

(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
2016 年 3 月 3 日 (03.03.2016)



(10) 国际公布号
WO 2016/029795 A1

- (51) 国际专利分类号:
G06Q 20/38 (2012.01)
- (21) 国际申请号: PCT/CN2015/086618
- (22) 国际申请日: 2015 年 8 月 11 日 (11.08.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410431210.6 2014 年 8 月 27 日 (27.08.2014) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [GB/CN]; 开曼群岛大开曼乔治城资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 沈星宇 (SHEN, Xingyu) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。黄冕 (HUANG, Mian) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。李潇霄 (LI, Xiaoxiao) [CN/CN]; 中国浙江省杭州市余杭区文一

西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY, INC.); 中国北京市朝阳区西坝河西里 28 号英特公寓 C 座 104 室, Beijing 100028 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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,

[见续页]

(54) Title: METHOD AND DEVICE FOR DETECTING PAYMENT SECURITY

(54) 发明名称: 支付安全性的检测方法和装置

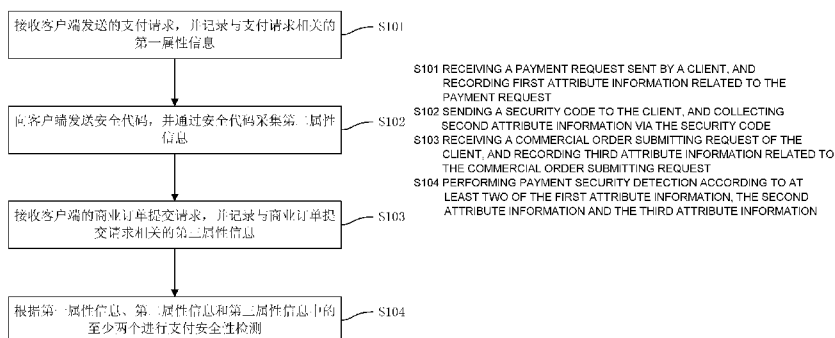


图 1 / Fig. 1

(57) Abstract: A detection method and detection device for payment security. The method comprises the following steps: receiving a payment request sent by a client, and recording first attribute information related to the payment request (S101); sending a security code to the client, and collecting second attribute information via the security code (S102); receiving a commercial order submitting request of the client, and recording third attribute information related to the commercial order submitting request (S103); and performing payment security detection according to at least two of the first attribute information, the second attribute information and the third attribute information (S104). The method enables an IP acquired by a payment service provider to be more accurate, so that the payment service provider can perform security detection on a payment operation according to the more accurate IP, and the accuracy is improved.

(57) 摘要: 一种支付安全性的检测方法及检测装置, 该方法包括下述步骤: 接收客户端发送的支付请求, 并记录于支付请求相关的第一属性信息 (S101); 向客户端发送安全代码, 并通过安全代码采集第二属性信息 (S102); 接收客户端的商业订单提交请求, 并记录与商业订单提交请求相关的第三属性信息 (S103); 以及根据第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测 (S104)。该方法使得支付服务商获取到的 IP 更加准确, 从而支付服务商根据更加准确的 IP 即可对支付操作进行安全性检测, 提高了准确率。



WO 2016/029795 A1



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))。

支付安全性的检测方法和装置

技术领域

本申请涉及电子商务技术领域，尤其涉及一种支付安全性的检测方法和装置。

背景技术

目前互联网上存在一种钓鱼欺诈方式，即钓鱼网站自动在服务端创建商家网站的支付订单，之后将跳转到支付服务提供商页面的链接或表单在用户页面上触发提交或跳转，因为钓鱼网站会模拟用户想要支付的订单的页面，所以用户就会继续支付，导致上当受骗，遭到金钱损失。这类钓鱼网站的特征是创建商家网站的支付订单的 IP（Internet Protocol，网络之间互连的协议）和用户支付平台付款的 IP 不是同一个 IP，但是正常用户操作应该是同一个 IP。

相关技术中，为了避免钓鱼网站模拟用户想要支付的订单页面而导致用户上当受骗的问题，可通过商家网站先获取创建订单的 IP，再通过表单将该 IP 提交给支付服务提供商的页面，以供支付平台判断是否有钓鱼风险。

但是，通过商家网站获取创建订单的 IP 再将其传给支付平台的方法存在以下缺陷：

1) 商家网站取 IP 的逻辑会由于商家开发的技术或服务器架构中的负载均衡、反向代理等设备的存在导致无法统一，例如，有取到内网 IP 而导致大批支付失败，又如，如果取了标头 header（服务器以 HTTP（Hypertext transfer protocol，超文本传输协议）协议传 HTML（HyperText Markup language，超级文本标记语言）资料到浏览器前所送出的字串）中的 IP 会被钓鱼网站恶意伪

造 header 中的 IP，绕过防控，因此，商家很难获取到准确的 IP；

2) 由于有些网络服务商的设备会因为某些业务需要配置了修改 URL (Uniform Resource Locator: 统一资源定位器) 中的 IP 值，如内容服务器，因此，IP 在传输过程中可能会被网络服务商篡改，从而导致区域性的支付失败。

由于存在上述缺陷，所以会导致支付服务提供商接收到的商家网站提供的用户 IP 不准确，从而影响支付安全性的检测，可能会导致检测结果不准确。

发明内容

本申请的目的在于至少在一定程度上解决上述的技术问题之一。

为此，本申请的一个目的在于提出一种支付安全性的检测方法。该方法使得支付服务商获取到的 IP 更加准确，从而支付服务商根据更加准确的 IP 即可对支付操作进行安全性检测，提高了准确率。

本申请的另一个目的在于提出一种支付安全性的检测装置。

为了实现上述目的，本申请一方面实施例的支付安全性的检测方法，包括：接收客户端发送的支付请求，并记录与所述支付请求相关的第一属性信息；向所述客户端发送安全代码，并通过所述安全代码采集第二属性信息；接收所述客户端的商业订单提交请求，并记录与所述商业订单提交请求相关的第三属性信息；以及根据所述第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测。

本申请实施例的支付安全性的检测方法，可先接收客户端发送的支付请求，并记录与支付请求相关的第一属性信息，之后可向客户端发送安全代码，并通过安全代码采集第二属性信息，然后接收客户端的商业订单提交请求，并

