(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 104040933 A
(43)申请公布日 2014.09.10

(21)申请号 201280059324.1
(22)申请日 2012.10.01
(30)优先权数据
61/541,875 2011.09.30 US
(85)PCT国际申请进入国家阶段日
2014.05.30
(86)PCT国际申请的申请数据
PCT/US2012/058371 2012.10.01
(87)PCT国际申请的公布数据
WO2013/049857 EN 2013.04.04
(71)申请人 电子湾有限公司
地址 美国加利福尼亚州
(72)发明人 丹尼尔·麦戈斯
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 李晓冬
(51)Int.Cl.
H04L 9/00(2006.01)

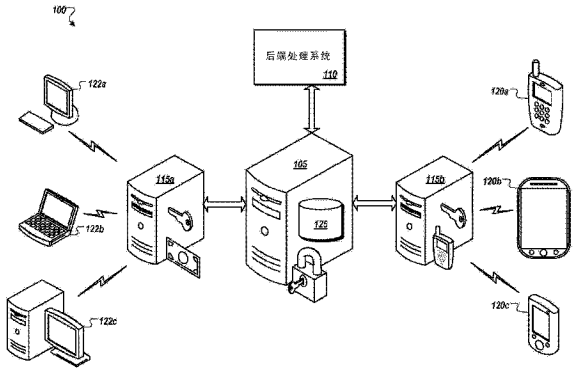
权利要求书5页 说明书18页 附图7页

(54)发明名称

源自客户端的信息的差异客户端侧加密

(57)摘要

一种方法可以包括：分配多个公钥，其中每个相应的公钥都被分配给许多实体中的相应的实体；存储多个私钥，其中每个相应的私钥都对应于相应的公钥；存储一个或多个解密算法，其中每个相应的解密算法都被配置为对使用所述加密算法中的至少一个加密算法先前加密的数据进行解密。每个相应的加密算法都可以被配置为使用至少一个公钥来对数据进行加密。每个相应的解密算法都可以被配置为使用至少一个私钥来对数据进行解密。所述方法可以包括接收加密的数据，其中所述加密的数据使用第一公钥和第一加密算法被加密，并且所述加密的数据通过网络来提供。



CN 104040933 A

1. 一种方法，包括：

接收由服务提供商分配以供实体使用的公钥，其中所述服务提供商维护与所述公钥配对的私钥；

由第一计算设备的处理器来确定包括所述公钥的交互程序；

为终端用户提供所述交互程序，其中所述交互程序被配置为使得第二计算设备的处理器能够使用所述公钥对数据进行加密，其中所述第二计算设备被所述终端用户控制；

跨越第一网络从所述第二计算设备接收加密的数据，其中所述第二计算设备的处理器已使用所述公钥对所述加密的数据进行加密；

跨越第二网络将所述加密的数据转发到所述服务提供商，其中所述服务提供商被配置为确定所述私钥并且对所述加密的数据进行解密，并且

所述第一计算设备无法访问经解密的数据；以及

从所述服务提供商接收与所述加密的数据的解密相关的处理结果。

2. 如权利要求 1 所述的方法，其中

所述交互程序是移动计算设备应用；以及

所述第二计算设备是移动计算设备，其中所述移动计算设备应用可配置为安装在所述第二计算设备的处理器上。

3. 如权利要求 1 所述的方法，其中所述交互程序包含指令，当被执行时，所述指令使所述第二计算设备的处理器使用所述公钥对数据进行加密。

4. 如权利要求 3 所述的方法，其中所述交互程序包含指令，当被执行时，所述指令进一步使所述第二计算设备的处理器从所述实体和所述服务提供商中的一个下载加密子程序。

