情况。但是考虑到本地数据可能搜集不够完整，或者更新不及时，因此对于无法匹配到特征的支付请求，也不直接认定其不需要使用安全码，而是转入银行侧反馈的方式做进一步判断。这样做的好处至少包括以下几个方面：

[0080] 首先，第三方支付平台仅在根据本地数据无法确定本次支付需要使用信用卡安全码的情况下，才会进一步与银行侧进行交互，可以有效节省交互开销；

[0081] 其次，经过第三方支付平台本地判断后，实际上已经筛选出一部分“需要安全码”的支付请求，这样在S102c所发送的支付请求成功率也会相应提高。

[0082] 最后，本地判断仅能确定“需要安全码”，而不会确定“不需要安全码”，从而避免将实际需要使用安全码的情形误判为不需要使用安全码。尽管仍然可能由于本地数据更新不及时等原因，导致将“不需要安全码”误判为“需要使用安全码”，但是后续也只会额外要求用户补充输入一次安全码，其代价远低于将“需要使用安全码”误判为“不需要使用安全码”、进而转入现有的正常支付处理流程所导致的各种问题。

[0083] 在S102d根据银行侧反馈的错误码确定本次支付需要使用安全码之后，还可以进一步针对本次支付的相关信息进行记录，这里的记录并不是指常规意义上的支付处理日志记录，而是希望利用这些信息来完善第三方支付平台本地的信用卡安全码使用场景特征数据。这是因为根据本实施例的方案，如何执行到了S102d分支，则说明第三方支付平台本地数据不足以识别当前的支付需求，而实时与银行侧交互的结果正好能够针对上述不足进行补充或更新。例如：用户希望使用银行D的信用卡支付人民币100元，而第三方支付平台本地并没有存储银行D的信用卡安全码使用场景特征，因此本地判断无法确定需要使用安全码，进而通过与银行侧交互的方式，得知在银行D使用信用卡支付任意金额都需要使用安全码，

则可以根据这条规则生成新的信用卡安全码使用场景特征，添加到本地存储的数据中。即便银行侧没有反馈具体的规则，所记录的内容也可以提醒维护人员：第三方支付平台本地数据不足以识别当前的支付需求，以便维护人员及时采取其他手段对本地数据进行更新，使得本地数据能够得到持续性完善。

[0084] 相应于上述方法实施例，本申请还提供一种应用于第三方支付平台的信用卡支付请求处理装置，参见4图所示，该装置可以包括：

[0085] 支付请求接收模块210，用于接收用户侧的支付请求；

[0086] 判断模块220，用于在所述支付请求为基于已绑定信用卡的支付请求的情况下，判断本次支付是否需要使用信用卡安全码；

[0087] 提示模块230，用于在判断本次支付需要使用信用卡安全码的情况下，则生成提示信息，以提示用户输入所述信用卡的安全码；

[0088] 安全码获得模块240，用于获得用户根据所述提示信息输入的安全码；

[0089] 支付请求重构模块250，用于利用所获得的安全码和所述信用卡的绑定信息，对所述用户侧的支付请求进行重构，得到携带安全码信息的支付请求；

[0090] 支付请求发送模块260，用于将所述携带安全码信息的支付请求发送至银行侧。

[0091] 在本申请的第一种装置具体实施方式中，判断模块220可以具体用于：

[0092] 利用信用卡的绑定信息，对用户侧的支付请求进行重构；将重构得到的支付请求发送至银行侧；如果支付失败，则根据银行侧反馈的错误码判断支付失败原因是否包括缺少安全码，如果包括则确定本次支付需要使用信用卡安全码。

