

支付安全管理的方法、装置和支付系统

技术领域

[01]本公开涉及区块链技术领域,具体涉及一种支付安全管理的方法、装置和支付系统。

背景技术

[02]在使用物联网机具进行支付时,无法得知物联网机具展示的结果页是否准确。

发明内容

[03]有鉴于此,本公开提供一种支付安全管理的方法、装置和支付系统。

[04]第一方面,提供一种支付安全管理的方法,应用于支付系统,所述支付系统包括物联网机具和服务端,所述物联网机具用于向所述服务端发送支付请求,所述服务端用于响应所述支付请求,所述方法包括:获取第一支付数据,其中,所述第一支付数据根据所述支付请求对应的清算数据生成;获取第二支付数据,其中,所述第二支付数据根据所述支付请求对应的结果页生成,所述结果页用于所述物联网机具向外展示;对所述第一支付数据和所述第二支付数据进行一致性对比,得到对比结果。

[05]可选地,在一些实施例中,所述服务端包括物联网机具服务端和支付服务端,所述清算数据包括所述物联网机具服务端的收单数据和/或所述支付服务端的结算数据。

[06]可选地,在一些实施例中,所述支付服务端包括统一支付。

[07]可选地,在一些实施例中,在所述得到对比结果之后,所述方法还包括:当所述对比结果为对比不一致时,保存所述对比结果。

[08]可选地,在一些实施例中,在所述得到对比结果之后,所述方法还包括:当所述对比结果为对比不一致时,拦截所述支付请求。

[09]可选地,在一些实施例中,所述第一支付数据和所述第二支付数据包括所述支付请求对应的信息流数据和/或资金流数据。

[10]第二方面,提供一种支付安全管理的装置,应用于支付系统,所述支付系统包括物联网机具和服务端,所述物联网机具用于向所述服务端发送支付请求,所述服务端用于响应所述支付请求,所述装置包括:第一获取单元,用于获取第一支付数据,其中,所

述第一支付数据根据所述支付请求的清算数据生成；第二获取单元，用于获取第二支付数据，其中，所述第二支付数据根据所述支付请求的结果页生成，所述结果页用于所述物联网机具向外展示；对比单元，用于对所述第一支付数据和所述第二支付数据进行一致性对比，得到对比结果。

[11]可选地，在一些实施例中，所述服务端包括物联网机具服务端和支付服务端，所述清算数据包括所述物联网机具服务端的收单数据和/或所述支付服务端的结算数据。

[12]可选地，在一些实施例中，所述支付服务端包括统一支付。

[13]可选地，在一些实施例中，所述装置还包括：保存单元，用于在所述得到对比结果之后，当所述对比结果为对比不一致时，保存所述对比结果。

[14]可选地，在一些实施例中，所述装置还包括：拦截单元，用于在所述得到对比结果之后，当所述对比结果为对比不一致时，拦截所述支付请求。

[15]可选地，在一些实施例中，所述第一支付数据和所述第二支付数据包括所述支付请求对应的信息流和/或资金流。

[16]第三方面，提供一种支付系统，包括：物联网机具，用于向服务端发送支付请求；服务端，用于处理所述支付请求，生成支付结果数据；平台，用于执行以下操作：获取第一支付数据，其中，所述第一支付数据根据所述支付请求的清算数据生成；获取第二支付数据，其中，所述第二支付数据根据所述支付请求对应的结果页生成，所述结果页用于所述物联网机具向外展示；对所述第一支付数据和所述第二支付数据进行一致性对比，得到对比结果。

[17]第四方面，提供一种支付安全管理的装置，包括：存储器，用于存储指令；处理器，用于执行所述存储器中存储的指令，以执行如第一方面所述的方法。

[18]第五方面，提供一种计算机可读存储介质，其上存储有可执行代码，当所述可执行代码被执行时，能够实现如第一方面所述的方法。

[19]第六方面，提供一种计算机程序产品，包括可执行代码，当所述可执行代码被执行时，能够实现如第一方面所述的方法。

[20]本公开实施例提供的支付安全管理的方法，通过对支付请求的清算结果和物联网机具用于向外展示的支付结果进行对比，能够自动化地监控每一笔支付在物联网机具端展示的结果页是否准确。