记录与商业订单提交请求相关的第三属性信息，以及根据第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测，在整个支付检测过程中，通过支付服务商来获取用户 IP，至少具有以下优点：（1）不会受到商家开发的技术或服务器架构中的负载均衡、反向代理等设备的影响，通过支付接口直接即可准确地获取到用户 IP；（2）通过支付接口直接获取网络层 IP，避免了 IP 在传输过程中会被网络服务商篡改的风险，从而使得支付服务商获取到的 IP 更加准确，从而支付服务商根据更加准确的 IP 即可对支付操作进行安全性检测，提高了准确率。

为了实现上述目的，本申请另一方面实施例的支付安全性的检测装置，包括：第一接收模块，用于接收客户端发送的支付请求，并记录与所述支付请求相关的第一属性信息；发送模块，用于向所述客户端发送安全代码；采集模块，用于通过所述安全代码采集第二属性信息；第二接收模块，用于接收所述客户端的商业订单提交请求，并记录与所述商业订单提交请求相关的第三属性信息；以及检测模块，用于根据所述第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测。

本申请实施例的支付安全性的检测装置，可通过第一接收模块接收客户端发送的支付请求，并记录与支付请求相关的第一属性信息，发送模块向客户端发送安全代码，采集模块通过安全代码采集第二属性信息，第二接收模块接收客户端的商业订单提交请求，并记录与商业订单提交请求相关的第三属性信息，检测模块根据第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测，在整个支付检测过程中，通过支付服务商来获取用户 IP，至少具有以下优点：（1）不会受到商家开发的技术或服务器架构中的负载均衡、反向代理等设备的影响，通过支付接口直接即可准确地获取到用户 IP；（2）

通过支付接口直接获取网络层 IP，避免了 IP 在传输过程中会被网络服务商篡改的风险，从而使得支付服务商获取到的 IP 更加准确，从而支付服务商根据更加准确的 IP 即可对支付操作进行安全性检测，提高了准确率。

5 本申请附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本申请的实践了解到。

附图说明

本申请上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

10 图 1 是根据本申请一个实施例的支付安全性的检测方法的流程图；

图 2 是根据本申请一个实施例的通过安全代码采集第二属性信息的流程图；

图 3 是根据本申请一个实施例的支付安全性的检测方法的示意图；

图 4 是根据本申请一个实施例的支付安全性的检测装置的结构示意图；

15 图 5 是根据本申请另一个实施例的支付安全性的检测装置的结构示意图；

图 6 是根据本申请又一个实施例的支付安全性的检测装置的结构示意图；

图 7 是根据本申请再一个实施例的支付安全性的检测装置的结构示意图；

图 8 是根据本申请又另一个实施例的支付安全性的检测装置的结构示意图。

20

具体实施方式

下面详细描述本申请的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元

件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本申请，而不能理解为对本申请的限制。

下面参考附图描述本申请实施例的支付安全性的检测方法和装置。

图 1 是根据本申请一个实施例的支付安全性的检测方法的流程图。如图 1 所示，该支付安全性的检测方法可以包括：

S101，接收客户端发送的支付请求，并记录与支付请求相关的第一属性信息。

其中，在本申请的实施例中，客户端可理解为商户网站。

具体地，客户端可在下单页面向支付平台发起 JS（JavaScript，直译式脚本语言）支付请求，支付平台服务器在接收到客户端发送的支付请求之后，可获取并记录与该支付请求相关的第一属性信息，如网络层的 IP，此处的 IP 可理解为在客户端下单页面时的 IP。

S102，向客户端发送安全代码，并通过安全代码采集第二属性信息。

进一步的，在本申请的一个实施例中，在向客户端发送安全代码之前，该支付安全性的检测方法还可包括：提取支付请求中的 Refer 信息，其中，当 Refer 信息为空时将安全代码发送至客户端。

需要说明的是，在客户端下单页面时，下单页面发起的支付请求的来源，正常情况下应该是客户端的页面。因此，此时需判断该支付请求的来源是否为客户端的下单页面。具体地，可提取支付请求中的 Refer 信息，并记录该 Refer 信息所对应的值。其中，当 Refer 信息所对应的值为空时，可判断该支付请求可能是钓鱼网站创建的支付请求，此时，将安全代码发送至客户端以使客户端对钓鱼风险进行防控。

进一步的，在本申请的一个实施例中，在向客户端发送安全代码之前，该

支付安全性的检测方法还可包括：通过混淆算法对安全代码进行混淆以生成混淆字符串以将混淆之后的安全代码和混淆字符串发送至客户端。其中，在本申请的实施例中，安全代码可理解为攻防 JS 代码。例如，可通过不可逆混淆算法对攻防 JS 代码进行混淆，生成混淆字符串，之后将混淆之后的攻防 JS 代码和混淆字符串发送至客户端。其中，可以理解，混淆字符串可起动防采集的作用。需要说明的是，在本申请的实施例中，混淆算法需要定期更新，或者安全代码进行实时混淆，且在定期更新或实时混淆时加入一个混淆字符串定义在安全代码的变量中，从而对安全代码起到保护作用。

在本申请的实施例中，如图 2 所示，通过安全代码采集第二属性信息具体可包括：客户端运行安全代码以使安全代码采集第二属性信息（S201）。之后，客户端对第二属性信息和混淆字符串进行签名以生成签名信息（S202）。然后，接收客户端发送的第二属性信息和签名信息，并根据签名信息对第二属性信息进行验证（S203）。应当理解，此处的混淆字符串为上述客户端接收的混淆字符串。

举例而言，在本申请的实施例中，第二属性信息以“location.host”、“parent.location.host”为例，在客户端接收到安全代码，并运行安全代码之后，可通过安全代码采集“location.host”、“parent.location.host”信息。之后，客户端可对“location.host”、“parent.location.host”和混淆字符串进行 MD5（Message Digest Algorithm，消息摘要算法第五版）签名，以生成签名信息，如：MD5(location.host+混淆字符串+parent.location.host)，防止篡改。然后，可接收客户端发送的第二属性信息和签名信息，之后可对签名信息进行解密，根据解密后的签名信息对第二属性信息进行验证，以验证接收到的第二属性信息是否与解密后的签名信息中的第二属性信息一致。由此，保证第二属性信息的来源