[0093] 在本申请的第二种装置具体实施方式中，判断模块220可以具体用于：

[0094] 根据用户侧的支付请求所对应的支付信息，判断本次支付是否与预先存储的信用卡安全码使用场景特征匹配，如果匹配则确定本次支付需要使用信用卡安全码。

[0095] 在本申请的第三种装置具体实施方式中，判断模块220可以具体用于：

[0096] 首先根据用户侧的支付请求所对应的支付信息，判断本次支付是否与预先存储的信用卡安全码使用场景特征匹配，如果匹配则确定本次支付需要使用信用卡安全码。

[0097] 在判断结果为不匹配的情况下，利用信用卡的绑定信息，对用户侧的支付请求进行重构；将重构得到的支付请求发送至银行侧；如果支付失败，则根据银行侧反馈的错误码判断支付失败原因是否包括缺少安全码，如果包括则确定本次支付需要使用信用卡安全码。

[0098] 如图4所示，根据本申请的第三种装置具体实施方式，该装置还可以进一步包括：

[0099] 记录模块270，用于在判断模块220根据银行侧反馈的错误码确定本次支付需要使用信用卡安全码后，对本次支付进行记录，所记录的内容用于生成信用卡安全码使用场景特征。

[0100] 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。

[0101] 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申请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)执行本申请各个实施例或者实施例的某些部分所述的方法。

[0102] 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,在实施本申请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。

[0103] 以上所述仅是本申请的具体实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本申请原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本申请的保护范围。