5. 如权利要求 1 所述的方法，其中所述交互程序包括能够在互联网浏览器应用内被呈现的指令。

6. 如权利要求 1 所述的方法，进一步包括将结果信息提供给所述第二计算设备，其中所述结果信息被配置为呈现在所述第二计算设备的显示屏上。

7. 一种方法，其包括：

接收一个或多个加密算法和公钥，其中

所述第一或多个加密算法被配置为使用所述公钥对数据进行加密以获得加密的数据，其中所述加密的数据被配置为使用与所述公钥配对的私钥来被解密，并且

所述一个或多个加密算法和所述公钥由服务提供商通过网络来提供，其中

所述服务提供商分配了所述公钥以供实体使用，并且

所述服务提供商存储所述私钥；

由第一计算设备的处理器来生成包括所述一个或多个加密算法和所述公钥的移动设备应用；

提供所述移动设备应用以供通过所述网络下载；

接收加密的数据，其中所述数据由移动计算设备的处理器通过所述一个或多个加密算法和所述公钥来加密，其中所述移动设备应用被安装在所述移动计算设备上；

将所述加密的数据转发到第二计算设备，其中

所述第二计算设备被所述服务提供商控制，并且

所述服务提供商被配置为：

对所述加密的数据进行解密以获得解密的数据，并且

管理所述解密的数据的处理以获得处理结果；以及

从所述第二计算设备接收所述处理结果。

8. 如权利要求 7 所述的方法，进一步包括：

由第三计算设备的处理器来生成结果信息，其中所述结果信息是基于所述处理结果的；以及

经由所述网络将所述结果信息提供给执行在所述移动计算设备上的所述移动设备应用。

9. 如权利要求 8 所述的方法，其中所述第一计算设备是所述第三计算设备。

10. 如权利要求 7 所述的方法，进一步包括：

将处理类型的指示提供给所述第二计算设备，其中所述处理类型与所述加密的数据相关联，以及

所述服务提供商基于所述处理类型来管理所述解密的数据的处理。

11. 一种方法，包括：

由第一计算设备的处理器来分配多个公钥，其中所述多个公钥中的每个相应的公钥被分配给多个实体中的相应的实体；

将多个私钥存储在所述第一计算设备的存储器中，其中所述多个私钥中的每个相应的私钥都对应于所述多个公钥中的相应的公钥；

将一个或多个解密算法存储在所述第一计算设备的存储器中，其中

所述一个或多个解密算法中的每个相应的解密算法都被配置为对使用一个或多个加密算法中的至少一个加密算法先前加密的数据进行解密，其中所述一个或多个加密算法中的每个相应的加密算法都被配置为使用所述多个公钥中的至少一个公钥来对数据进行加密，并且

所述一个或多个解密算法中的每个相应的解密算法都被配置为使用所述多个私钥中的至少一个私钥来对数据进行解密；

接收解密的数据，其中

所述解密的数据使用所述多个公钥中的第一公钥和所述一个或多个加密算法中的第一加密算法被加密，并且

所述加密的数据通过网络来提供；

由所述第一计算设备的处理器来确定所述多个私钥中的第一私钥，其中

所述第一私钥对应于所述第一公钥，并且

所述第一公钥被分配给所述多个实体中的第一实体；

由所述第一计算设备的处理器使用所述第一私钥和所述一个或多个解密算法中的至少一个解密算法来对所述加密的数据进行解密，其中

解密的数据通过对所述加密的数据进行解密来获得；

提供所述解密的数据的一部分以供处理引擎处理，其中第二计算设备包括所述处理引擎；

接收由所述处理引擎所生成的处理结果，其中所述处理结果与所述解密的数据的部分相关；以及

通过所述网络将所述处理结果提供给所述第一实体。

12. 如权利要求 11 所述的方法，进一步包括：在提供所述解密的数据的部分以供所述处理引擎处理之前，由所述第一计算设备的处理器对用于处理的所述解密的数据进行排队。

