



(12)发明专利

(10)授权公告号 CN 104272331 B

(45)授权公告日 2017.06.23

(21)申请号 201380020679.4

(22)申请日 2013.04.09

(65)同一申请的已公布的文献号
申请公布号 CN 104272331 A

(43)申请公布日 2015.01.07

(30)优先权数据
61/635,277 2012.04.18 US

(85)PCT国际申请进入国家阶段日
2014.10.17

(86)PCT国际申请的申请数据
PCT/US2013/035865 2013.04.09

(87)PCT国际申请的公布数据
W02013/158419 EN 2013.10.24

(73)专利权人 谷歌公司
地址 美国加利福尼亚州

(72)发明人 萨雷尔·科布斯·约斯滕

(74)专利代理机构 中原信达知识产权代理有限
责任公司 11219
代理人 周亚荣 安翔

(51)Int.Cl.
G06Q 20/20(2006.01)
G06Q 20/32(2006.01)
H04B 5/02(2006.01)

(56)对比文件
WO 2010126509 A2,2010.11.04,说明书第
[0005]-[0079]段.

US 2011078079 A1,2011.03.31,全文.
KR 20060109303 A,2006.10.19,全文.
US 2011191252 A1,2011.08.04,全文.

审查员 李小娅

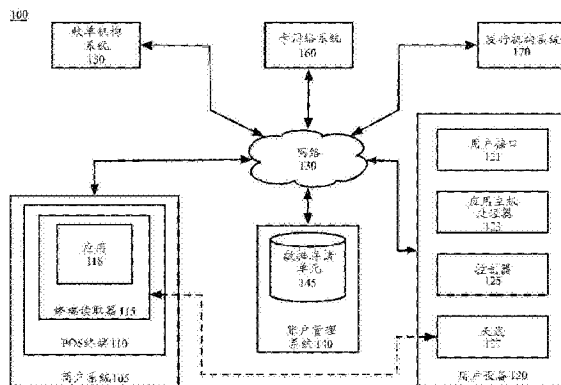
权利要求书3页 说明书13页 附图6页

(54)发明名称

在不具有安全元件的情况下处理支付交易

(57)摘要

用户在不访问驻留在用户设备上的安全元件的情况下通过将来自所述用户设备的支付信息传输到终端读取器来使用商户系统进行无线支付交易。用户在商户系统的终端读取器的射频场中点击用户设备。所述终端读取器和所述用户设备建立通信信道,并且所述终端读取器传输包括对支付处理响应的请求的信号。所述信号由所述用户设备接收,并且由控制器转换成可被应用主机处理器理解请求。所述控制器将所述请求传输到在其中处理所述请求的所述应用主机处理器,并且响应被传输到所述控制器且随后传输到所述终端读取器。由所述应用主机处理器生成的所述响应可由所述商户系统识别为支付响应。



1. 一种用于在不访问安全元件的情况下处理支付交易的计算机实施的方法,其包括:
由移动通信设备且从销售点系统读取器接收对支付账户信息的请求以处理支付交易;
通过对所述支付账户信息的所述请求转换为非安全元件处理器可理解的请求,由所述移动通信设备处理对所述支付账户信息的所述请求;

由所述移动通信设备的所述非安全元件处理器生成对所述支付账户信息的所述请求的响应,所述响应无法从由安全元件处理器生成的响应分辨出来,所述响应包括支付账户识别符,其中由所述非安全元件处理器生成所述响应允许所述移动通信设备使用多个支付提供商中的任何一个的金融账户信息处理支付交易;以及

由所述移动通信设备将对所述支付账户信息的所述请求的所述响应传输到所述销售系统点读取器。

2. 根据权利要求1所述的计算机实施的方法,其中所述支付账户识别符由所述移动通信设备生成。

3. 根据权利要求1所述的计算机实施的方法,其中所述支付账户识别符由账户管理系统生成且被传输到所述移动通信设备,并且所述账户管理系统维护账户,所述账户包括与所述移动通信设备相关联的用户的信用卡账户、借方账户、储值账户、礼品卡账户和银行账户中的至少一个的信息。

4. 根据权利要求1所述的计算机实施的方法,其中所述支付账户识别符对有限次数的使用有效。

5. 根据权利要求1所述的计算机实施的方法,其中所述支付账户识别符与地理限制和时间限制中的至少一个相关联。

6. 根据权利要求1所述的计算机实施的方法,其中所述支付账户识别符包括信用卡账户、借方账户、储值账户、礼品卡账户和银行账号中的一个。

7. 根据权利要求1所述的计算机实施的方法,其中所述支付账户识别符是从数字钱包应用中检索。

8. 根据权利要求1所述的计算机实施的方法,其中使用近场通信(NFC)协议接收对支付处理响应的所述请求。

9. 根据权利要求1所述的计算机实施的方法,其还包括由所述移动通信设备将所述支付账户识别符传送到账户管理系统以进行支付账户识别符验证,到所述账户管理系统的传送包括对由所述移动通信设备传输到所述销售点读取器的所述支付账户信息的所述请求的所述响应。

10. 根据权利要求1所述的计算机实施的方法,其中所述移动通信设备上的所述非安全元件处理器在处理支付请求期间使用可由账户管理系统复制的方案来生成支付账号。

11. 一种用于在不访问安全元件的情况下处理支付交易的移动通信设备,其包括:
安全元件存储设备;
控制器,所述控制器通信耦合到所述存储设备;以及
非安全元件处理器,所述非安全元件处理器通信耦合到所述存储设备和所述控制器,
所述移动通信设备的所述控制器执行存储在所述非安全元件存储设备中的应用代码指令,以使得所述移动通信设备:

从销售点系统读取器接收对支付账户信息的请求以处理支付交易;以及

通过对所述支付账户信息的所述请求转换为非安全元件处理器可理解的请求,处理对所述支付账户信息的所述请求;以及

所述移动通信设备的所述非安全元件处理器执行存储在所述非安全元件存储设备中的应用代码指令,以使得所述移动通信设备:生成对所述支付账户信息的所述请求的响应,所述响应无法从由安全元件处理器生成的响应分辨出来,所述响应包括支付账户识别符,其中由所述非安全元件处理器生成所述响应允许所述移动通信设备使用多个支付提供商中的任何一个的金融账户信息处理支付交易。

12. 根据权利要求11所述的移动通信设备,其中所述支付账户识别符包括由所述移动通信设备生成的支付账号。

13. 根据权利要求11所述的移动通信设备,其中所述支付账户识别符包括由账户管理系统生成且被传输到所述移动通信设备的支付账号,并且所述账户管理系统维护账户,所述账户包括与所述移动通信设备相关联的用户的信用卡账户、借方账户、储值账户、礼品卡账户和银行账号中的一个的信息。

14. 根据权利要求11所述的移动通信设备,其中所述支付账户识别符包括对有限次数的使用有效的支付账号。

15. 根据权利要求11所述的移动通信设备,其中所述支付账户识别符包括与地理限制和时间限制中的至少一个相关联的支付账号。

16. 一种用于在不访问安全元件的情况下处理支付交易的系统,其包括:

存储介质;以及

处理器,其被配置来执行存储在所述存储介质中的计算机可执行指令以使所述系统:

将对支付处理响应的请求传输到移动通信设备,其中所述支付处理响应指示所述移动通信设备是否能够完成支付交易;

从所述移动通信设备接收对所述支付处理响应的所述请求的响应,其中所述移动通信设备通过驻留在所述移动通信设备上的非安全元件处理器处理所述请求,且其中所述响应包括对所述移动通信设备能够完成所述支付交易的批准;

将对支付账户信息的请求传输到所述移动通信设备以处理所述支付交易;以及

响应于所述移动通信设备处理对所述支付账户信息的所述请求,从所述移动通信设备接收由所述移动通信设备的所述非安全元件处理器生成的对所述支付账户信息的所述请求的响应,所述响应无法从由安全元件处理器生成的响应分辨出来,其中所述移动通信设备通过对所述支付账户信息的所述请求转换为非安全元件处理器可理解的请求处理所述请求,其中所述响应包括支付账户识别符,并且其中由所述非安全元件处理器生成所述响应允许所述移动通信设备使用多个支付提供商中的任何一个的金融账户信息处理支付交易。

17. 根据权利要求16所述的系统,其中所述支付账户识别符包括由所述移动通信设备生成的支付账号。

18. 根据权利要求16所述的系统,其中所述支付账户识别符包括由账户管理系统生成且被传输到所述移动通信设备的支付账号,并且所述账户管理系统维护账户,所述账户包括与所述移动通信设备相关联的用户的信用卡账户、借方账户、储值账户、礼品卡账户和银行账号中的一个的信息。

19. 根据权利要求16所述的系统,其中所述支付账户识别符包括对有限数量的使用有效的支付账号。

20. 根据权利要求16所述的系统,其中所述支付账户识别符包括与地理限制和时间限制中的至少一个相关联的支付账号。

在不具有安全元件的情况下处理支付交易

[0001] 相关申请

[0002] 本申请要求2012年4月18日提交且名称为“Processing a Contactless Payment Transaction Without a Secure Element”的美国专利申请第61/635,277号的优先权。上文识别的申请的全部内容特此通过引用的方式全部并入本文。