是客户端。

S103, 接收客户端的商业订单提交请求, 并记录与商业订单提交请求相关的第三属性信息。

其中, 在本申请的实施例中, 第三属性信息可为商业订单在支付平台收
5 台支付时的网络层 IP 地址。

S104, 根据第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测。

其中, 在本申请的一个实施例中, 第一属性信息可为客户端发送支付请求时的第一 IP 地址, 第二属性信息可为通过安全代码采集的客户端的第二 IP 地
10 址, 第三属性信息可为客户端发送商业订单提交请求时的第三 IP 地址。其中, 在本申请的实施例中, 如果第一 IP 地址、第二 IP 地址和第三 IP 地址中的任意两个不同, 则判断为高危支付。

例如, 第一属性信息为客户端发送支付请求时的网络层第一 IP 地址, 第二属性信息为在通过安全代码采集第二属性信息之后返回客户端信息时的网
15 络层第二 IP 地址, 第三属性信息为客户端发送商业订单提交请求时的网络层第三 IP 地址, 将第一 IP 地址、第二 IP 地址和第三 IP 地址进行对比, 当第一 IP 地址、第二 IP 地址和第三 IP 地址中的任意两个不同时, 可判断支付过程为高危支付, 并可提醒用户有钓鱼风险。

在本申请的另一个实施例中, 第一属性信息可为通过支付请求获取的第一
20 域名信息, 第二属性信息可为安全代码采集的第二域名信息。其中, 在本申请的实施例中, 如果第一域名信息与第二域名信息不同, 则判断为高危支付。

例如, 第一属性信息可为通过支付请求获取的 Refer 信息的域名 location.host (即第一域名信息), 第二属性信息为安全代码采集客户端的域名

“location.host”（即第二域名信息），可将第一域名信息和第二域名信息进行对比，当第一域名信息和第二域名信息不同时，可判断支付过程为高危支付，并可提醒用户有钓鱼风险。

进一步的，在本申请的一个实施例中，该支付安全性的检测方法还可包括：

- 5 记录接收到支付请求时的第一时间戳，并记录接收到第二属性信息时的第二时间戳；如果第一时间戳和第二时间戳之间的时间小于第一预设阈值，或者，第一时间戳和第二时间戳之间的时间大于第二预设阈值，则判断为高危支付，其中，第二预设阈值大于第一预设阈值。可以理解，第一预设阈值和第二预设阈值可根据实际情况设定。由此，为保证支付的安全性，需保证从接收到的支付
- 10 请求开始直到接收到第二属性信息时为止，这个过程所花费的时间控制在正常合理的范围内。

- 本申请实施例的支付安全性的检测方法，可先接收客户端发送的支付请求，并记录与支付请求相关的第一属性信息，之后可向客户端发送安全代码，并通过安全代码采集第二属性信息，然后接收客户端的商业订单提交请求，并
- 15 记录与商业订单提交请求相关的第三属性信息，以及根据第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测，在整个支付检测过程中，通过支付服务商来获取用户 IP，至少具有以下优点：（1）不会受到商家开发的技术或服务器架构中的负载均衡、反向代理等设备的影响，通过支付接口直接即可准确地获取到用户 IP；（2）通过支付接口直接获取网络层 IP，
- 20 避免了 IP 在传输过程中会被网络服务商篡改的风险，从而使得支付服务商获取到的 IP 更加准确，从而支付服务商根据更加准确的 IP 即可对支付操作进行安全性检测，提高了准确率。

为了使得本领域的技术人员更加地了解本申请，下面可举例说明。

举例而言，如图 3 所示，以客户端为商户网站为例，首先，商户网站可通过商业页面发起 JS 请求（即支付请求）。支付平台可接收到该 JS 请求（S1），并获取到该商户网站在下单页面时的网络层 IP1，并可将 IP1 记录到会话 session 中（S11），之后可记录 JS 请求中的 Refer1 到 session，并通过 Refer1 的值来判断是否需要向商户网站发送攻防 JS 代码；当 Refer1 的值为空时，向商户网站发送攻防 JS 代码（S12），同时获取接收到支付请求时的当前时间戳 1（即第一时间戳）（S13），并记录到 session，之后可通过混淆算法将混淆之后的攻防 JS 代码返回到商户网站，即返回不可逆混淆的“js+cookie(sessionid)”（S14）。支付平台向商户网站返回 JS+cookie（S2），通过攻防 JS 代码可获取 location.host（S21），获取 parent（S22），获取攻防 JS 代码自带的混淆字符串（S23），之后对 location.host、parent 和混淆字符串这三个字符串进行 MD5 签名以得到签名信息（S24），之后通过 get 提交 location.host、parent 和签名信息到支付平台（S25）。支付平台接收到商户网站返回的验证字符串（S3），同时获取此时的网络层 IP2（S31），并获取当前时间戳 2（即第二时间戳），并将其记录到 session（S32），之后解密被加密的字符串以取到 location.host1 和 parent.location.host2（S33）。当支付平台接收到商业订单提交请求时（S4），支付平台获取此时的网络层 IP3（S41），之后，取出 session 中的 IP1、Refer1、时间戳 1、时间戳 2、IP2、location.host1、parent.location.host2 和 IP3（S42），之后可根据这些数据来综合判断用户付款时是否安全（S43）。

为了实现上述实施例，本申请还提出了一种支付安全性的检测装置。

图 4 是根据本申请一个实施例的支付安全性的检测装置的结构示意图。如

图 4 所示, 该支付安全性的检测装置可以包括: 第一接收模块 10、发送模块 20、采集模块 30、第二接收模块 40 和检测模块 50。

具体地, 第一接收模块 10 可用于接收客户端发送的支付请求, 并记录与支付请求相关的第一属性信息。其中, 在本申请的实施例中, 客户端可理解为
5 商户网站。

更具体地, 客户端可在下单页面向支付平台发起 JS (JavaScript, 直译式脚本语言) 支付请求, 第一接收模块 10 在接收到客户端发送的支付请求之后, 可获取并记录与该支付请求相关的第一属性信息, 如网络层的 IP, 此处的 IP 可理解为在客户端下单页面时的 IP。

10 发送模块 20 可用于向客户端发送安全代码。采集模块 30 可用于通过安全代码采集第二属性信息。

进一步的, 在本申请的一个实施例中, 如图 5 所示, 该支付安全性的检测装置还可包括提取模块 60。提取模块 60 可用于提取支付请求中的 Refer 信息, 其中, 发送模块 20 具体用于在 Refer 信息为空时将安全代码发送至客户端。