附图说明

[21]图 1 是相关技术中支付系统的支付流程示意图。

[22]图 2 是本公开一实施例提供的支付安全管理方法的流程示意图。

[23]图 3 是本公开又一实施例提供的支付安全管理方法的流程示意图。

[24]图 4 是本公开一实施例提供的支付安全管理装置的结构示意图。

[25]图 5 是本公开一实施例提供的支付系统的示意图。

[26]图 6 是本公开又一实施例提供的支付安全管理装置的结构示意图。

具体实施方式

[27]下面对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本公开一部分实施例，而不是全部的实施例。

[28]随着物联网技术的快速发展，依托于物联网技术的物联网机具发展迅猛。通过物联网机具进行支付的笔数日均超千万。

[29]图 1 是相关技术中支付系统的支付流程示意图。图 1 所示的支付系统可以包括物联网机具 110 和服务端 120。

[30]物联网机具 110 可以用于提供支付通道。用户可以通过物联网机具 110 提供的支付通道进行支付操作。物联网机具 110 也可以称为物联网设备、iot 设备、支付设备、设备、iot 机具、支付机具、机具、支付终端等。

[31]如图 1 所示，在步骤 S101，物联网机具 110 向服务端 120 发送支付请求。该支付请求例如可以指用户的付款请求。

[32]物联网机具 110 可以向用户提供刷脸、刷二维码等支付方式。用户可以通过被物联网机具 110 扫描面部特征或二维码的方式完成支付操作。

[33]物联网机具 110 获取用户的支付消息后，可以根据该支付消息向服务端 120 发送支付请求。

[34]在步骤 S102，服务端 120 处理支付请求。服务端 120 处理支付请求可以包括分析该支付请求。根据该支付请求完成资金的流转。例如，服务端 120 可以根据支付请求，从

用户 A 的支付宝账户中扣除 10 元，并在商户 B 的支付宝账户中增加 10 元。

[35]应理解，实际中用户或商户使用的账户可以是任意的账户。例如，用户 A 的账户可以是支付宝提供的余额宝，也可以是银行（例如建行）提供的银行卡账户。

[36]在步骤 S103，服务端 120 根据对支付请求的处理结果，向物联网机具 110 发送结果页。结果页也可以称为结果页数据。结果页中可以包括物联网机具展示时所需的数据。

[37]在步骤 S104，物联网机具 110 可以展示结果页。

[38]物联网机具 110 可以通过多种方式展示结果页，本公开对结果页的具体展示方式不做限定。例如，结果页可以通过一个页面的形式向用户展示。又如，结果页可以指通过语音播报的方式向用户展示。

[39]服务端 120 发送的结果页中可以包括信息流和资金流相关的信息。例如，服务端 120 发送的结果页中可以包括用户 id、交易号、支付渠道、支付状态、支付金额等。

[40]物联网机具 110 可以通过多种方式获取待展示的结果页所需要的数据。例如，待展示的结果页所需要的数据可以全部由服务端 120 计算并传输给物联网机具 110。

[41]又如，待展示的结果页所需的数据可以由服务端 120 和物联网机具 110 共同生成。例如，可以由物联网机具 110 完成部分生成结果页所需数据的计算，由服务端 120 完成另外部分生成结果页所需数据的计算。物联网机具 110 汇总展示所需的数据，生成结果页，并将结果页向外展示。

[42]根据前文中的流程介绍可知，一次支付请求需要至少经过物联网机具 110 以及服务端 120 的处理。通常物联网机具 110 和服务端 120 位于不同的地理位置，需要通过有线或无线通信的方式传递信息。

[43]在传递信息的过程中可能由于各种原因，导致传递的信息与原信息出现偏差。例如，可能由于网络问题导致物联网机具 110 展示的结果页中的数据与实际服务端存储的数据不一致。

[44]又如，信息在传递过程中可能被篡改，导致最终展示给用户的结果页的信息，与实际支付信息不一致。例如，用户完成了一笔 20 元钱的付款，付款渠道是刷脸支付。然而，由于支付过程中信息被篡改，导致物联网机具 110 中显示的支付结果为用户支付 200 元钱，付款渠道是刷二维码支付。即，用户支付后，物联网机具 110 中展示支付渠道和金额和最终所支付的不一致。

[45]又如，服务端 120 使用的结算单位和物联网机具 110 使用的结算单位可能不同，导致最终物联网机具 110 显示的金额出现差异。例如，在用户支付后，商家在结果页中向用户发放可供下次消费使用的 10 分钱的优惠券。然而，在物联网机具 110 中将 10 分钱的优惠券展示成了 10 元钱。

[46]即，对于支付数量巨大的基于物联网的支付系统（例如，刷脸支付的笔数日均超千万），物联网机具 110 向外展示的支付结果可能与服务端 120 下发或存证的支付数据不一致。