技术领域

[0003] 本公开一般涉及一种支付交易,且更具体而言,涉及一种在不访问用户设备的安全元件的情况下经由用户计算设备进行的支付交易。

[0004] 发明背景

[0005] 当前的近场通信(“NFC”)系统依赖通常称为“安全元件”的硬件组件,其安装在通信设备上以便为金融交易、交通票务、识别与认证、物理安全访问和其它功能提供安全的操作环境。安全元件通常包括其本身的操作环境,所述环境具有防篡改微处理器、存储器和操作系统。NFC控制器从商户的销售点(“POS”)系统接收支付请求消息,且将该消息传输到安全元件以供处理。典型的NFC控制器包括安全元件。信任服务管理器(“TSM”)或其它形式的安全服务提供商可尤其在安全元件中安装、配置和个性化应用和数据。安全元件具有通常在制造时安装的一个或多个访问密钥。由TSM共享对应的密钥,使得TSM可通过密码建立至安全元件的安全信道,以用于安全元件的安装、配置和个性化,同时终端用户拥有具有安全元件的设备。以此方式,即使设备中的主机CPU已损坏,安全元件仍可保持安全。

[0006] 当前的NFC系统的一个缺点在于在安全元件与TSM之间存在紧密耦合。对于当前部署,仅一个TSM能够访问特定的安全元件的密钥。因此,终端用户可选择配置仅由一个TSM提供的安全元件特征。设备的制造商通常选择该TSM。例如,在购买智能手机的移动网络运营商(“MNO”),诸如Sprint或Verizon而不是终端用户的指导下,智能手机的制造商可为智能手机选择TSM。因此,终端用户可能对其可获得的TSM特征不感兴趣。作为例子,MNO可能仅与一个支付提供商(诸如,万事达卡(MasterCard)或美国银行)有业务关系。所述TSM可允许安全元件配置有仅来自所述一个支付提供商的支付指令。因此,终端用户将无法访问来自其他支付提供商(诸如维萨卡(VISA))的服务。

发明内容

[0007] 在本文描述的某些示例方面中,一种用于在不访问包括促进与用户设备的通信的终端读取器的安全元件的情况下处理支付交易。用户在终端读取器的射频场中点击用户装置。终端读取器和用户设备建立通信信道,以及终端读取器将包括针对支付处理响应的请求的信号。所述信号由用户设备接收,并且由控制器转换成可被应用主机处理器理解请求,其中所述请求被处理,并且响应被传输到控制器且随后传输到终端读取器。由所述应用主机处理器生成的响应可由所述商户系统识别为支付响应,并且无法从由常规的安全元件生成的响应分辨出来,或提供与由常规的安全元件生成的响应相同的功能。

[0008] 在考虑有关示出的示例实施方案的以下详细描述之后,示例实施方案的这些和其

它方面、目的、特征和优点将对本领域的普通技术人员变得显而易见。

[0009] 附图简述

[0010] 图1是描绘根据示例实施方案的支付处理系统的方框图。

[0011] 图2是描绘根据示例实施方案的用于在不访问安全元件的情况下处理支付的方法的方框流程图。

[0012] 图3是描绘根据示例实施方案的用于处理支付处理响应的方法的方框流程图。

[0013] 图4是描绘根据示例实施方案的用于处理有关支付信息的请求的方框流程图。

[0014] 图5是描绘根据示例实施方案的用于处理支付的方框流程图。

[0015] 图6是描绘根据示例实施方案的计算机机器和模块的方框图。

具体实施方式

[0016] 概述

[0017] 本文描述的示例实施方案提供能够在不访问用户设备的安全元件的情况下处理支付交易的方法和系统。在示例实施方案中,用户正通过将支付信息从用户设备传输到终端读取器而使用商户系统进行无线支付交易。在制造时,可将驻留在用户设备上的安全元件紧密耦合到TSM,从而防止用户向不在安全元件上配置的支付账户提供支付指令。在示例实施方案中,用户设备包括能够在不访问安全元件的情况下传输支付信息的应用主机处理器。

[0018] 用户在终端读取器的射频场中点击用户设备。终端读取器和用户设备建立通信信道,并且终端读取器传输包括对支付处理响应的请求的信号。信号由用户设备接收且由控制器转换成可被应用主机处理器理解的请求。控制器将请求传输到应用主机处理器,其中处理所述请求并且生成响应。由应用主机处理器生成的响应可由商户系统识别为支付响应且可从由安全元件生成的响应分辨出来。所述响应由应用主机处理器传输到控制器,其中响应被转换成信号以传输到终端读取器。将信号传输到终端读取器,其中信号被接收且被传输到商户系统。商户系统读取响应,所述响应包括对用户设备可继续进行支付交易的批准指示。

[0019] 商户系统生成对支付信息的请求且将该请求传输到终端读取器。终端读取器以可经由在终端读取器与用户设备之间建立的通信信道传输的信号的形式传输请求。所述信号由用户设备接收且由控制器转换成可被应用主机处理器理解的请求。控制器将请求传输到应用主机处理器,其中处理所述请求且生成响应。响应包括用于交易的支付账号。支付账号可包括与关于用户的金融账户相关联的号码,例如,信用账号、借方账号、储值账号、礼品卡账号、优惠券、忠诚度账号、奖励账号或银行账号。响应还可以包括或替代地包括由账户管理系统或应用主机处理器生成的代理账号。代理账号包括将支付交易路由到其中可检索用户的实际金融账户信息的账户管理系统的信息。代理账号可具有时间、地理和/或价值限制。代理账号还可具有对其被使用的次数的限制。

[0020] 包括支付账户信息的响应由应用主机处理器传输到控制器,其中所述响应被转换成信号以传输到终端读取器。将信号传输到终端读取器,其中信号被接收且被传输到商户系统。驻留在商户系统上的应用处理所述信号,且将其转换成可被商户系统理解的响应。商户系统读取支付账户信息,并且处理该支付。

[0021] 在参考示出程序流程的附图阅读的以下描述中将更详细地解释本发明的发明功能。

[0022] 示例系统架构

[0023] 现转向附图,其中在全部图中,相似的数字指示相似的(但不必相同)元件,详细描述示例实施方案。

[0024] 图1是描绘根据某些示例实施方案的支付处理系统的方框图。如在图1中描绘,示例操作环境100包括商户系统105、用户设备系统120、账户管理系统140和收单机构系统150、卡网络系统160和发行机构系统170,这些系统被配置来经由一个或多个网络130相互通信。在一些示例实施方案中,这些系统中的两个或更多个(包括系统105、120、140、150、160和170)被集成在相同的系统中。

[0025] 每个网络130包括有线或无线电信装置,网络系统(包括系统105、120、140、150、160和170)通过该电信装置可通信且交换数据。例如,每个网络130可实施为或可以是下列项中的一部分:存储区域网(SAN)、个人局域网(PAN)、城域网(MAN)、局域网(LAN)、广域网(WAN)、无线局域网(WLAN)、虚拟专用网(VPN)、内联网、互联网、移动电话网、卡网络、蓝牙、近场通信网(NFC)、任何形式的标准化射频、或其任何组合、或促进信号、数据和/或消息(通常称为数据)的通信的任何其它合适的架构或系统。在通篇说明书中,应理解,术语“数据”和“信息”在本文可互换使用来指代文本、消息、音频、视频或可在基于计算机的环境中存在的任何其它形式的信息。

[0026] 在示例实施方案中,NFC通信协议包括但不限于ISO/IEC 14443类型A和/或B技术(以下称为“ISO 14443”)、MIFARE技术(以下称为“MIFARE”)和/或ISO/IEC 18092技术(以下称为“ISO 18092”)。ISO 14443是用于与读取器邻近操作的用户设备的通信协议。ISO 14443通信协议用于安全卡支付,包括但不限于信用卡支付、借记卡支付或其它形式的金融卡支付。MIFARE是用于符合基于ISO 14443的专用设备标准。MIFARE协议用于存储功能交易,包括但不限于礼品卡、交通卡、车票、访问卡、忠诚卡和其它形式的储值卡交易。MIFARE协议还可用于有限的增值服务。ISO 18092是用于以更高比特率操作的用户设备的通信协议,其允许在设备之间进行更丰富的通信。ISO 18092通信协议用于对等式通信、增值服务(包括但不限于优惠券、忠诚卡、签入卡、会员卡、礼品卡和其它形式的增值服务)和其它形式的更丰富的通信。任何适合的NFC通信协议可用于用户设备120与终端读取器115之间的NFC通信,以实现本文描述的方法和功能。

[0027] 在示例实施方案中,每个网络系统(包括系统105、120、140、150、160和170)包括具有能够通过网络130传输并接收数据的通信模块的设备。例如,每个网络系统(包括系统105、120、140、150、160和170)可包括服务器、个人计算机、移动设备(例如,笔记本电脑、平板电脑、上网本、个人数字助理(PDA)、视频游戏设备、GPS定位器设备、蜂窝电话、智能手机或其它移动设备)、电视机(其中一个或多个处理器嵌入其中和/或与其耦合)或其它适当技术,所述技术包括或耦合到网络浏览器或其它应用以经由网络130进行通信。在图1中描绘的示例实施方案中,网络系统(包括系统105、120、140、150、160和170)分别由商户、用户或顾客、账户管理系统操作员、收单机构系统操作员、卡网络系统操作员和发行机构系统操作员操作。