15 需要说明的是, 在客户端下单页面时, 下单页面发起的支付请求的来源, 正常情况下应该是客户端的页面。因此, 此时需判断该支付请求的来源是否为客户端的下单页面。具体地, 提取模块 60 可提取支付请求中的 Refer 信息, 并记录该 Refer 信息所对应的值。其中, 当 Refer 信息所对应的值为空时, 可判断该支付请求可能是钓鱼网站创建的支付请求, 此时, 发送模块 20 将安全
20 代码发送至客户端以使客户端对钓鱼风险进行防控。

进一步的, 在本申请的一个实施例中, 如图 6 所示, 该支付安全性的检测装置还可包括生成模块 70。生成模块 70 可用于通过混淆算法对安全代码进行混淆以生成混淆字符串。在本申请的实施例中, 发送模块 20 还可用于

将混淆之后的安全代码和混淆字符串发送至客户端。其中，在本申请的实施例中，安全代码可理解为攻防 JS 代码。

例如，生成模块 70 可通过不可逆混淆算法对攻防 JS 代码进行混淆，生成混淆字符串。发送模块 20 可将混淆之后的攻防 JS 代码和混淆字符串发送至客户端。其中，可以理解，混淆字符串可起动防采集的作用。需要说明的是，在本申请的实施例中，混淆算法需要定期更新，或者安全代码进行实时混淆，且在定期更新或实时混淆时加入一个混淆字符串定义在安全代码的变量中，从而对安全代码起到保护作用。

如图 4 所示，第二接收模块 40 可用于接收客户端的商业订单提交请求，并记录与商业订单提交请求相关的第三属性信息。其中，在本申请的实施例中，第三属性信息可为商业订单在支付平台收银台支付时的网络层 IP 地址。

如图 4 所示，检测模块 50 可用于根据第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测。

其中，在本申请的一个实施例中，第一属性信息为客户端发送支付请求时的第一 IP 地址，第二属性信息为通过安全代码采集的客户端的第二 IP 地址，第三属性信息为客户端发送商业订单提交请求时的第三 IP 地址，其中，检测模块 50 可具体用于在第一 IP 地址、第二 IP 地址和第三 IP 地址中的任意两个不同时，判断为高危支付。

例如，第一属性信息为客户端发送支付请求时的网络层第一 IP 地址，第二属性信息为在通过安全代码采集第二属性信息之后返回客户端信息时的网络层第二 IP 地址，第三属性信息为客户端发送商业订单提交请求时的网络层第三 IP 地址，检测模块 50 可将第一 IP 地址、第二 IP 地址和第三 IP 地址进行对比，当第一 IP 地址、第二 IP 地址和第三 IP 地址中的任意两个不同时，可

判断支付过程为高危支付，并可提醒用户有钓鱼风险。

在本申请的另一个实施例中，第一属性信息为通过支付请求获取的第一域名信息，第二属性信息为安全代码采集的第二域名信息，其中，检测模块 50 可具体用于在第一域名信息与第二域名信息不同时，判断为高危支付。

5 例如，第一属性信息可为通过支付请求获取的 Refer 信息的域名 location.host（即第一域名信息），第二属性信息为安全代码采集客户端的域名“location.host”（即第二域名信息），检测模块 50 可将第一域名信息和第二域名信息进行对比，当第一域名信息和第二域名信息不同时，可判断支付过程为高危支付，并可提醒用户有钓鱼风险。

10 进一步的，在本申请的一个实施例中，如图 7 所示，采集模块 30 可包括接收单元 31 和验证单元 32。接收单元 31 可用于接收客户端发送的第二属性信息和签名信息，其中，客户端运行安全代码以使安全代码采集第二属性信息，客户端对第二属性信息和混淆字符串进行签名以生成签名信息。验证单元 32 可用于根据签名信息对第二属性信息进行验证。应当理解，此处的混淆字符串
15 为上述客户端接收的混淆字符串。

举例而言，在本申请的实施例中，第二属性信息以“location.host”、“parent.location.host”为例，在客户端接收到安全代码，并运行安全代码之后，可通过安全代码采集“location.host”、“parent.location.host”信息。之后，客户端可对“location.host”、“parent.location.host”和混淆字符串进行 MD5（Message
20 Digest Algorithm，消息摘要算法第五版）签名，以生成签名信息，如：
MD5(location.host+混淆字符串+parent.location.host)，防止篡改。然后，接收单元 31 可接收客户端发送的第二属性信息和签名信息，验证单元 32 可对签名信息进行解密，根据解密后的签名信息对第二属性信息进行验证，以验证接收到

的第二属性信息是否与解密后的签名信息中的第二属性信息一致。由此，保证第二属性信息的来源是客户端。

进一步的，在本申请的一个实施例中，如图 8 所示，该支付安全性的检测装置还可包括记录模块 80。记录模块 80 可用于记录接收到支付请求时的第一时间戳，并记录接收到第二属性信息时的第二时间戳。其中，在本申请的实施例中，检测模块 50 还可具体用于在第一时间戳和第二时间戳之间的时间小于第一预设阈值，或者，第一时间戳和第二时间戳之间的时间大于第二预设阈值时，判断为高危支付，其中，第二预设阈值大于第一预设阈值。可以理解，第一预设阈值和第二预设阈值可根据实际情况设定。由此，为保证支付的安全性，需保证从接收到的支付请求开始直到接收到第二属性信息时为止，这个过程所花费的时间控制在正常合理的范围内。

本申请实施例的支付安全性的检测装置，可通过第一接收模块接收客户端发送的支付请求，并记录与支付请求相关的第一属性信息，发送模块向客户端发送安全代码，采集模块通过安全代码采集第二属性信息，第二接收模块接收客户端的商业订单提交请求，并记录与商业订单提交请求相关的第三属性信息，检测模块根据第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测，在整个支付检测过程中，通过支付服务商来获取用户 IP，至少具有以下优点：（1）不会受到商家开发的技术或服务器架构中的负载均衡、反向代理等设备的影响，通过支付接口直接即可准确地获取到用户 IP；（2）通过支付接口直接获取网络层 IP，避免了 IP 在传输过程中会被网络服务商篡改的风险，从而使得支付服务商获取到的 IP 更加准确，从而支付服务商根据更加准确的 IP 即可对支付操作进行安全性检测，提高了准确率。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本申请的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本申请的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本申请的实施例所属技术领域的技术人员所理解。