[47]当结果页展示的数据与实际的支付数据不一致时，可能使得用户或商家的资金受损。严重时，可能导致公司名誉受损。

[48]通常，服务端提供的数据具有可靠性。因此，只需保证物联网机具端用于展示的结果页相关的数据正确，即可保证物联网机具提供的支付结果与用户实际的支付结果一致。即，可以保证用户所见即所得。

[49]为了保证用户所见即所得，通常需要将物联网机具端的结果页数据与服务端的数据进行对比。如果对比结果存在不一致，则说明该支付请求在执行的过程中存在问题。即，用户所见与最终的支付结果可能不同。

[50]相关技术提供的支付核对的方法，通常通过拉取存储系统中存证的数据的方式进行一致性对比。

[51]然而，由于物联网机具端的流水（例如支付请求数量）巨大，而且物联网机具端的流水信息没有存证的必要，因此，物联网机具端通常并不配置存储系统（例如数据库）。

[52]没有存储系统的物联网机具，无法使用通用的自动化核对方式进行数据正确性核对。因此，使用物联网机具的支付系统，目前仍然通过人工对账的方式确保支付的正确性。

[53]人工对账可以通过多种形式完成。例如，商户主动向物联网机具的提供商申请账单，由商户人工进行账单核对。

[54]又如，由于使用物联网机具的商户很多，物联网机具的提供商通常与 isv 机构合作，由 isv 机构向商户提供物联网机具，并管理使用物联网机具的商户。商户可以向 isv 机构申请对账，isv 机构可以收集商户的对账信息，并向 isv 机构提供账单。

[55]上述两种对账方式，本质上都是通过人工完成对账。可以理解，使用人工对账的方式，对账效率低，人工需求量大，成本高。

[56]此外,由于物联网支付系统的支付量极大,联网机具的类型众多,覆盖面广。因此,要通过人工的方式监控每一笔通过物联网支付系统的支付请求难以实现。

[57]综上可知,对于使用物联网机具的支付系统,如何有效地监控每一笔支付的正确性是目前面临的难点。

[58]为了解决上述问题,本公开提供了一种支付安全管理的方法,能够高效地监控每一笔支付的正确性,从而提高支付系统的安全性。

[59]下面结合附图 2,对本公开实施例提供的支付安全管理的方法进行详细描述。

[60]图 2 是本公开一实施例提供的支付安全管理方法的流程示意图。图 2 所示的支付安全管理的方法可以应用于支付系统。支付系统可以指用于支付的系统。资金可以通过支付系统完成流转。

[61]例如,用户向商户购买一件价值 10 元的商品。用户可以通过支付系统向商户付款。支付系统可以处理该笔交易,从用户的账户中扣除 10 元,并在商户的账户中增加 10 元。

[62]支付系统可以包括物联网机具和服务端。物联网机具可以向外提供支付通道。例如,物联网机具可以接受用户的支付请求。又如,物联网机具可以向服务端发送支付请求。又如,物联网机具可以从服务端接收支付请求对应的支付结果。

[63]服务端可以指用于与物联网机具交互,以完成支付处理的服务装置。服务端可以用于响应物联网机具发送的支付请求。响应物联网机具发送的支付请求可以包括根据支付请求中的信息,完成资金的流转。

[64]本公开对服务端的具体实现形式不做限定。例如,服务端可以包括能够向外提供服务的服务器或计算机。

[65]参见图 2,在步骤 S210,获取第一支付数据。第一支付数据可以根据支付请求对应的清算数据生成。

[66]可以通过多种方式获取第一支付数据。例如,可以主动向服务端发起获取请求。服务端在接收到该获取请求后,提供第一支付数据。

[67]又如,可以直接从服务端获取第一支付数据。直接获取例如可以通过在服务端埋点的方式实现。在服务端中埋点可以通过多种方式实现。例如,可以通过在服务端中设置 sdk 实现。

[68]第一支付数据可以通过多种方式根据支付请求对应的清算数据生成。例如，可以直接将支付请求对应的清算数据作为第一支付数据。

[69]又如，可以获取支付请求的清算数据中的部分数据作为第一支付数据。部分数据例如可以包括与资金要素相关的数据。资金要素例如可以包括用户 id、支付金额、支付状态等与资金相关的数据。

[70]清算数据可以由支付系统的服务端生成。清算数据可以包括支付请求相关的信息流数据，和/或资金流数据。

[71]信息流也可以称为数据流。信息流数据例如可以包括物联网机具相关的数据（例如物联网机具的 sn 码、mac 码等）、用户的支付方式（例如刷脸支付、二维码支付等）等。资金流数据例如可以包括用户 id、交易号、支付渠道、支付状态、支付金额等。