[0028] 商户系统105包括至少一个销售点(“POS”)终端110,其能够处理由用户发起的购

买交易。在示例实施方案中,商户操作网上商店,且用户通过在网站上单击链接或“购买”按钮来指示购买的欲望。在一些示例实施方案中,用户设备120被配置来执行POS终端110的功能。在该实例中,用户在不与POS终端110交互的情况下经由用户设备120扫描和/或支付该交易。示例商户系统105至少包括终端读取器115,其能够经由应用118与用户设备系统120和商户POS终端110通信。根据一些示例实施方案,应用118可以是POS终端110或商户系统105(图1中未示出)的集成部分、终端读取器115(示出)的集成部分或独立的硬件设备(未示出)。

[0029] 在示例实施方案中,终端读取器115能够使用NFC通信方法与用户设备120通信。在另一示例实施方案中,终端读取器115能够使用蓝牙通信方法与用户设备120通信。在又一示例实施方案中,终端读取器115能够使用Wi-Fi通信方法与用户设备120通信。在一些示例实施方案中,用户扫描QR码或条形码或在用户设备120上单击URL链接,其将用户设备120与在线商户系统105暂时关联起来。POS终端110查询在线商户系统105以链接到用户和/或用户设备120。在示例实施方案中,终端读取器115可被配置来读取任何数量的条形码格式,包括但不限于,QR码、通用产品代码(“UPC”)、全球贸易项目代码(“GTIN”)、库存单位(“SKU”)、日本商品代码(“JAN”)、世界产品代码(“WPC”)、国际标准书号(“ISBN”)、欧洲商品编号(“EAN”)等。根据其它示例实施方案,终端读取器115可以是电子场发生器,其具有CPU、激光扫描器、电荷耦合设备(“CCD”)读取器、基于摄像机读取器、全方位条形码扫描器、摄像机、RFID读取器或能够读取商户系统105中的产品识别符信息的任何其它设备。

[0030] 在示例实施方案中,用户设备120可以是个人计算机、移动设备(例如,笔记本电脑、平板电脑、上网本、个人数字助理(“PDA”)、视频游戏设备、GPS定位器设备、蜂窝电话、智能手机或其它移动设备)、电视机(其中一个或多个处理器嵌入其中和/或与其耦合)或其它适当技术,所述技术可经由设备120与另一设备(诸如终端读取器115)之间的电子场、磁场或射频场进行通信。在示例实施方案中,用户设备120具有处理能力,诸如存储能力/内存和可执行特定功能的一个或多个应用(未图示)。在示例实施方案中,用户设备120包含操作系统(未图示)和用户接口121。在一些示例实施方案中,用户设备120包括操作系统(未图示),其在没有用户接口121的情况下通过音频端口或辅助数据端口进行通信。

[0031] 用户设备120还包括控制器125。在示例实施方案中,控制器125是NFC控制器。在一些示例实施方案中,控制器125是蓝牙链接控制器。蓝牙链接控制器可能发送并接收数据,执行认证和加密功能,以及指导用户设备120如何将如何监听来自终端读取器115的传输或如何根据蓝牙特定程序将用户设备120配置成各种省电模式。在另一示例实施方案中,控制器125是能够执行相似功能的Wi-Fi控制器或NFC控制器。

[0032] 用户设备120经由天线127与终端读取器115通信。在示例实施方案中,一旦用户设备应用已被激活并且优先化,则通知控制器125用户设备120关于交易的准备状态。控制器125通过天线127输出无线电信号,或监听来自设备读取器115的无线电信号。在于用户设备120与终端读取器115之间建立安全通信之后,读取器115从用户设备120请求支付处理响应。

[0033] 示例控制器125从终端读取器115接收通过天线127传输的无线电波通信信号。控制器125将信号转换成可读字节。在示例实施方案中,字节包括数字信息,诸如对支付处理响应的请求或对支付卡信息的请求。控制器125将请求传输到应用主机处理器123。

[0034] 示例用户设备120可包括安全元件或安全存储器(未示出),其可存在于可移动的智能芯片或安全数字(“SD”)卡内或其可嵌入在设备120上的固定芯片内。在某些示例实施方案中,用户身份模块(“SIM”)卡可能够托管安全元件,例如,NFC SIM卡。安全元件(未示出)允许设备用户120与安全元件内的某些功能安全交互,同时保护存储在安全元件(未示出)内的信息。在示例实施方案中,安全元件(未示出)包括智能卡典型的组件,诸如加密处理器或随机生成器。在示例实施方案中,安全元件(未示出)在由智能卡操作系统(诸如JavaCard开放平台(“JCOP”)操作系统控制的高度安全的系统级芯片中包括智能MX类型NFC控制器。在另一示例实施方案中,安全元件(未示出)被配置来包括非EMV类型非接触智能卡,作为可选的实施方式。安全元件(未示出)与用户设备120中的应用通信。在示例实施方案中,安全元件(未示出)能够存储加密的用户信息且仅允许信任应用访问存储的信息。在示例实施方案中,控制器125与安全密钥加密的应用交互以在安全元件中进行解密和安装。

[0035] 在示例用户设备120中,支付请求由应用主机处理器123而不是由安全元件(未示出)处理。示例应用主机处理器123可存在于可移动的智能芯片或安全数字(“SD”)卡内或其可嵌入在设备120上的固定芯片内。应用主机处理器可包括在其上运行的执行本文描述的功能的应用(未示出)。在示例实施方案中,用户设备120将支付账户信息以代理或虚拟账户识别符的形式传送到商户系统105,而不传输用户的实际账户信息。用户的实际账户信息由账户管理系统140维护而不是在驻留在用户设备120上的安全元件(未示出)内维护。

[0036] 示例商户系统105和用户设备120与账户管理系统140通信。账户管理系统140能够为用户存储一个或多个支付账户。在示例实施方案中,用户注册一个或多个支付账户,例如,信用卡账户、借方账户、银行账户、礼品卡账户、优惠券、储值账户、忠诚度账户、奖励账户和其它形式的支付账户,这些账户能够使用账户管理系统140进行购买。例如,用户可使用账户管理系统140创建数字钱包账户。支付账户可与用户的由账户管理系统140维护的数字钱包账户相关联。用户可在任何时间访问数字钱包账户以增加、修改或移除支付账户。在示例实施方案中,将用户的数字钱包信息传输到用户的用户设备120,以能够在不访问账户管理系统140的情况下使用用户的支付账户。在一些示例实施方案中,账户管理系统140将限制使用的代理账户信息传输到用户设备120,以能够在支付交易期间使用支付账户,所述支付交易在支付处理期间被路由到账户管理系统140。例如,代理账号可将支付授权请求路由到账户管理系统140,其充当用于代理账户的发行机构系统170。在另一示例实施方案中,用户设备120可包括生成使得支付交易能够被路由到账户管理系统140的限制使用的代理账号的应用(未示出)。在一些示例实施方案中,应用主机处理器123执行该功能。

[0037] 示例账户管理系统140包括可由账户管理系统140访问的数据存储单元145。示例数据存储单元145可包括一个或多个有形的计算机可读存储设备,其能够存储用户的支付账户信息。用户可从商户系统105请求购买。在示例实施方案中,购买由用户设备120和终端读取器115的无线“点击”发起。商户系统105与收单机构系统150(例如,Chase、PaymentTech或其它第三方支付处理公司)、卡网络系统160(例如,维萨卡、万事达卡、美国运通卡、发现卡(Discover)或其它卡处理网络)和发行机构系统170(例如,花旗银行、第一资本金融公司(CapitalOne)、美国银行或授权支付的其它金融机构)交互以处理支付。在一些示例实施方案中,由用户设备120传输到终端读取器115的支付卡信息是代理账号或令牌账号,其将支付交易链接到由账户管理系统140维护的用户账户。将支付交易路由到账户管理系统140用

于识别用户的正确支付卡信息。

[0038] 下文参考图2-5中图示的示例方法来描述示例操作环境100的组件。还可使用其它系统且在其它环境中执行图2-5的示例方法。

[0039] 示例系统处理

[0040] 图2是描绘根据示例实施方案的用于在不访问安全元件的情况下处理支付的方法的方框流程图。参考图1中图示的组件来描述方法200。

[0041] 在方框205中,用户点击位于终端读取器115近端的用户设备120。在示例实施方案中,终端读取器115生成射频(“RF”)场或其它场以轮询用户设备120的存在,以及用户通过将设备120放在终端读取器115的场内而“点击”用户设备120。在一些示例实施方案中,商户使用终端读取器115的应用118激活RF场或其它场以轮询用户设备120的存在。在某些示例实施方案中,在点击用户设备120时,执行本文的图2-5中描述的系统和方法。

[0042] 在方框210,用户设备120和终端读取器115建立通信信道。在示例实施方案中,通信信道是NFC信道。在一些示例实施方案中,通信信道是蓝牙通信信道。在又一示例实施方案中,通信信道是Wi-Fi通信信道。因此,可经由用户设备120与终端读取器115之间的无线或“无接触”通信来进行支付交易。