13. 如权利要求 11 所述的方法，进一步包括在接收所述加密的数据之前：

接收针对所述第一加密算法的下载请求，其中所述下载请求跨越所述网络从第三计算设备被接收；以及

经由所述网络将所述第一加密算法提供给所述第三计算设备。

14. 如权利要求 13 所述的方法，其中所述下载请求包括超文本传输协议请求。

15. 如权利要求 13 所述的方法，进一步包括：

将所述一个或多个加密算法作为一个或多个加密子程序存储在所述第一计算设备的存储器中，其中

提供所述第一加密算法包括提供所述一个或多个加密子程序中的第一加密子程序，其中所述第一加密子程序包括所述第一加密算法。

16. 如权利要求 15 所述的方法，其中所述第一加密子程序包括运行时解释指令。

17. 如权利要求 11 所述的方法，进一步包括将所述解密的数据和所述加密的数据中的至少一个存储在所述第一计算设备可访问的存储档案中。

18. 如权利要求 11 所述的方法，进一步包括：

通过所述网络接收未加密的数据，其中所述未加密的数据与所述加密的数据相关；以及

提供所述未加密的数据的一部分以供所述处理引擎处理，其中所述未加密的数据的一部分中提供有所述解密的数据的一部分。

19. 如权利要求 11 所述的方法，进一步包括通过所述网络接收将对所述解密的数据执行的处理的类型的指示，其中所述处理的类型的指示由被所述第一实体所控制的第三计算设备来提供。