[72]在一些实施例中，服务端可以存储清算数据。服务端可以通过多种方式存储清算数据。例如，服务端可以将清算数据以单据的形式存储。

[73]在一些实施例中，服务端可以与存储系统相连。清算数据可以以单据的形式存储在存储系统中。存储系统例如可以指数据库。

[74]在步骤 S220，获取第二支付数据。第二支付数据可以根据支付请求对应的结果页生成。结果页用于物联网机具向外展示。

[75]可以通过多种方式获取第二支付数据。例如，可以直接从服务端获取第二支付数据。

[76]又如，可以由物联网机具在接收到支付结果后，以主动上报的方式上报第二支付数据。

[77]又如，可以直接从物联网机具截取第二支付数据。截取方式例如可以在物联网机具中埋点。在物联网机具中埋点例如可以通过在物联网机具中设置相应的 sdk 实现。

[78]结果页可以用于物联网机具向外展示。应理解，使用结果页描述向用户展示支付结果的页面仅为了使描述更加清楚。结果页例如可以指结果页相关的数据，也可以指一个可以在显示屏上显示的页面，或通过其他形式展示的展示信息（例如语音播报信息）。

[79]例如，对于具有显示屏的物联网机具（例如蜻蜓机具），结果页可以指展示在物联网机具的显示屏上的支付结果。又如，对于具有放音模块的物联网机具（例如小白盒机具），结果页也可以指物联网机具的语音播报结果。

[80]结果页显示的内容可以根据实际的需求任意设置，本公开对结果页具体显示的内容不做限定。例如，结果页可以向用户展示支付金额、用户 id、支付状态（例如支付成功或支付失败）等。

[81]在一些实施例中，结果页中还可以包括商户投放的广告。商户投放的广告可以包括任意类型的广告。例如，商户投放的广告可以包括商场促销信息、餐饮店打折信息等。又如，商户投放的广告可以包括下一次消费时可以使用的代金券。

[82]可以通过多种方式根据支付请求对应的结果页生成第二支付数据。例如，可以直接将支付请求对应的结果页作为第二支付数据。

[83]又如，可以将支付请求对应的结果页中的部分数据作为第二支付数据。结果页中的部分数据例如可以包括资金要素相关的数据。资金要素相关的数据例如可以包括用户 id、支付金额、支付状态等。

[84]在步骤 S230，对第一支付数据和第二支付数据进行一致性对比，得到对比结果。

[85]第一支付数据和第二支付数据可以包括相同的数据。例如，第一支付数据和第二支付数据可以都包括资金流数据和/或信息流数据。

[86]资金流数据例如可以包括用户 id、交易号、支付渠道、支付状态、金额等。信息流数据例如可以包括物联网机具相关的数据（例如物联网机具的 sn 码、mac 码等）、用户的支付方式（例如刷脸支付、二维码支付等）等。

[87]一致性对比可以指，对第一支付数据包含的数据项和第二支付数据包含的数据项进行一一对比，确认数据是否完全相同。

[88]例如，第一支付数据和第二支付数据可以包括用户 id、交易号、支付金额、支付方式、支付状态、物联网设备的设备码等信息。

[89]将第一支付数据和第二支付数据中的上述数据项一一进行对比。例如，对比用户 id 是相同、交易号是否相同、支付金额是否相同等等。

[90]只要对比的所有数据项中有任何一个数据项不相同，即认为第一支付数据和第二支付数据对比不一致。

[91]第一支付数据和第二支付数据对比不一致，表示服务端存储的清算数据，与物联网机具向外展示的结果页中的数据不一致。

[92]通过在支付系统中增加数据对比机制，可以监控使用物联网机具的支付系统中的每一笔支付请求。进一步地，本公开提供的方法，可以及时发现物联网机具展示的结果页存在错误的支付请求。通过自动化的方式监控支付系统中每一笔支付的正确性。