[0043] 在示例实施方案中,终端读取器115从用户设备120请求协议和特性以建立通信信道。例如,终端读取器115可请求识别来自用户设备120的通信协议(例如,ISO/IEC 14443、MIFARE和/或ISO/IEC 18092)、可用的应用列表和安全协议。

[0044] 在方框215中,终端读取器115将请求支付处理响应的信号传输到用户设备120。在示例实施方案中,支付处理响应是继续进行金融支付交易的请求。在示例实施方案中,支付处理响应向终端读取器115指示用户设备120能够执行金融交易。在涉及安全元件的典型无线支付交易中,用户设备120使用由安全元件创建的消息对终端读取器115的请求作出响应。该消息可被终端读取器115理解以包括支付处理响应。在示例实施方案中,支付处理响应由驻留在用户设备120中的应用主机处理器123而不是安全元件创建。支付处理响应可以与由安全元件创建的响应的相同方式被终端读取器115理解。

[0045] 在方框220中,用户设备120接收由终端读取器115传输的信号。在示例实施方案中,信号由天线127接收且被传输到控制器125。在示例实施方案中,点击是NFC点击,且控制器125是NFC控制器。

[0046] 在方框225中,控制器125将信号转换成对支付处理响应的可读请求。在示例实施方案中,将信号转换成包括对支付处理响应的可读请求的字节。

[0047] 在方框230中,控制器125将对支付处理响应的请求传输到应用主机处理器123。在示例实施方案中,应用主机处理器123在支付交易期间以类似于安全元件的方式运行。

[0048] 在方框235中,处理对支付处理响应的请求。以下参考图3中描述的方法更详细地描述用于处理对支付处理响应的请求的方法。

[0049] 图3是参考图2的方框235描绘根据示例实施方案的用于处理支付处理响应的方法的方框流程图。参考图1中图示的组件描述方法235。

[0050] 在方框310中,应用主机处理器123接收对支付处理响应的请求。在示例实施方案中,所述请求在被应用主机处理器123接收前通过一系列连接进行传输。在一些示例实施方案中,将请求从控制器125直接传输到应用主机处理器123。

[0051] 在方框320中,应用主机处理器123生成支付处理响应。在示例实施方案中,支付处理响应包括可被终端读取器115理解的语言,指示用户设备120能够完成支付交易。在示例实施方案中,支付处理响应包括与由常规安全元件或安全储存器生成的支付处理响应相同的语言和/或信息。在示例实施方案中,支付处理响应包括用户可识别数据、个人识别符、账户识别符、支付网络配置数据、商户特定数据和/或安全数据,其中的任一项可用来验证在用户的账户上执行的交易的序列。

[0052] 在方框330中,应用主机处理器123将支付处理响应传输到控制器125。在示例实施方案中,支付处理响应在被控制器125接收前通过一系列连接进行传输。在一些示例实施方案中,将支付处理响应直接传输到控制器125。

[0053] 在方框340中,控制器125接收支付处理响应。在示例实施方案中,支付处理响应包括将由控制器125转换成可传输的信号的字节。

[0054] 在方框350中,控制器125将支付处理响应传输到终端读取器115。在示例实施方案中,支付处理响应是由天线127传输到终端读取器115的信号。

[0055] 在方框360中,终端读取器115接收支付处理响应。在示例实施方案中,终端读取器115接收由用户设备传输的信号。

[0056] 在方框370中,终端读取器将支付处理响应传输到商户系统105。在示例实施方案中,将支付处理响应传输到驻留在商户系统105中的POS终端110。

[0057] 在方框380中,商户系统105接收支付处理响应。在示例实施方案中,驻留在商户系统上的应用118将信号转换成可被商户系统105理解的语言。在示例实施方案中,商户系统105理解支付处理响应以包括对用户设备120能够执行支付交易的批准响应。

[0058] 方法235随后进行到图2中的方框240。

[0059] 回到图2,在方框240中,处理对支付账户信息的请求。以下参考图4中描述的方法更详细地描述用于处理支付账户信息的方法。

[0060] 图4是参考图2的方框240描绘根据示例实施方案的用于处理对支付信息的请求的方法的方框流程图。参考图1中图示的组件来描述方法240。

[0061] 在方框410中,商户系统105生成对支付账户信息的请求并将其传输到终端读取器115。在示例实施方案中,对支付处理响应的请求包括对支付账户信息的请求,且不需要在方框410至490和在方框240至265中描述的方法。

[0062] 在方框420中,终端读取器115接收由商户系统105传输的对支付账户信息的请求。在示例实施方案中,驻留在商户系统105上的应用118读取支付处理响应,且生成对支付账户信息的请求作为响应。在示例实施方案中,将请求转换成信号,该信号能够经由通信信道传输到用户设备120且被转换成可被应用主机处理器123理解的字节。

[0063] 在方框430中,终端读取器115将包括对支付账户信息的请求的信号传输到用户设备120。在示例实施方案中,对支付账户信息的请求包括对完成支付交易的信息(诸如账号、截止日期和安全码)的请求。

[0064] 在方框440中,用户设备120接收由终端读取器115传输的信号。在示例实施方案中,信号由天线127接收且被传输到控制器125。

[0065] 在方框450中,控制器125将信号转换成对支付账户信息的可读请求。在示例实施方案中,信号被转换成包括对支付账户信息的可读请求的字节。

[0066] 在方框460中,控制器125将对支付账户信息的请求传输到应用主机处理器123。在示例实施方案中,应用主机处理器123在支付交易期间以类似于安全元件的方式运行。

[0067] 在方框470中,应用主机处理器123接收对支付账户信息的请求。在示例实施方案中,请求在被应用主机处理器123接收前通过一系列连接进行传输。在一些示例实施方案中,将请求从控制器125直接传输到应用主机处理器123。

[0068] 在方框480中,应用主机处理器123生成将用于支付交易的支付账户信息。在示例实施方案中,用户注册一个或多个支付账户,例如,信用卡账户、借方账户、银行账户、礼品卡账户、优惠券、储值账户、忠诚度账户、奖励账户和其它形式的支付账户,这些账户能够使用账户管理系统140进行购买。例如,用户可使用账户管理系统140创建数字钱包账户,其将支付账户与用户和/或用户的用户设备120相关联。数字钱包账户信息可存储在账户管理系统140中,且还可本地存储在用户的用户设备120中。

[0069] 在示例实施方案中,将用户的数字钱包信息传输到用户的用户设备120,并且应用主机处理器123通过访问用户的保存在用户的数字钱包账户的支付账户来生成支付账户信息。在该实施方案中,应用主机处理器123可选择特定的支付账户用于支付交易。

[0070] 在一些示例实施方案中,账户管理系统140将一个或多个限制使用的代理账号传输到用户设备120。应用主机处理器123通过访问传输的限制使用的代理账号并选择特定代理账号用于交易来生成支付账户信息。在示例实施方案中,账户管理系统140可定期地生成限制使用的代理账号并使用当前号码更新用户的用户设备120。在一些示例实施方案中,用户的用户设备120可将限制使用的代理账号的请求传送到账户管理系统140,并且作为响应,账户管理系统140可将限制使用的代理账号传送到用户的用户设备120以用于支付交易。在又一示例实施方案中,应用主机处理器123本地生成代理账号。当账户管理系统140从商户系统105接收支付请求时,应用主机处理器123可将生成的限制使用的代理账号传送到账户管理系统140以供账户管理系统140验证。在一些示例实施方案中,当账户管理系统140从商户系统105接收支付请求时,应用主机处理器可使用可被账户管理系统140复制的方案来生成限制使用的代理账号以允许账户管理系统140验证生成的限制使用的代理账号。

[0071] 代理账号可具有时间或地理限制。例如,代理账号可能仅对有限的时间有效或其可能仅在具体的地理位置中有效。限制使用的代理账号标有、其中编码有或另外包含参考时间、持续时间、用户设备120的地理位置和/或基于用户设备120的地理位置的地理区域。这些特征可允许限制使用的代理账号在指定的时间段之后或在超出指定的地理位置外使用时过期。代理账号还可具有对其可被使用的次数的限制。例如,每个代理账号可能仅对单次使用有效。

[0072] 在方框490中,应用主机处理器123将支付账户信息传输到控制器125。在示例实施方案中,支付账户信息在被控制器125接收前通过一系列连接进行传输。在一些示例实施方案中,将支付处理响应直接传输到控制器125。

[0073] 方法240随后进行到图2中的方框245。

[0074] 回到图2,在方框250中,控制器125接收支付账户信息。在示例实施方案中,支付账户信息包括将由控制器125转换成可传输的信号的字节。

[0075] 在方框250中,控制器125将支付账户信息传输到终端读取器115。在示例实施方案中,支付账户信息是由天线127传输到终端读取器115的信号。

[0076] 在方框255中,终端读取器115接收支付账户信息。在示例实施方案中,终端读取器115接收由用户设备120传输的信号。

[0077] 在方框260中,终端读取器将支付处理响应传输到商户系统105。在示例实施方案中,将支付处理响应传输到驻留在商户系统105中的POS终端110。

[0078] 在方框265中,商户系统105接收支付账户信息。在示例实施方案中,驻留在商户系统105上的应用118将信号转换成可被商户系统105理解的语言。在示例实施方案中,用户可被提示将个人识别号(“PIN”)输入商户系统105中。