在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备（如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统）使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，“计算机可读介质”可以是任何可以包含、存储、通信、传播或传输程序以供指

令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。计算机可读介质的更具体的示例（非穷尽性列表）包括以下：具有一个或多个布线的电连接部（电子装置），便携式计算机盘盒（磁装置），随机存取存储器（RAM），只读存储器（ROM），可擦除可编程只读存储器（EPROM 或闪速存储器），光纤装置，以及便携式光盘只读存储器（CDROM）。另外，计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质，因为可以例如通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序，然后将其存储在计算机存储器中。

应当理解，本申请的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列（PGA），现场可编程门阵列（FPGA）等。

本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

此外，在本申请各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的

形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

上述提到的存储介质可以是只读存储器，磁盘或光盘等。尽管上面已经示出和描述了本申请的实施例，可以理解的是，上述实施例是示例性的，不能理解为本申请的限制，本领域的普通技术人员在本申请的范围内可以对上述实施例进行变化、修改、替换和变型。

权 利 要 求 书

1、一种支付安全性的检测方法，其特征在于，包括以下步骤：

接收客户端发送的支付请求，并记录与所述支付请求相关的第一属性信息；

向所述客户端发送安全代码，并通过所述安全代码采集第二属性信息；

接收所述客户端的商业订单提交请求，并记录与所述商业订单提交请求相关的第三属性信息；以及

根据所述第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测。

2、如权利要求 1 所述的支付安全性的检测方法，其特征在于，其中，所述第一属性信息为所述客户端发送所述支付请求时的第一 IP 地址，所述第二属性信息为通过所述安全代码采集的所述客户端的第二 IP 地址，所述第三属性信息为所述客户端发送所述商业订单提交请求时的第三 IP 地址，其中，

如果所述第一 IP 地址、所述第二 IP 地址和所述第三 IP 地址中的任意两个不同，则判断为高危支付。

3、如权利要求 1 所述的支付安全性的检测方法，其特征在于，所述第一属性信息为通过所述支付请求获取的第一域名信息，所述第二属性信息为所述安全代码采集的第二域名信息，其中，

如果所述第一域名信息与所述第二域名信息不同，则判断为高危支付。

4、如权利要求 1-3 任一项所述的支付安全性的检测方法，其特征在于，在所述向所述客户端发送安全代码之前，还包括：

提取所述支付请求中的 Refer 信息，其中，当所述 Refer 信息为空时将所

述安全代码发送至所述客户端。

5、如权利要求 4 所述的支付安全性的检测方法，其特征在于，在所述向所述客户端发送安全代码之前，还包括：

通过混淆算法对所述安全代码进行混淆以生成混淆字符串以将混淆之后
5 的安全代码和所述混淆字符串发送至所述客户端。

6、如权利要求 5 所述的支付安全性的检测方法，其特征在于，所述通过所述安全代码采集第二属性信息具体包括：

所述客户端运行所述安全代码以使所述安全代码采集所述第二属性信息；

所述客户端对所述第二属性信息和所述混淆字符串进行签名以生成签名
10 信息；

接收所述客户端发送的所述第二属性信息和所述签名信息，并根据所述签名信息对所述第二属性信息进行验证。

7、如权利要求 1-3 任一项所述的支付安全性的检测方法，其特征在于，还包括：

15 记录接收到所述支付请求时的第一时间戳，并记录接收到所述第二属性信息时的第二时间戳；

如果所述第一时间戳和第二时间戳之间的时间小于第一预设阈值，或者，所述第一时间戳和第二时间戳之间的时间大于第二预设阈值，则判断为高危支付，其中，所述第二预设阈值大于所述第一预设阈值。

20

8、一种支付安全性的检测装置，其特征在于，包括：

第一接收模块，用于接收客户端发送的支付请求，并记录与所述支付请求相关的第一属性信息；

发送模块，用于向所述客户端发送安全代码；

采集模块，用于通过所述安全代码采集第二属性信息；

第二接收模块，用于接收所述客户端的商业订单提交请求，并记录与所述商业订单提交请求相关的第三属性信息；以及

5 检测模块，用于根据所述第一属性信息、第二属性信息和第三属性信息中的至少两个进行支付安全性检测。

9、如权利要求 8 所述的支付安全性的检测装置，其特征在于，其中，所述第一属性信息为所述客户端发送所述支付请求时的第一 IP 地址，所述第二属性信息为通过所述安全代码采集的所述客户端的第二 IP 地址，所述第三属性信息为所述客户端发送所述商业订单提交请求时的第三 IP 地址，其中，所述检测模块具体用于：

在所述第一 IP 地址、所述第二 IP 地址和所述第三 IP 地址中的任意两个不同时，判断为高危支付。

10、如权利要求 8 所述的支付安全性的检测装置，其特征在于，所述第一属性信息为通过所述支付请求获取的第一域名信息，所述第二属性信息为所述安全代码采集的第二域名信息，其中，所述检测模块具体用于：

在所述第一域名信息与所述第二域名信息不同时，判断为高危支付。

11、如权利要求 8-10 任一项所述的支付安全性的检测装置，其特征在于，还包括：

20 提取模块，用于提取所述支付请求中的 Refer 信息，其中，所述发送模块具体用于在所述 Refer 信息为空时将所述安全代码发送至所述客户端。

12、如权利要求 11 所述的支付安全性的检测装置，其特征在于，还包括：生成模块，用于通过混淆算法对所述安全代码进行混淆以生成混淆字符

串；

所述发送模块还用于将混淆之后的安全代码和所述混淆字符串发送至所述客户端。

13、如权利要求 12 所述的支付安全性的检测装置，其特征在于，所述采集模块包括：

接收单元，用于接收所述客户端发送的所述第二属性信息和所述签名信息，其中，所述客户端运行所述安全代码以使所述安全代码采集所述第二属性信息，所述客户端对所述第二属性信息和所述混淆字符串进行签名以生成签名信息；