[93]对比结果不一致，通常表明支付系统存在漏洞。因此，为了提高支付系统的健壮性，可以在对比结果不一致时，对对比结果进行进一步地处理。

[94]例如，当对比结果为对比不一致时，可以保存该对比不一致的对比结果。对比结果可以以日志的形式呈现。因此，保存对比结果也可以指保存对比过程中生成的对比日志。

[95]保存对比结果可以通过多种方式实现。例如，可以将对比结果存储于存储空间（例如计算机或服务器的硬盘）中。又如，可以将对比结果打印出来。

[96]通过将对比不一致的结果保存的方式，可以帮助软件从业人员（例如软件开发或运维人员）定位系统中存在的问题，提升处理问题的效率。

[97]又如，当对比结果不一致时，可以为对比不一致的场景配置告警信息。当某个支付请求对应的场景与配置告警信息的场景一致时，可以发送该告警信息。

[98]例如，物联网机具展示结果页时使用的单位为元，而服务端保存结算数据时使用的单位为分。如果支付系统存在逻辑问题，可能导致物联网机具展示的结果页存在错误。例如，本应展示 0.1 元（服务端存储的单位为分，即，服务端存储的数据为 10 分，应展示为 0.1 元），结果展示成了 10 元。

[99]可以为该场景配置告警信息。当再次遇到单位换算错误的场景，可以触发配置好的告警信息。

[100] 软件从业人员可以根据保存的对比结果或配置的告警信息对支付系统进行排查。修复支付系统中存在的漏洞，提高系统的健壮性，提高支付过程的安全性。

[101] 在一些实施例中，为了进一步提升支付系统的安全性，可以在对比结果不一致时，拦截该支付。通过实时拦截存在错误的支付请求，可以保证用户的资金安全。

[102] 由于存在问题的支付请求被拦截，保证了用户在物联网机具上获得的结果页与实际的支付信息一致。即，保证用户所见即所得。

[103] 在一些实施例中，可以使用上述方法的结合。例如，可以当对比结果不一致时，对对比结果不一致的对比结果进行打印。当对比结果不一致对应的场景为严重场景时，对该对比结果对应的支付请求进行拦截。当对比结果不一致的场景为不严重的场景时，

可以仅为该结果配置告警信息，不对支付请求进行拦截。

[104] 场景是否为严重场景可以根据实际的业务需要设置。例如，严重的场景可以包括结果页待展示的支付结果数据中对应的支付金额，与服务端清算数据中对应的支付金额完全不同的场景。

[105] 本公开提供的方法，可以自动对比支付请求对应的结果页与服务端的清算数据（例如收单数据）是否一致。如出现不一致，可以对出现不一致的支付请求进行报警或拦截。因此，本公开提供的方法实现了自动巡检、秒级告警。

[106] 在一些实施例中，服务端可以包括多个不同的服务端。不同的服务端可以由不同的运营商提供。不同的服务端可以用于处理支付过程中不同的操作。

[107] 在一些实施例中，服务端可以包括物联网机具服务端和支付服务端。应理解，服务端除了物联网机具服务端和支付服务端外，还可以包括其他用于提供服务的服务端。本公开对服务端具体包含的服务端的类型和数量不做限定。

[108] 每个服务端可以通过多种方式实现。例如，服务端可以通过服务器向外提供服务。每个服务端可以包括任意数量的服务器。本公开对服务端的具体实现形式或服务端包含的服务器数量不做限定。

[109] 支付服务端可以用于根据支付请求进行结算。例如，支付服务端可以完成支付清算扣款。又如，支付服务端可以生成清算单据。

[110] 在一些实施例中，支付服务端可以与存储系统相连。存储系统可以包括数据库。支付服务端可以将相关数据存储在存储系统中。相关数据例如可以包括支付清算扣款信息或清算单据。支付清算扣款信息或清算单据例如可以包括用户的账户信息、支付的结算信息等。

[111] 在一些实施例中，支付服务端可以包括统一支付。统一支付可以指建立在支付核心软件之上的支付服务系统。统一支付可以实现全面的业务管理、用户管理、账务方管理、付费方管理等功能。统一支付可以为多种业务系统提供安全高效的支付支持环境。

[112] 统一支付的目的是，建立一个支付方(银行、其他支付系统)和账务方(全业务运营支撑系统)的用于支付充值的系统。

[113] 物联网机具服务端可以用于接收物联网机具发送的支付请求，并将支付请求向支付服务端转发。

[114] 在接收到支付结果后，物联网机具服务端可以对支付结果进行处理，生成用于物联网机具的结果页。用户可以根据物联网机具展示的结果查看支付结果。用户可以指向商户付款的消费者，也可以指使用物联网机具作为收款工具的商户。

[115] 在一些实施例中，物联网机具服务端可以根据支付请求生成收单数据。收单数据可以包括支付请求对应的用户 id、交易号、支付渠道、支付状态等。

[116] 在一些实施例中，清算数据可以包括物联网机具服务端的收单数据和/或支付服务端的结算数据。第一支付数据可以根据清算数据生成。

[117] 第一支付数据可以包括支付服务端的结算数据。由于支付服务端的结算数据通常是正确的，因此通过将第二支付数据与包括支付服务端的结算数据进行一致性对比，可以快速确认用户物联网机具生成向外展示的结果页的支付结果数据是否正确。