[0079] 在方框270中,处理支付。以下参考在图5中描述的方法来更详细地描述用于处理支付的方法。

[0080] 图5是参考图2的方框270描绘的根据示例实施方案的用于处理支付的方法的方框流程图。参考图1中图示的组件来描述方法270。

[0081] 在方框505中,商户系统105使用由用户设备120提供的支付账户信息生成支付请求消息以请求支付,并且将支付请求提交到收单机构系统150。在示例实施方案中,商户的POS终端110经由网络130将请求提交到收单机构系统150。

[0082] 在方框510中,收单机构系统150接收支付请求,并且将其提交到卡网络系统160。

[0083] 在方框515中,卡网络系统160确定用来支付交易的支付账户信息是否是经典账号。在示例实施方案中,卡网络系统160使用一系列号码或路由支付账户信息中的信息来自自动做出该确定。在一些示例实施方案中,卡网络系统160查阅由账户管理系统140提供到卡网络系统160的保存账户识别信息的列表。

[0084] 如果账号是经典账号,则根据传统的支付处理方法处理支付(在方框520中)。在示例实施方案中,如果账号能够在不被账户管理系统140处理的情况下(例如,如果用户设备120将用户的实际信用卡账号、借记卡账号、储值账号、礼品卡账号或银行账号传输到商户系统105)被路由到发行机构系统,则该账号是经典支付账户。

[0085] 回到方框515,如果账号不是经典账号,则发行机构系统170是账户管理系统140(例如,如果代理账户信息用于交易)。在方框525中,卡网络系统160随后将支付请求转发到账户管理系统140。

[0086] 在一些示例实施方案中,支付账户信息可包括与保存的账户识别信息的列表对应的识别符,诸如一批账号或其它标记,其识别发行机构系统170或账户管理系统140。基于该识别符,如果识别符对应于常规的发行机构系统170,则根据传统的支付处理方法处理支付(在方框520中);或如果识别符对应于账户管理系统140,则将支付转发到账户管理系统140(在方框525中)。

[0087] 在一些示例实施方案中,参考方框515和525描述的方法可由收单机构系统150或发行机构系统170而不是卡网络系统160执行。

[0088] 在方框530中,账户管理系统140从卡网络系统160接收支付请求。

[0089] 在方框535中,账户管理系统140识别与代理账户信息相关联的用户。在示例实施方案中,账户管理系统140包含针对每个用户生成的代理账户信息的列表,并且可将该信息映射到用户的数字钱包账户。在一些示例实施方案中,单向算法(诸如哈希函数)可用于识别用户的数字钱包账户或将用户的数字钱包账户与代理账户信息关联起来。在又一示例实施方案中,硬件安全模块(“HSM”)可用于存储安全的数字,诸如针对每个用户生成的代理账

户信息的列表。HSM可由账户管理系统140通过安全网络接触以将针对每个用户生成的代理账户信息的列表映射到用户的数字钱包账户。

[0090] 在示例实施方案中,账户管理系统140证实尚未违反代理账户信息的限制规则。例如,账户管理系统140确认代理号码尚未违反时间/地理限制或对使用次数的限制。

[0091] 在方框540中,账户管理系统140识别用户的保存支付账户信息。在示例实施方案中,用户的数字钱包账户包含由用户定义的规则(或如果用户尚未修改默认规则,则为默认规则)。如果用户已定义支付规则,则账户管理系统140首先应用用户定义的规则以确定将支付账户应用于交易的顺序。在示例实施方案中,账户管理系统140首先应用用户定义的规则。

[0092] 在方框545中,账户管理系统140生成新的支付请求并经由卡网络系统160将其传输到选定支付账户的发行机构系统170。在一些示例实施方案中,账户管理系统140是支付账户的发行机构系统170。在该实施方案中,账户管理系统140将确定是否有足够的资金用于交易并且因此批准/拒绝交易。

[0093] 在方框550中,发行机构170从账户管理系统140接收新的支付请求。

[0094] 在方框555中,发行机构170批准或拒绝交易。如果交易被拒绝,则在方框557中,将通知账户管理系统140所拒绝的交易。账户管理系统140通知商户系统105所拒绝的交易。

[0095] 如果交易被批准,则发行机构系统170经由卡网络系统160将授权消息传输到账户管理系统140(在方框560中)。如果账户管理系统140是支付账户的发行机构系统170(见方框515),则账户管理系统140注明对交易的授权。

[0096] 在方框565中,账户管理系统140接收授权消息并且将对原始支付请求的批准传输到卡网络系统160。

[0097] 在方框570中,通过收单机构系统150将授权消息传输到商户系统105。

[0098] 在示例实施方案中,终端读取器115与用户设备120之间的通信信道随后被终止。在示例实施方案中,当终止终端读取器115与用户设备120之间的通信信道的请求被传送时或在其后任何何时的时间,可终止原始的通信信道。

[0099] 其它示例实施方案

[0100] 图6描绘根据某些示例实施方案的计算机器2000和模块2050。计算机器2000可与本文呈现的各种计算机、服务器、移动设备、嵌入式系统或计算系统中的任一个对应。模块2050可包括被配置来促进计算机器2000执行本文呈现的各种方法和处理功能的一个或多个硬件或软件元件。计算机器2000可包括用于与网络2080通信的各种内部或附接组件,诸如处理器2010、系统总线2020、系统存储器2030、存储介质2040、输入/输出接口2060和网络接口2070。

[0101] 计算机器2000可实施为常规的计算机系统、嵌入式控制器、膝上型电脑、服务器、移动设备、智能手机、机顶盒、一体机、车载信息系统、与电视机相关联的一个或多个处理器、定制机器或任何其它硬件平台、或其任何组合或多样性。计算机器2000可以是分布式系统,其被配置来使用经由数据网络或总线系统互连的多个计算机器来运行。

[0102] 处理器2010可被配置来执行代码或指令以执行本文描述的操作和功能,管理请求流和地址映射,并且执行计算且生成命令。处理器2010可被配置来监测且控制计算机器2000中的组件的操作。处理器2010可以是通用处理器、处理器核心、多重处理器、可重配置

处理器、微控制器、数字信号处理器(“DSP”)、特定应用集成电路(“ASIC”)、图形处理单元(“GPU”)、现场可编程门阵列(“FPGA”)、可编程逻辑设备(“PLD”)、控制器、状态机、门控逻辑、分立硬件组件、任何其它处理单元或其任何组合或多样性。处理器2010可以是单个处理单元、多个处理核心、单个处理核心、多个处理核心、专用处理核心、协同处理器或其任何组合。根据某些实施方案,处理器2010连同计算机器2000的其它组件可以是在一个或多个其它计算机器中执行的虚拟计算机器。

[0103] 系统存储器2030可包括非易失性存储器,诸如只读存储器(“ROM”)、可编程只读存储器(“PROM”)、可擦除可编程只读存储器(“EPROM”)、闪存或任何其它设备,这些设备在施加电力或不施加电力的情况下能够存储程序指令或数据。系统存储器2030还可包括易失性存储器,诸如随机存取存储器(“RAM”)、静态随机存取存储器(“SRAM”)、动态随机存取存储器(“DRAM”)和同步动态随机存取存储器(“SDRAM”)。其它类型的RAM还可用于实施系统存储器2030。系统存储器2030可使用单个存储器模块或多个存储器模块实施。虽然系统存储器2030被描绘成计算机器2000的一部分,但是本领域的技术人员将理解,在不脱离主题技术的范围的情况下,系统存储器2030可独立于计算机器2000。还应理解,系统存储器2030可包括非易失性存储器(诸如存储介质2040)或结合其进行操作。

[0104] 存储介质2040可包括硬盘、软盘、只读存储光盘(“CD-ROM”)、数字通用光盘(“DVD”)、蓝光光盘、磁带、闪存、其它非易失性存储设备、固态驱动器(“SSD”)、任何磁性存储设备、任何光学存储设备、任何电气存储设备、任何半导体存储设备、任何基于物理的存储设备、任何其它数据存储设备或其任何组合或多样性。存储介质2040可存储一个或多个操作系统、应用程序和程序模块(诸如模块2050)、数据、或任何其它信息。存储介质2040可以是计算机器2000的一部分或连接到计算机器2000。存储介质2040还可以是与计算机器2000通信的一个或多个其它计算机器(诸如服务器、数据库服务器、云存储、网络附加存储等)的一部分。

[0105] 模块2050可包括一个或多个硬件或软件元件,其被配置来促进计算机器2000执行本文呈现的各种方法和处理功能。模块2050可包括一个或多个指令的序列,其存储为与系统存储器2030、存储介质2040或二者相关联的软件或固件。存储介质2040可因此表示机器或计算机可读介质的实例,指令或代码可存储在机器或计算机可读介质上以供处理器2010执行。机器或计算机可读介质可通常指代用于向处理器2010提供指令的任何媒介或介质。与模块2050相关联的这种机器或计算机可读介质可包括计算机软件产品。应理解,包括模块2050的计算机软件产品还可与一个或多个进程或方法相关联,所述一个或多个进程或方法经由网络2080、任何信号承载媒介或任何其它通信或递送技术来将模块2050递送到计算机器2000。模块2050还可包括硬件电路,或用于配置硬件电路的信息(诸如微码)或用于FPGA或其它PLD的配置信息。