10 验证单元，用于根据所述签名信息对所述第二属性信息进行验证。

14、如权利要求 8-10 任一项所述的支付安全性的检测装置，其特征在于，还包括：

记录模块，用于记录接收到所述支付请求时的第一时间戳，并记录接收到所述第二属性信息时的第二时间戳；其中，

15 所述检测模块还具有用于：

在所述第一时间戳和第二时间戳之间的时间小于第一预设阈值，或者，所述第一时间戳和第二时间戳之间的时间大于第二预设阈值时，判断为高危支付，其中，所述第二预设阈值大于所述第一预设阈值。

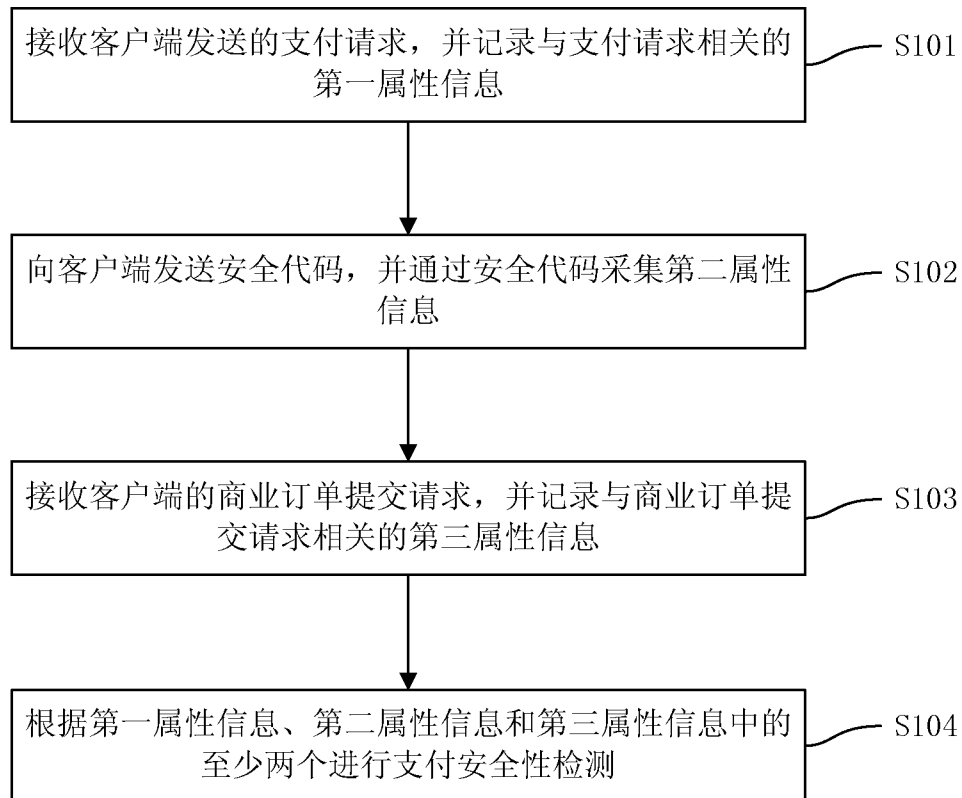


图 1

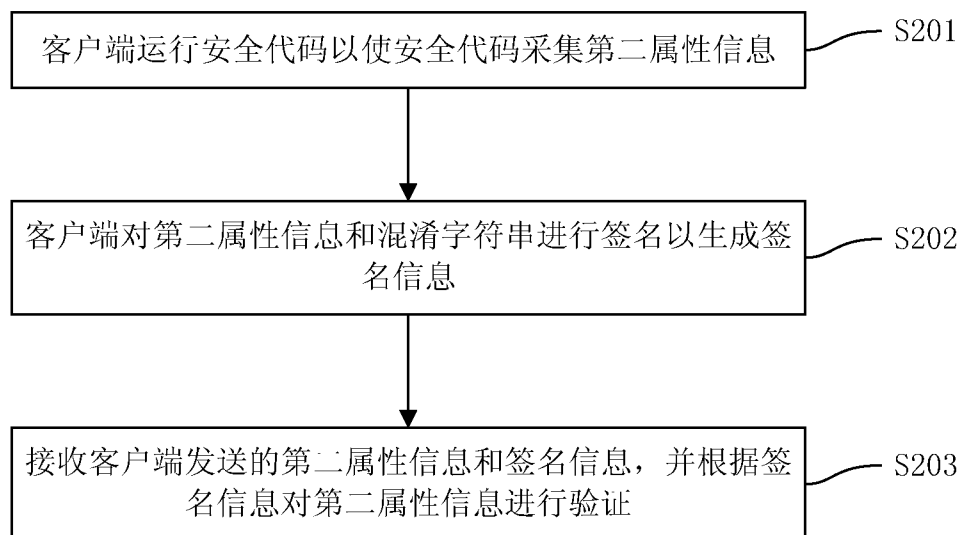


图 2

商户网站

支付平台

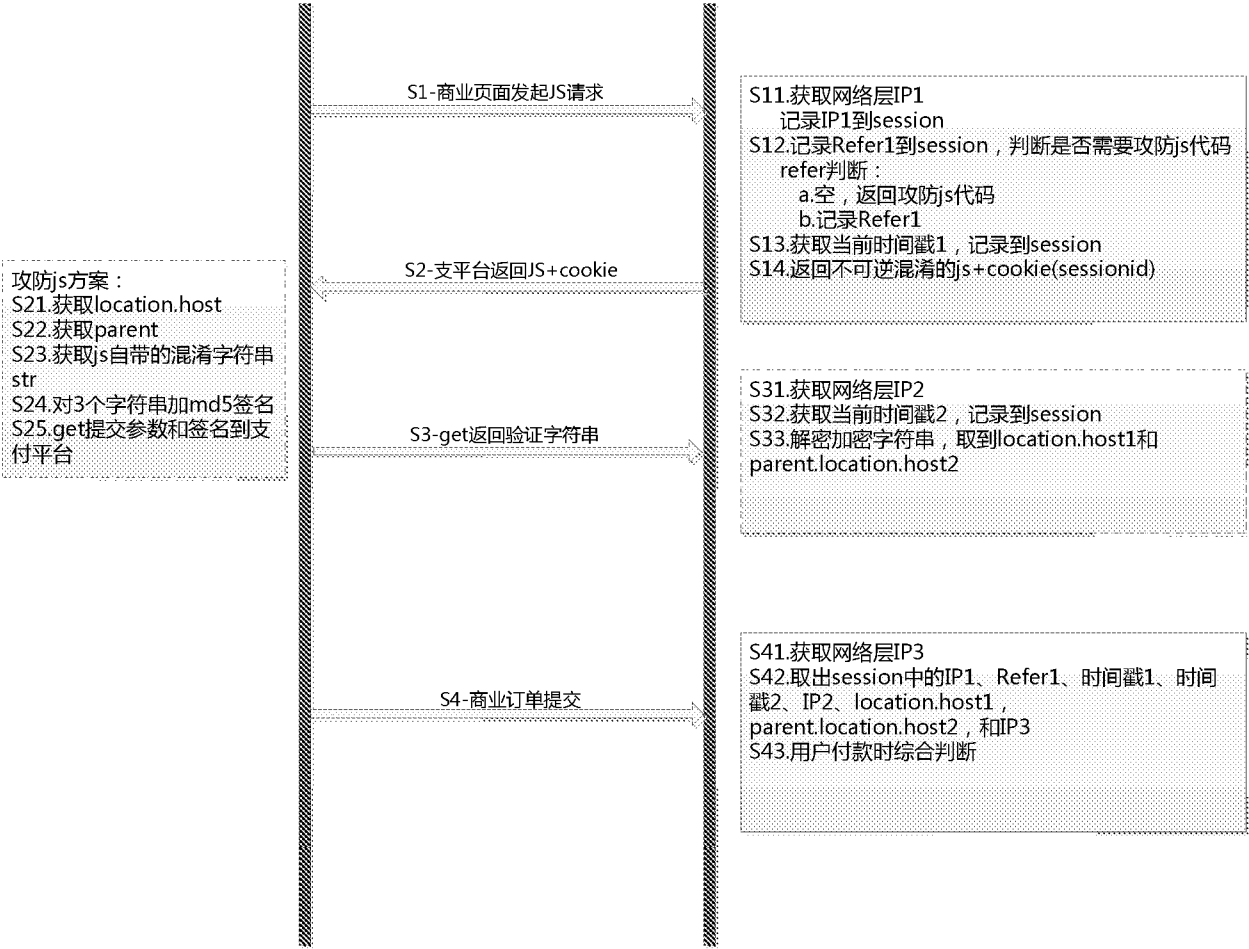


图 3

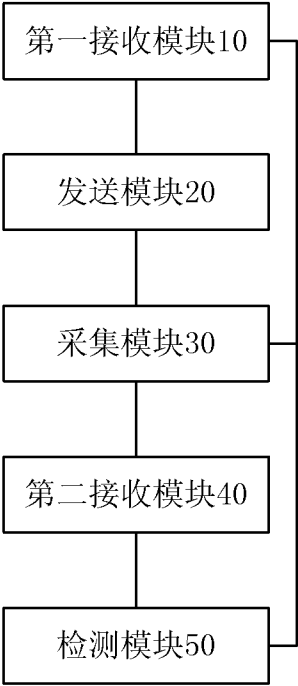


图 4

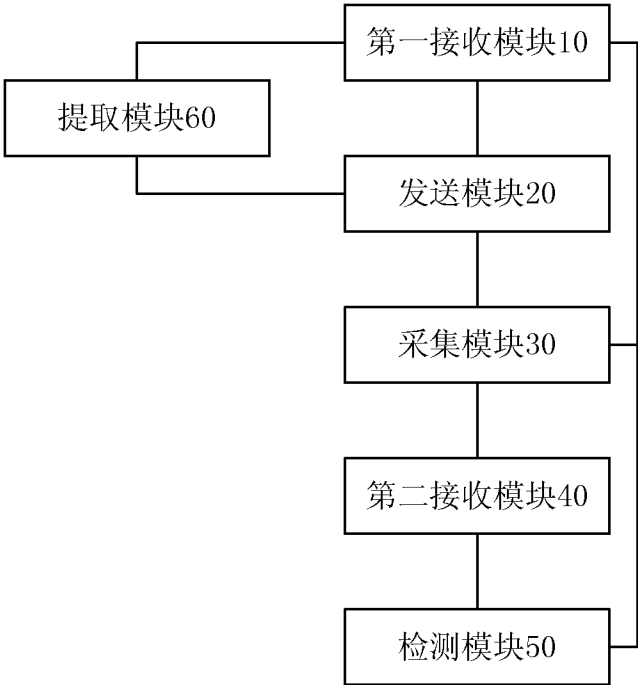


图 5

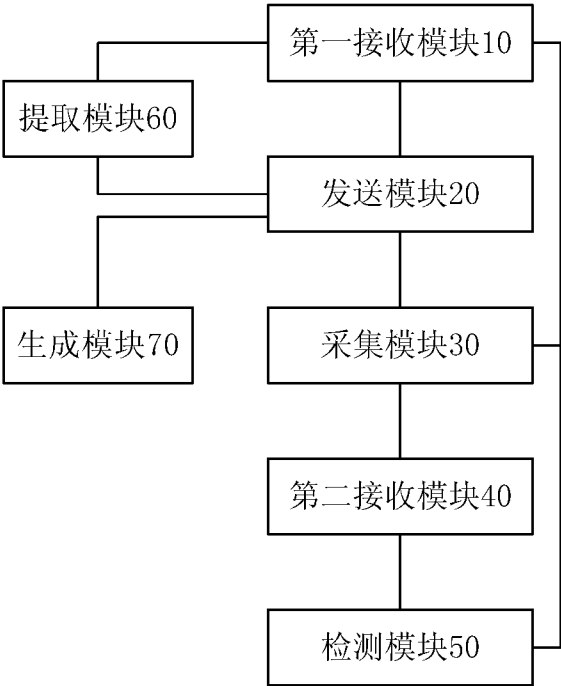


图 6

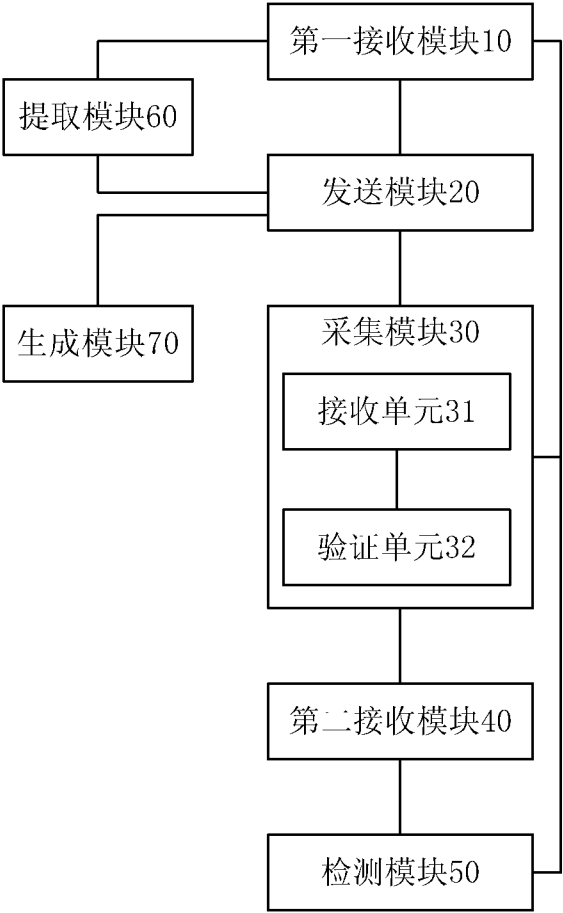


图 7

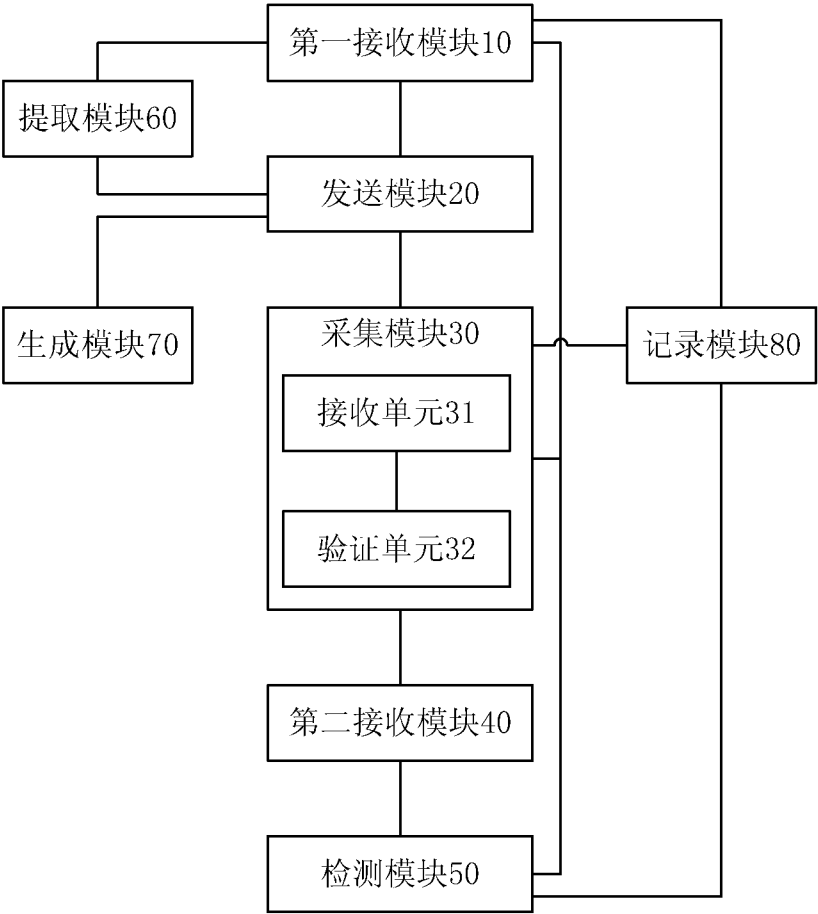


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/086618

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38 (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)

G06F, G06Q, H04L

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)

WPI, EPODOC, CNPAT, CNKI, IEEE: AVS, Address Verification Service, anti-phishing, phishing, IP address, address, online payment, payment, refer, referer, source of request, timestamp