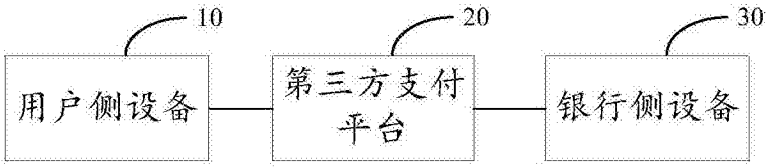

10
20
30
用户侧设备
第三方支付平台
银行侧设备

图1

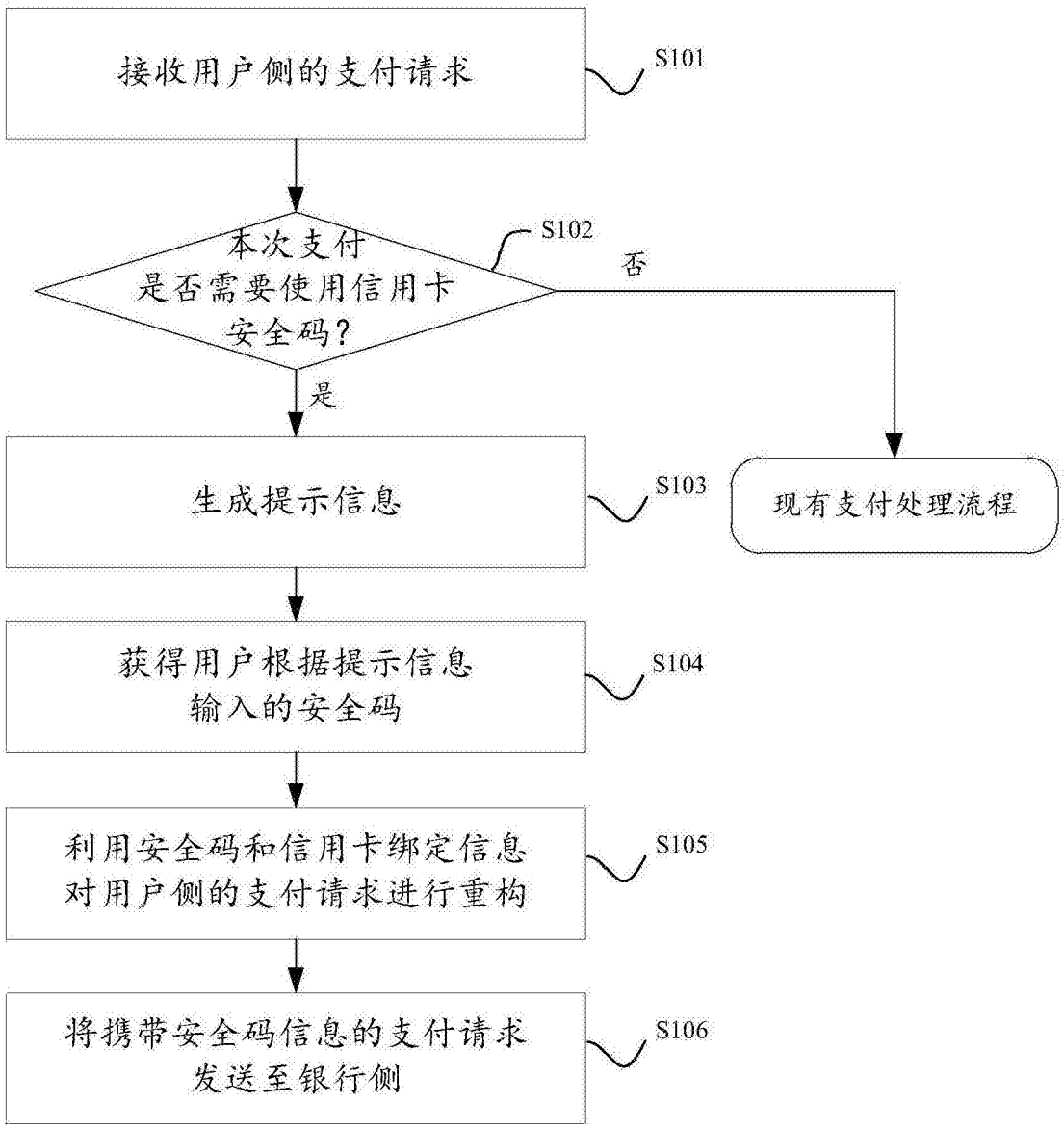

接收用户侧的支付请求
S101
本次支付是否需要使用信用卡安全码?
S102
否
是
生成提示信息
S103
现有支付处理流程
获得用户根据提示信息输入的安全码
S104
利用安全码和信用卡绑定信息对用户侧的支付请求进行重构
S105
将携带安全码信息的支付请求发送至银行侧
S106