[0106] 输入/输出(“I/O”)接口2060可被配置来耦合到一个或多个外部设备,以接收来自所述一个或多个外部设备的数据并且将数据发送到所述一个或多个外部设备。此类外部设备连同各种内部设备还可被称为外围设备。I/O接口2060可包括用于可操作地将各种外围设备耦合到计算机器2000或处理器2010的电气和物理连接。I/O接口2060可被配置来在外围设备、计算机器2000或处理器2010之间传送数据、地址和控制信号。I/O接口2060可被配置来实施任何标准接口,诸如小型计算机系统接口(“SCSI”)、串行SCSI(“SAS”)、光纤通道、

外围组件互连(“PCI”)、PCI express (PCIe)、串行总线、并行总线、高级技术附加装置(“ATA”)、串行ATA(“SATA”)、通用串行总线(“USB”)、Thunderbolt、火线、各种视频总线等。I/O接口2060可被配置来仅实施一个接口或总线技术。替代地,I/O接口2060可被配置来实施多个接口或总线技术。I/O接口2060可被配置成系统总线2020的一部分或全部,或结合系统总线2020进行操作。I/O接口2060可包括一个或多个缓冲器,其用于缓冲一个或多个外部设备、内部设备、计算机器2000或处理器2010之间的传输。

[0107] I/O接口2060可将计算机器2000耦合到各自输入设备,其包括鼠标、触摸屏、扫描器、生物特征读取器、电子数字化器、传感器、接收器、触摸板、轨迹球、摄像机、麦克风、键盘、任何其它指点设备或其任何组合。I/O接口2060可将计算机器2000耦合到各自输出设备,其包括视频显示器、扬声器、打印机、投影机、触觉反馈设备、自动控制、机械组件、制动器、电动机、风扇、螺线管、阀门、泵、传输器、信号发射器、灯等。

[0108] 计算机器2000可在使用通过网络接口2070到跨网络2080的一个或多个其它系统或计算机器的逻辑连接的联网环境中操作。网络2080可包括广域网(WAN)、局域网(LAN)、内联网、互联网、无线接入网络、有线网络、移动网络、电话网络、光网络或其组合。网络2080可以是任何拓扑的分组交换、电路交换且可使用任何通信协议。网络2080内的通信链路可涉及各种数字或模拟通信介质,诸如光纤电缆、自由空间光学器件、波导管、电导体、无线链路、天线、射频通信等。

[0109] 处理器2010可通过系统总线2020连接到计算机器2000的其它元件或本文讨论的各种外围设备。应理解,系统总线2020可位于处理器2010内、处理器2010外或二者皆可。根据一些实施方案,本文所讨论的处理器2010的任一个、计算机器2000的其它元件或各种外围设备可集成在单个设备中,诸如系统级芯片(“SOC”)、系统级封装(“SOP”)或ASIC设备。

[0110] 在其中本文讨论的系统收集关于用户的个人信息或可利用个人信息的情况下,用户可被提供以下机会:控制程序或特征是否收集用户信息(例如,关于用户的社交网络、社交行为或活动、职业、用户的偏好或用户的当前位置的信息),控制是否和/或如何从内容服务器接收可能与用户更相关的内容。此外,某些数据在其被存储或使用之前可以一种或多种方式进行处理,使得个人可识别信息被移除。例如,可处理用户的身份,使得无法确定关于用户的个人可识别信息,或可生成用户的地理位置,其中获取位置信息(诸如城市、邮政编码或国家级),使得无法确定用户的特定位置。因此,用户可控制如何收集有关用户的信息以及内容服务器如何使用信息。

[0111] 实施方案可包括体现本文描述和图示的功能的计算机程序,其中计算机程序在包括存储于机器可读介质中的指令的计算机系统和执行所述指令的处理器中实现。然而,应显而易见的是,可能存在于计算机编程中实现实施方案的许多不同的方式,且实施方案不应被理解为受限于任何一组计算机程序指令。进一步地,熟练的编程人员将能够写入这样的计算机程序以基于随附的流程图和在申请文本中的相关描述来实现公开的实施方案。因此,特定一组程序代码指令的公开内容不被认为对充分理解如何制作并使用实施方案是必要的。进一步地,本领域的技术人员将理解,本文描述的实施方案的一个或多个方面可由如可嵌入在一个或多个计算系统中的硬件、软件或其组合实施。另外,对由计算机执行的行为的任何参考不应被理解成由单个计算机执行,因为超过一个计算机可执行这种行为。

[0112] 本文描述的示例实施方案可与执行本文描述的方法和处理功能的计算机硬件和软件一起使用。本文描述的系统、方法和流程可体现于可编程计算机、计算机可执行软件或数字电路中。软件可存储在计算机可读介质上。例如，计算机可读介质可包括软盘、RAM、ROM、硬盘、可移动介质、闪存、记忆棒、光学介质、磁光介质、CD-ROM等。数字电路可包括集成电路、门阵列、构件块逻辑、现场可编程门阵列 (FPGA) 等。

[0113] 在先前呈现的实施方案中描述的示例系统、方法和行为是说明性的，且在替代实施方案中，某些行为可以不同的顺序执行、彼此并行执行、可被完全省略和/或在不同示例实施方案之间组合，和/或可执行某些额外的行为，而不脱离各种实施方案的范围和精神。因此，此类替代实施方案包括在本文请求的发明中。

[0114] 虽然上文已详细描述具体实施方案，但是本描述仅用于说明的目的。因此，上文描述的许多方面不打算作为必需或必要的元素，除非另有说明。得益于本公开，本领域的普通技术人员还可作出对与除了上文描述的那些方面之外的示例实施方案的公开方面对应的等同组件或行为的修改，而不脱离在以下权利要求定义的实施方案的精神和范围，所述权利要求的范围被赋予最广义的解释以涵盖此类修改和等同结构。