[118] 第一支付数据还可以包括支付服务端的结算数据和物联网机具服务端的收单数据。在一些实施例中，支付服务端的结算数据可以称为结算数据，物联网机具服务端的收单数据可以称收单数据。第一支付数据可以包括结算数据和收单数据。

[119] 对第一支付数据和第二支付数据进行一致性对比，可以包括对结算数据和第二支付数据进行一致性对比，以及对收单数据和结算数据进行一致性对比。

[120] 通过对多端存储的数据进行一致性对比，可以进一步保证最终的支付结果数据的准确性。

[121] 由于数据在传输的过程中，可能在任意一个节点出现问题，造成最终的支付结果出现错误。因此，对多端数据进行一致性对比，可以帮助开发人员快速定位出现问题的节点，提升运维效率。

[122] 本公开提供的方法可以部署在支付系统的任意一个节点上。例如，本方案可以部署在物联网机具上。本方案部署在物联网机具上，可以实现实时的一致性对比。当对比不一致时，可以及时拦截对不一致的支付请求，保障用户的资金安全。

[123] 又如，本方案可以部署在服务端。具体地，本方案可以部署在物联网机具服务端上。通过将本方案部署在服务端，可以从源头保证数据的一致性。

[124] 在一些实施例中，也可以在物联网机具端和服务端都部署该方案。从而进一步确保最终展现给用户的结果页与服务端存储的支付数据一致。即，进一步确保用户的资金安全。

[125] 在一些实施例中，该方案也可以独立地部署在核对平台上。通过核对平台对支付过程进行监控，保证用户所见即所得。

[126] 核对平台可以独立与支付系统。因此，通过在支付系统中部署核对平台的方式，可以不对支付系统进行侵入，实现简单，维护方便。

[127] 核对平台可以实时地对每一笔交易进行监控。为了提高核对平台的处理效率，也可以每隔固定的时间，对该时间间隔内的所有交易进行统一的比对和处理。这种间隔固定时间进行处理的方式，也可以称为自动巡检。巡检的间隔时间可以根据需要任意选择。例如，可以选择每 3 分钟巡检一次。

[128] 图 3 是本公开又一实施例提供的支付安全管理方法的流程示意图。如图 3 所示，该支付安全管理方法的流程包括步骤 S301 至步骤 S312。

[129] 在步骤 S301，用户通过物联网机具支付。物联网机具也可以简称为机具。

[130] 物联网机具可以提供各种供用户支付的通道。例如，物联网机具可以向用户提供刷脸或刷二维码的通道。

[131] 用户可以通过刷脸或刷二维码的形式支付。例如，用户可以通过刷脸的方式向物联网机具提交支付请求。支付请求可以包括向商户支付 10 元。

[132] 在步骤 S302，物联网机具发送给服务端处理支付。物联网机具可以通过物联网与服务端通信，并将支付请求发送给服务端。

[133] 在步骤 S303，服务端可以处理支付请求，并根据处理结果生成结果页所需的数据。在本实施例中，结果页由服务端独立构建。实际中，结果页可以由服务端构建，也可以由物联网机具构建，还可以由物联网机具和服务端共同构建。本公开对结果页的具体构建方式不做限定。

[134] 物联网机具在构建结果页时通常使用两套方案：主动轮询和统一支付发送消息给设备服务端。

[135] 主动轮询包括物联网机具主动向设备服务端索取构建结果页所需的数据。统一支付处理完支付请求后，也会主动向物联网机具服务端发送数据。物联网机具服务端在接收到该数据后，将主动将数据发送给物联网机具。

[136] 在构建结果页时，通常根据上述两套方案中首先达到的消息构建。本实施例在获取结果页数据时，可以通过在物联网机具端埋点的方式，获取首先达到物联网机具端

的结果页数据，并根据结果页数据获取第二支付数据。

[137] 在步骤 S304，判断支付是否成功。

[138] 当支付失败时，进入步骤 S305，服务端构建支付失败的信息。当支付成功时，进入步骤 S306，服务端构建支付成功的信息。

[139] 在步骤 S307，获取收单的信息流要素。

[140] 在步骤 S308，获取统一支付的资金流要素。

[141] 收单的信息流和统一支付的资金流可以由同一个服务端提供，也可以由不同的服务端提供。通常，收单的信息流和统一支付的资金流由不同的服务端提供。收单的信息流要素和统一支付的资金流要素可以统一生成第一支付数据。