图2

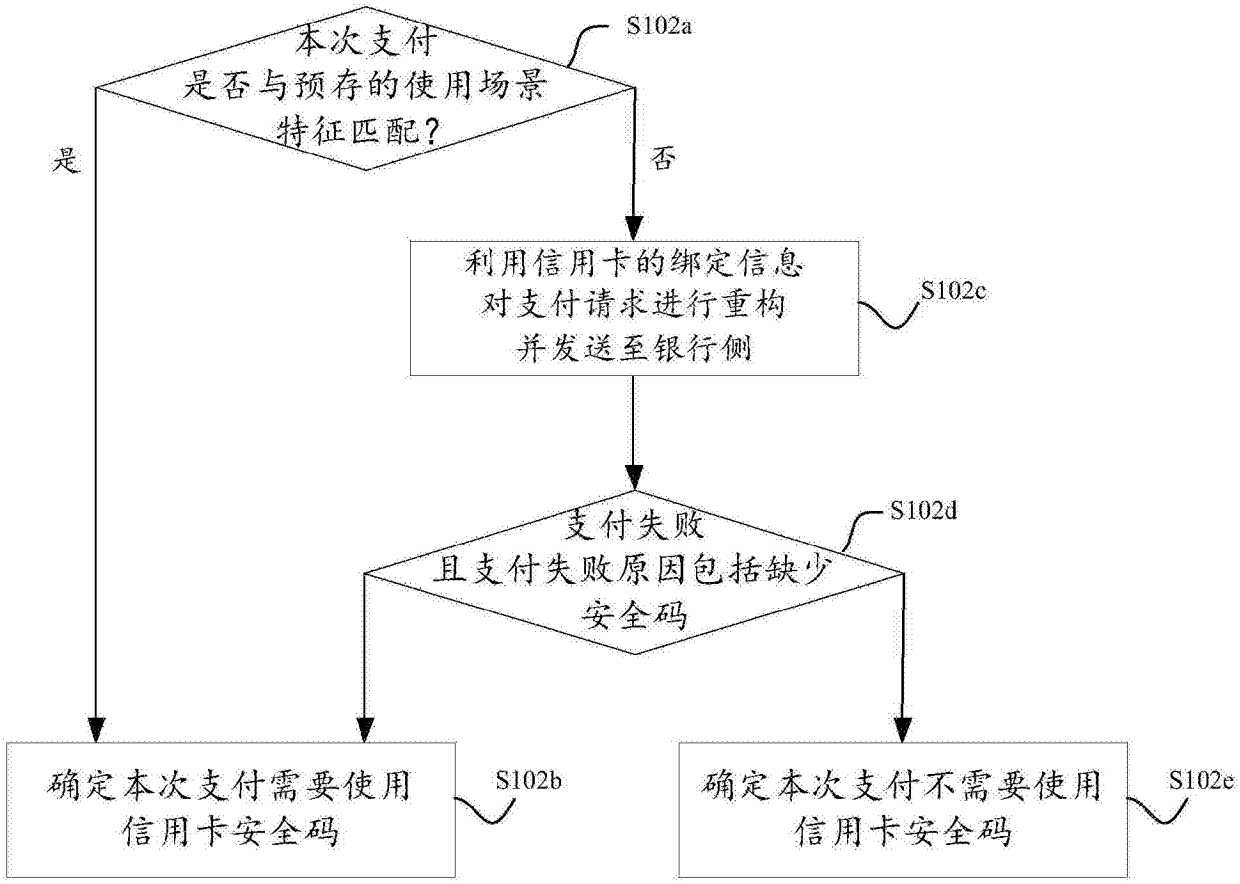

本次支付
是否与预存的使用场景
特征匹配?
S102a
是
否
利用信用卡的绑定信息
对支付请求进行重构
并发送至银行侧
S102c
支付失败
且支付失败原因包括缺少
安全码
S102d
确定本次支付需要使用
信用卡安全码
S102b
确定本次支付不需要使用
信用卡安全码
S102e

图3

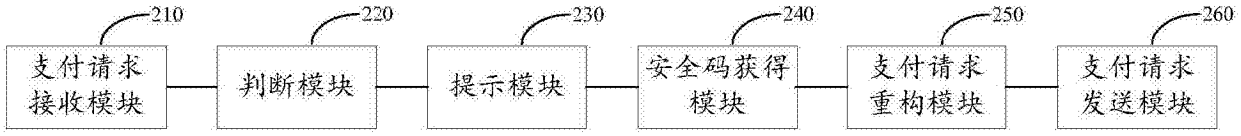

210
支付请求
接收模块
220
判断模块
230
提示模块
240
安全码获得
模块
250
支付请求
重构模块
260
支付请求
发送模块

图4

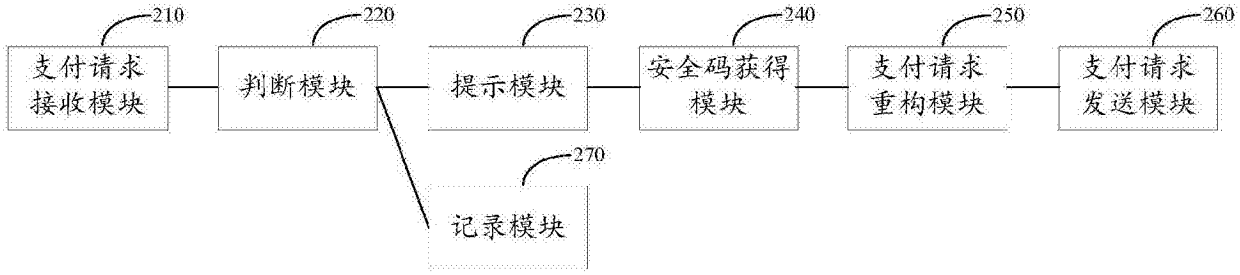

210
支付请求
接收模块
220
判断模块
230
提示模块
240
安全码获得
模块
250
支付请求
重构模块
260
支付请求
发送模块
270
记录模块

图5