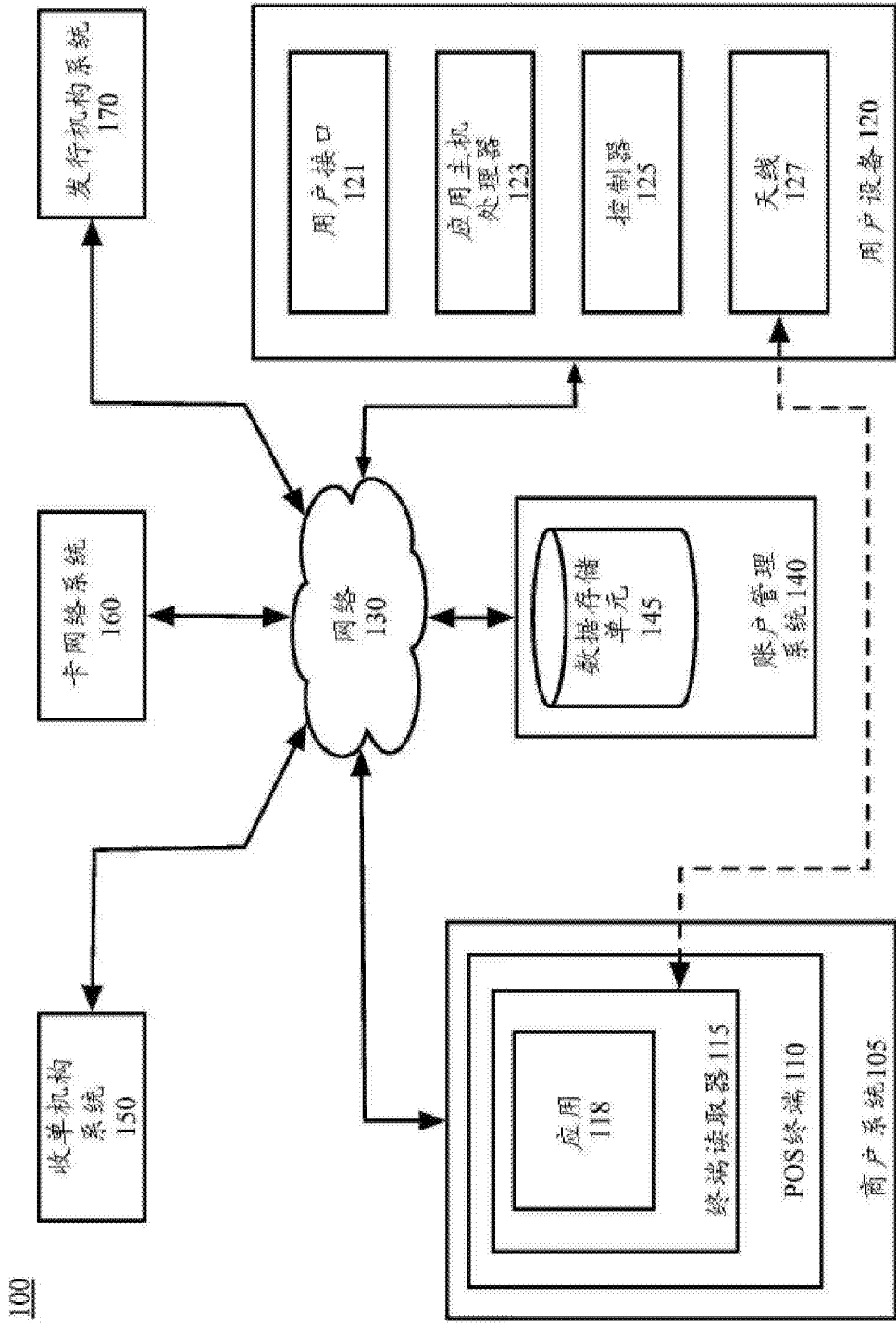


图1

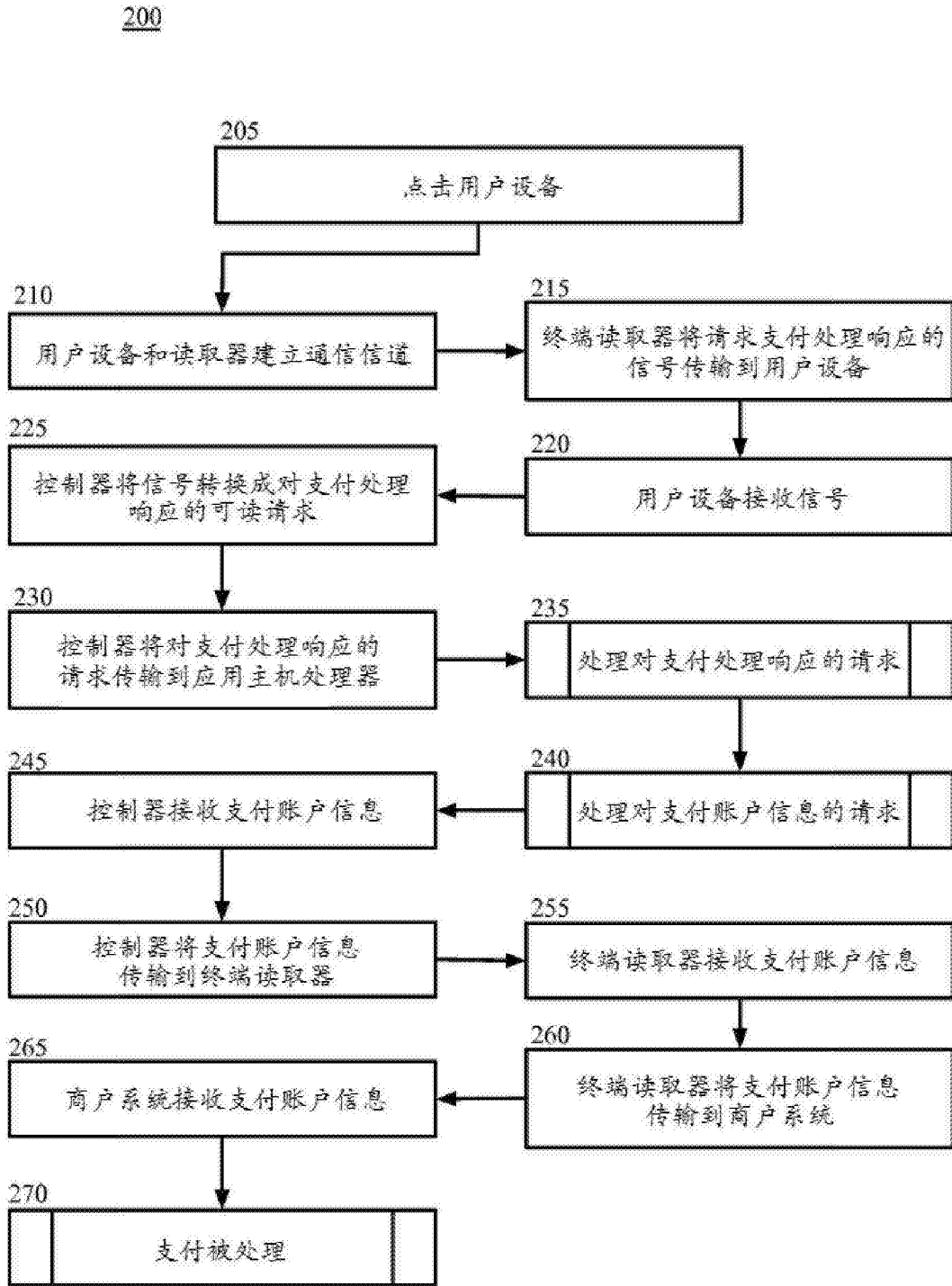


图2

235

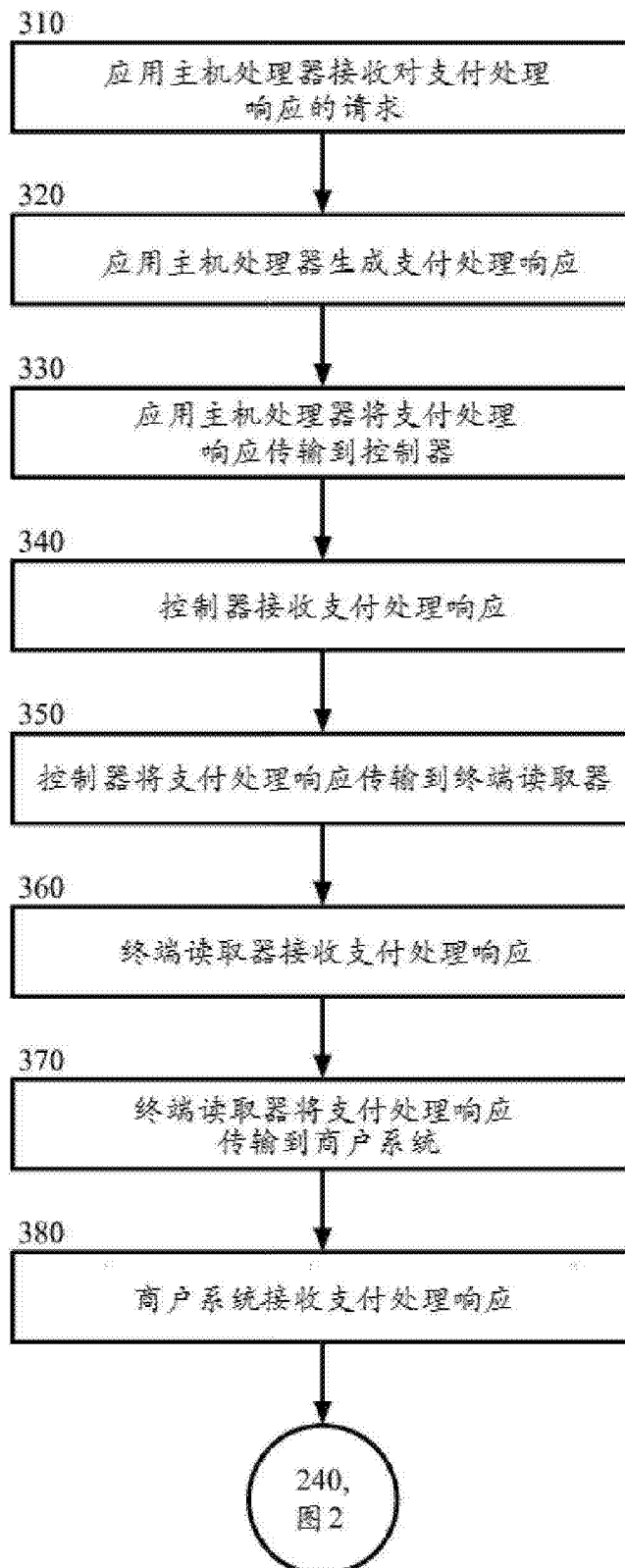


图3