[142] 在步骤 S309，比较重要资金流/信息流要素。

[143] 由于服务端之间在进行通信的过程中也可能存在问题。例如，服务端之间在进行通信的过程中，支付数据可能被篡改。又如，服务端之间的数据存储或构建逻辑可能存在差异，导致最终存储的数据存在差异。

[144] 因此，通过将第一支付数据数据和第二支付数据进行一致性对比，即，将结果页数据、收单的信息流要素以及统一支付的资金流要素进行对比，可以及时发现结果页显示的重要数据是否正确。重要数据例如可以包括终要的资金流要素和信息流要素。

[145] 资金流要素例如可以包括用户 id、交易号、支付渠道、支付状态、支付金额等。信息流要素例如可以包括支付方式（例如刷脸支付）、物联网机具的设备信息（例如设备 sn 码、设备 mac 码等）等。

[146] 在步骤 S310，确认对比结果。

[147] 当对比失败后，进入步骤 S311，告警和/或应急。告警可以包括配置告警信息，以供下次出现相同场景时向开发人员告警。告警还可以包括向开发人员提供告警信息，以供开发人员根据日志以及告警信息进行排查，确定并解决系统中可能存在的安全漏洞。

[148] 当对比成功后，进入步骤 S312，结束。

[149] 前文结合图 1 至图 3 详细介绍了本公开提供的方法实施例。下文结合图 4 至图 6 介绍本公开提供的装置实施例。应理解，装置实施例和方法实施例相互对应。因此，装置实施例未详尽介绍之处，请参考方法实施例部分的描述。

[150] 图 4 是本公开一实施例提供的支付安全管理装置的结构示意图。装置 400 可以应用于支付系统。支付系统可以包括物联网机具和服务端。物联网机具可以用于向服务端发送支付请求。服务端可以用于响应支付请求。

[151] 装置 400 可以包括第一获取单元 410、第二获取单元 420 以及对比单元 430。

[152] 第一获取单元 410 可以用于获取第一支付数据。第一支付数据可以根据支付请求随影的清算数据生成。

[153] 第二获取单元 420 可以用于获取第二支付数据。第二支付数据可以根据支付请求对应的结果页生成。结果页可以用于生成用户物联网机具向外展示。

[154] 对比单元 430 可以用于对第一支付数据和第二支付数据进行一致性对比。

[155] 可选地，在一些实施例中，服务端可以包括物联网机具服务端和支付服务端。清算数据可以包括物联网机具服务端的收单数据和/或支付服务端的结算数据。

[156] 可选地，在一些实施例中，支付服务端可以包括统一支付。

[157] 可选地，在一些实施例中，装置 400 还可以包括保存单元。保存单元可以用于在得到对比结果后，当对比结果为对比不一致时，保存对比结果。

[158] 可选地，在一些实施例中，装置 400 还可以包括拦截单元。拦截单元可以用于在得到对比结果后，当对比结果为对比不一致时，拦截支付请求。

[159] 可选地，在一些实施例中，第一支付数据和第二支付数据可以包括支付请求对应的信息流和/或资金流。

[160] 图 5 是本公开一实施例提供的支付系统的示意图。如图 5 所示，支付系统可以包括物联网机具 510、服务端 520 和平台 530。

[161] 物联网机具 510 可以用于向服务端发送支付请求。

[162] 服务端 520 可以用于处理支付请求，生成支付结果数据。

[163] 平台 530 可以用于执行以下操作：获取第一支付数据，其中，所述第一支付数据根据所述支付请求对应的清算数据生成；获取第二支付数据，其中，所述第二支付数据根据所述支付请求对应的结果页生成，所述结果页用于所述物联网机具向外展示；对所述第一支付数据和所述第二支付数据进行一致性对比，得到对比结果。

[164] 平台 530 可以指由硬件实现，也可以由软件实现，本公开对平台 530 的具体实

现形式不做限定。

[165] 平台 530 可以独立于物联网机具 510 和服务端 520。在一些实施例中，平台 530 也可以部署在物联网机具 510 上和/或服务端 520 上。本公开对平台 530 的部署位置不做限定。