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102073953 A (ALIBABA GROUP HOLDING LIMITED), 25 May 2011 (25.05.2011), description, paragraphs 35-118, and figures 2-3	1-14
X	CN 102096872 A (INDUSTRIAL AND COMMERCIAL BANK OF CHINA LIMITED), 15 June 2011 (15.06.2011), description, paragraphs 26-60	1-14
X	CN 102214334 A (ALIBABA GROUP HOLDING LTD.), 12 October 2011 (12.10.2011), description, paragraphs 99-155	1-14
A	CN 103745352 A (BEIJING SINODATA ELECTRONIC COMMERCE CO., LTD.), 23 April 2014 (23.04.2014), the whole document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 08 October 2015 (08.10.2015)	Date of mailing of the international search report 02 November 2015 (02.11.2015)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LIU, Xu Telephone No.: (86-10) 82245207

International application No.
PCT/CN2015/086618

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2015/086618

A. 主题的分类

G06Q 20/38(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)

G06F, G06Q, H04L

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))

WPI, EPODOC, CNPAT, CNKI, IEEE: AVS, Address Verification Service, 地址验证服务, 钓鱼, 反钓鱼, anti-phishing, phishing, IP address, IP地址, 地址, address, online payment, 在线支付, 支付, payment, refer, referer, 请求来源, 时间戳, timestamp

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 102073953 A (阿里巴巴集团控股有限公司) 2011年 5月 25日 (2011 - 05 - 25) 说明书第35-118段、附图2-3	1-14
X	CN 102096872 A (中国工商银行股份有限公司) 2011年 6月 15日 (2011 - 06 - 15) 说明书第26-60段	1-14
X	CN 102214334 A (阿里巴巴集团控股有限公司) 2011年 10月 12日 (2011 - 10 - 12) 说明书第99-155段	1-14
A	CN 103745352 A (北京中科金财电子商务有限公司) 2014年 4月 23日 (2014 - 04 - 23) 全文	1-14

☐ 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

2015年 10月 8日

国际检索报告邮寄日期

2015年 11月 2日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
北京市海淀区蓟门桥西土城路6号
100088 中国

传真号 (86-10)62019451

授权官员

刘栩

电话号码 (86-10)82245207

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/086618

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	102073953	A	2011年 5月 25日	HK	1153031	A0	2012年 3月 16日
CN	102096872	A	2011年 6月 15日	无			
CN	102214334	A	2011年 10月 12日	HK	1158794	A0	2012年 7月 20日
CN	103745352	A	2014年 4月 23日	无			