240

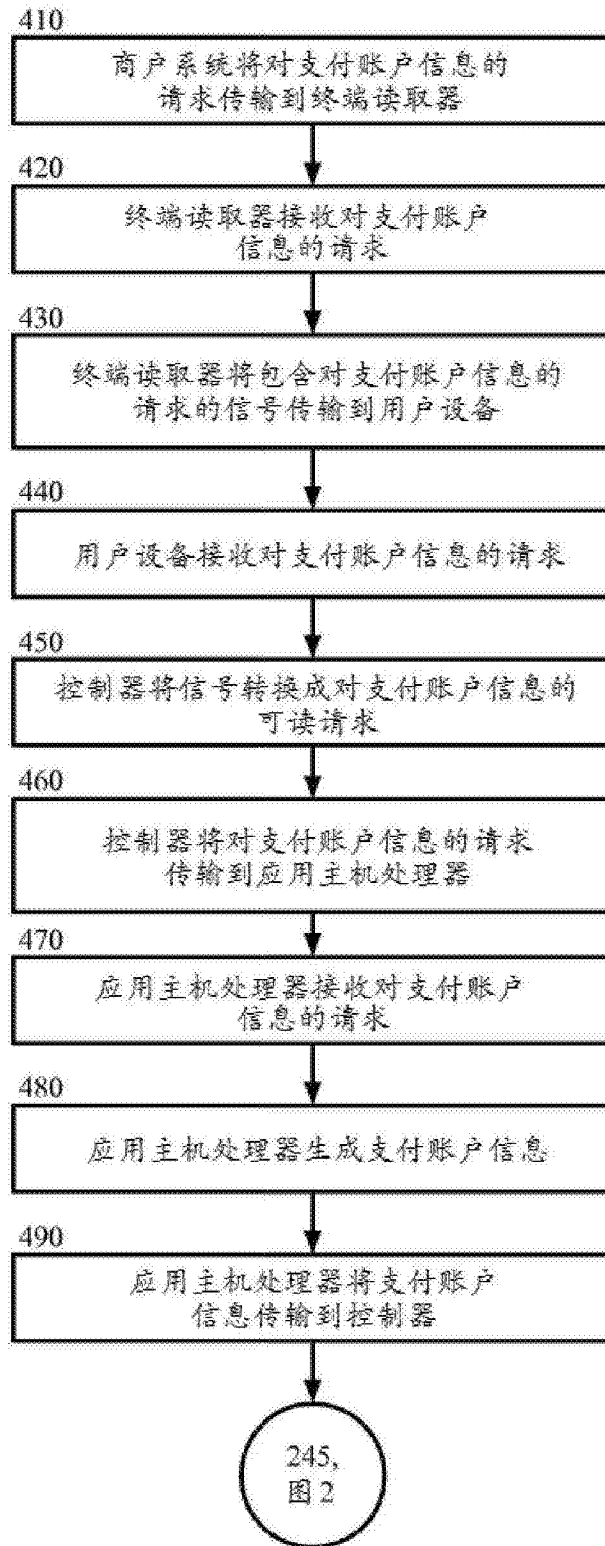


图4

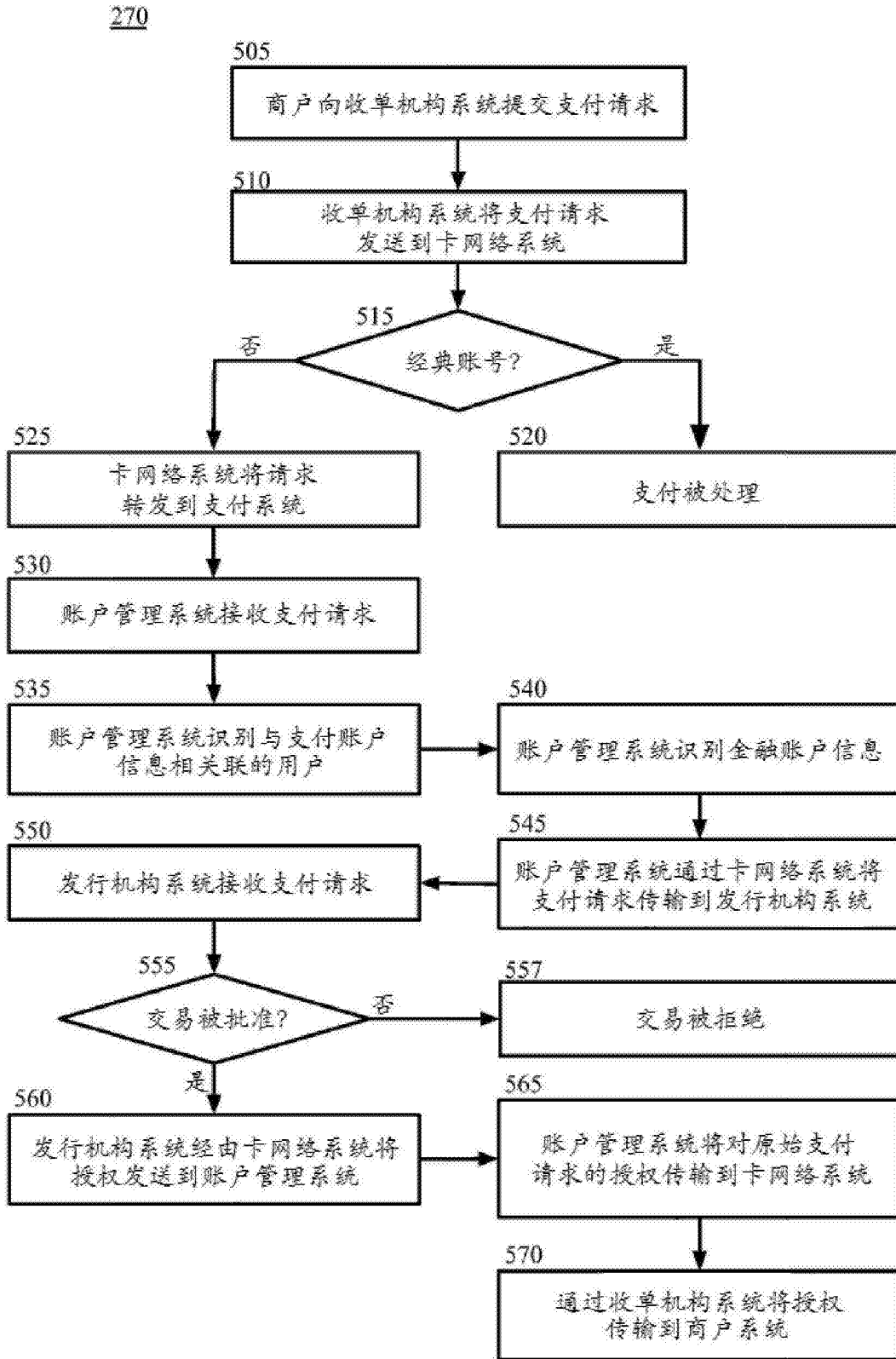


图5

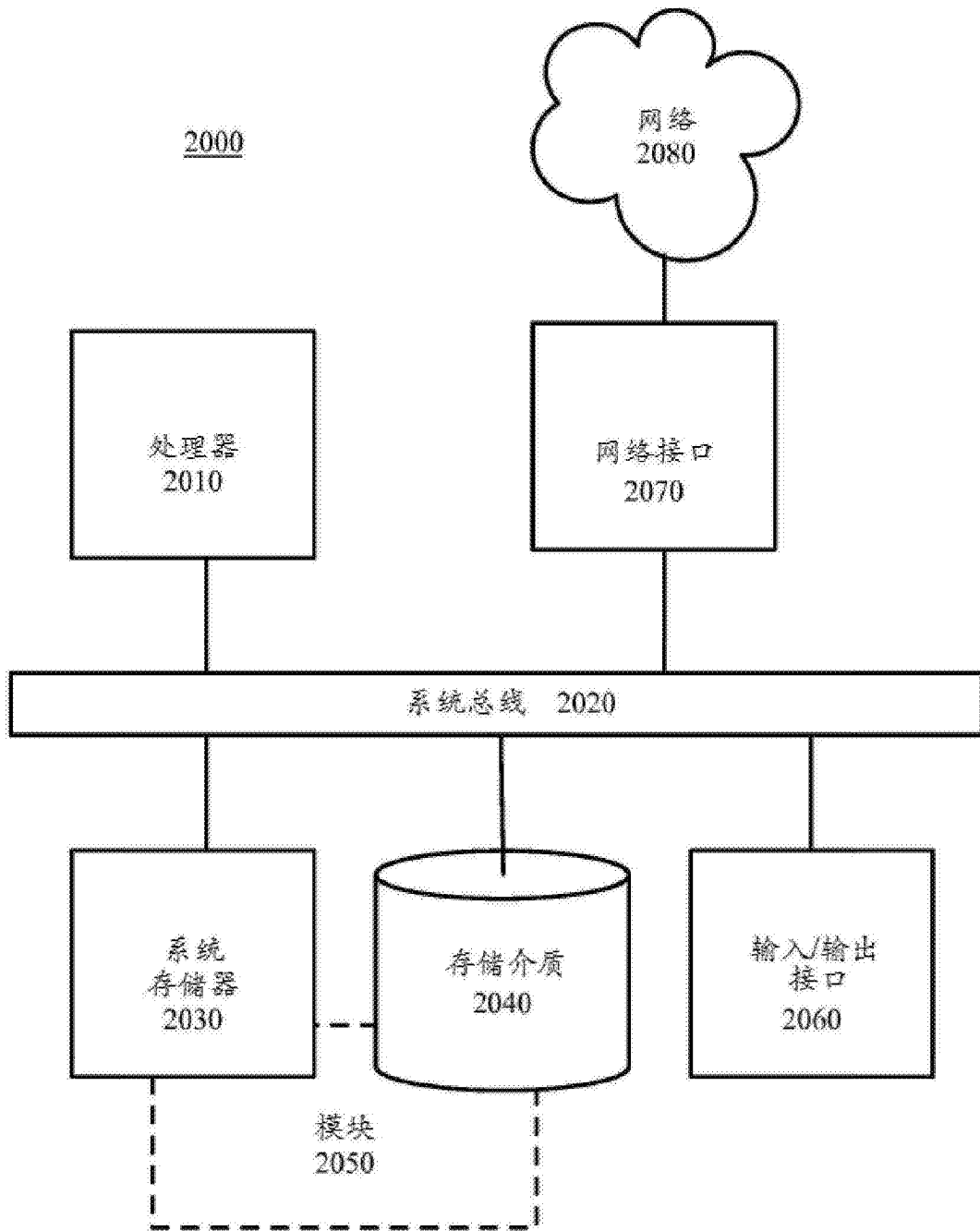


图6