[166] 图 6 是本公开又一实施例提供的支付安全管理装置的结构示意图。图 6 所示的装置 600 可以是能够执行本公开提供的支付安全管理方法的平台。该装置 600 例如可以是具有计算功能的计算设备。比如，装置 600 可以是移动终端或者服务器。装置 600 可以包括存储器 610 和处理器 620。存储器 610 可用于存储可执行代码。处理器 620 可用于执行所述存储器 610 中存储的可执行代码，以实现前文描述的各个方法中的步骤。在一些实施例中，该装置 600 还可以包括网络接口 630，处理器 620 与外部设备的数据交换可以通过该网络接口 630 实现。

[167] 在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其他任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本公开实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（Digital Subscriber Line, DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如数字视频光盘（Digital Video Disc, DVD））、或者半导体介质（例如固态硬盘（Solid State Disk, SSD））等。

[168] 本领域普通技术人员可以意识到，结合本公开实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本公开的范围。

[169] 在本公开所提供的几个实施例中，应该理解到，所揭露的系统、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例仅仅是示意性的，例如，所述单元的划分，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，例如多个单元或组件可以结合或者可以集成到另一个系统，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，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[170] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[171] 另外，在本公开各个实施例中的各功能单元可以集成在一个处理单元中，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单元中。

[172] 以上所述，仅为本公开的具体实施方式，但本公开的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本公开揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本公开的保护范围之内。因此，本公开的保护范围应以所述权利要求的保护范围为准。

权利要求书

1、一种支付安全管理的方法，应用于支付系统，所述支付系统包括物联网机具和服务端，所述物联网机具用于向所述服务端发送支付请求，所述服务端用于响应所述支付请求，所述方法包括：

获取第一支付数据，其中，所述第一支付数据根据所述支付请求对应的清算数据生成；

获取第二支付数据，其中，所述第二支付数据根据所述支付请求对应的结果页生成，所述结果页用于所述物联网机具向外展示；

对所述第一支付数据和所述第二支付数据进行一致性对比，得到对比结果。

2、根据权利要求1所述的方法，所述服务端包括物联网机具服务端和支付服务端，所述清算数据包括所述物联网机具服务端的收单数据和/或所述支付服务端的结算数据。

3、根据权利要求2所述的方法，所述支付服务端包括统一支付。

4、根据权利要求1所述的方法，在所述得到对比结果之后，所述方法还包括：

当所述对比结果为对比不一致时，保存所述对比结果。

5、根据权利要求1所述的方法，在所述得到对比结果之后，所述方法还包括：

当所述对比结果为对比不一致时，拦截所述支付请求。

6、根据权利要求1所述的方法，所述第一支付数据和所述第二支付数据包括所述支付请求对应的信息流数据和/或资金流数据。

7、一种支付安全管理的装置，应用于支付系统，所述支付系统包括物联网机具和服务端，所述物联网机具用于向所述服务端发送支付请求，所述服务端用于响应所述支付请求，所述装置包括：

第一获取单元，用于获取第一支付数据，其中，所述第一支付数据根据所述支付请求对应的清算数据生成；

第二获取单元，用于获取第二支付数据，其中，所述第二支付数据根据所述支付请求对应的结果页生成，所述结果页用于所述物联网机具向外展示；

对比单元，用于对所述第一支付数据和所述第二支付数据进行一致性对比，得到对比结果。

8、根据权利要求7所述的装置，所述服务端包括物联网机具服务端和支付服务端，所述清算数据包括所述物联网机具服务端的收单数据和/或所述支付服务端的结算数据。

9、根据权利要求8所述的装置，所述支付服务端包括统一支付。

10、根据权利要求 7 所述的装置，还包括：

保存单元，用于在所述得到对比结果之后，当所述对比结果为对比不一致时，保存所述对比结果。

11、根据权利要求 7 所述的装置，还包括：

拦截单元，用于在所述得到对比结果之后，当所述对比结果为对比不一致时，拦截所述支付请求。

12、根据权利要求 7 所述的装置，所述第一支付数据和所述第二支付数据包括所述支付请求对应的信息流和/或资金流。

13、一种支付系统，包括：

物联网机具，用于向服务端发送支付请求；

服务端，用于处理所述支付请求，生成支付结果数据；

平台，用于执行以下操作：

获取第一支付数据，其中，所述第一支付数据根据所述支付请求对应的清算数据生成；

获取第二支付数据，其中，所述第二支付数据根据所述支付请求对应的结果页生成，所述结果页用于所述物联网机具向外展示；

对所述第一支付数据和所述第二支付数据进行一致性对比，得到对比结果。

14、一种支付安全管理的装置，包括：

存储器，用于存储指令；

处理器，用于执行所述存储器中存储的指令，以执行如权利要求 1-6 中任一项所述的方法。