20. 如权利要求 19 所述的方法，其中所述处理的类型包括信用卡授权和背景检查中的至少一个。

21. 如权利要求 19 所述的方法，其中所述加密的数据包括信用卡信息、医疗历史信息、社会保障号、银行账户号以及驾驶执照号中的一个或多个。

22. 如权利要求 11 所述的方法，其中

所述加密的数据通过所述网络从被所述第一实体所控制的第三计算设备来提供；并且

所述第一实体能够对所述加密的数据进行解密。

23. 一种方法，其包括：

将一个或多个加密算法存储在第一计算设备的存储器中；

将所述一个或多个加密算法中的第一加密算法提供给跨越网络的请求者；

将一个或多个解密算法存储在所述第一计算设备的存储器中，其中

所述一个或多个解密算法中的每个相应的解密算法都被配置为对使用所述一个或多个加密算法中的至少一个加密算法先前加密的数据进行解密；

接收处理请求，其中所述处理请求包括加密的数据、非加密的数据以及要被执行的处

理的类型的指示，其中

所述处理请求通过网络从由实体所控制的第二计算设备来提供，并且

所述加密的数据使用所述第一加密算法被加密；

由所述第一计算设备的处理器来确定所述加密的数据与所述实体相关联；

由所述第一计算设备的处理器来确定所述一个或多个解密算法中的第一解密算法；

由所述第一计算设备的处理器使用所述第一解密算法对所述加密的数据进行解密，其中

解密的数据通过对所述加密的数据进行解密来获得；

由所述第一计算设备的处理器来确定被配置为使用所述处理的类型来处理所述解密的数据的处理引擎；

经由第二网络将所述解密的数据的一部分和所述未解密的数据的一部分提供给第三计算设备，其中

所述第三计算设备包括所述处理引擎；

从所述第三计算设备接收处理结果；以及

将所述处理结果提供给所述第二计算设备。

24. 如权利要求 23 所述的方法，其中所述第一加密算法是非对称加密算法。

25. 如权利要求 24 所述的方法，进一步包括：

由所述第一计算设备的处理器将公钥分配给所述实体；

将所述公钥提供给所述第二计算设备，其中所述加密的数据使用所述公钥被加密；并且

将私钥存储在所述第一计算设备的存储器中，其中

所述私钥与所述公钥配对，以及

对所述加密的数据进行解密包括使用所述私钥进行解密。

26. 一种方法，其包括：

将一个或多个加密算法作为一个或多个加密子程序存储在第一计算设备的存储器中；

通过网络接收针对所述一个或多个加密子程序中的第一加密子程序的下载请求；

通过所述网络提供所述第一加密子程序；

通过所述网络接收处理请求，其中

所述处理请求包括加密的数据，其中所述加密的数据使用所述第一加密子程序被加密；

由所述第一计算设备的处理器来确定所述加密的数据与所述实体相关联；

由所述第一计算设备的处理器来确定第一解密算法，其中所述第一解密算法被配置为对所述加密的数据进行加密；

由所述第一计算设备的处理器来使用所述第一解密算法对所述加密的数据进行解密，其中解密的数据通过对所述加密的数据进行解密来获得；

由所述第一计算设备的处理器来确定用于处理所述解密的数据的处理引擎；

通过第二网络将所述解密的数据的一部分提供给第二计算设备，其中

所述第二计算设备包括所述处理引擎；

从所述第二计算设备接收处理结果；以及

跨越所述网络将所述处理结果提供给第三计算设备，其中所述第三计算设备被所述实体所控制。

27. 如权利要求 26 所述的方法，其中所述处理请求被从所述第三计算设备接收。

28. 如权利要求 26 所述的方法，其中所述处理结果包括批准和拒绝中的至少一个的指示。

29. 如权利要求 26 所述的方法，其中所述下载请求被从由终端用户所控制的第四计算设备接收，其中所述第四计算设备不同于所述第二计算设备和所述第三计算设备。

源自客户端的信息的差异客户端侧加密

[0001] 相关申请

[0002] 本申请要求于2011年9月30日提交的题为“Systems and Methods for Differential Client-Side Encryption of Information Originating from a Client”的美国临时申请No.61/541,875的优先权，其全部内容通过引用结合于此。

[0003] 背景

[0004] 诸如个人数据和其它敏感信息的信息可以通过例如网络，诸如互联网传递以提供凭证信息，付款信息或者个人账户管理信息。为保护敏感信息，信息可以通过安全传输连接，诸如传输层安全（TLS）或安全套接层（SSL）来传输。

[0005] 为保护信息面授非法审查，信息可以数字加密。数字加密的一个示例是公钥密码。在公钥密码方案中，两个分离的但是算数上连接的秘钥（例如，数值）被用来保护信息。首先，公钥被用来使用加密算法加密数据。其次，公钥被用来使用数据接收器来解密加密信息。接收器向发送器提供公钥，使得发送器能够安全地将信息发送到接收器。

[0006] 敏感信息的接收器有义务好不用户的隐私免受对敏感信息的非法访问。如果信息是保密的（例如只是仅有指定方本该访问的信息的工业和/或专业标准），则信息是敏感的。如果一方因为信息暴露而承担处理信息的监管义务，则信息是敏感的。如果一方由于信息处理和/或信息暴露而招致潜在义务，信息可以是敏感的。

[0007] 在某些情况下，敏感信息的接收器可以从用户请求，不由请求者使用，但是由诸如信用卡系统或健康保险授权系统的第三方处理的敏感信息。存在对于能够使得敏感信息在没有请求者访问传输内容的情况下通过访问者的系统传输的方法和设备的要求。如果请求者不能提出和/或解释敏感信息，请求者可以避免保护敏感信息的义务。

发明内容

[0008] 在一个方面，本公开内容涉及包括通过第一计算设备的处理器来分配许多公钥的方法，其中许多公钥中的每个相应的公钥都被分配给许多实体中的相应的实体。所述方法可以包括将许多私钥存储在第一计算设备的存储器中，其中许多私钥中的每个相应的私钥都对应于许多公钥中的相应的公钥。所述方法可以包括将一个或多个解密算法存储在第一计算设备的存储器中，其中所述一个或多个解密算法中的每个相应的解密算法都被配置为对使用一个或多个加密算法中的至少一个加密算法先前加密的数据进行解密。所述一个或多个加密算法中的每个相应的加密算法都可以被配置为使用许多公钥中的至少一个公钥来对数据进行加密。所述一个或多个解密算法中的每个相应的解密算法都可以被配置为使用许多私钥中的至少一个私钥来对数据进行解密。所述方法可以包括接收加密的数据，其中加密的数据使用许多公钥中的第一公钥和所述一个或多个加密算法中的第一加密算法被加密，并且加密的数据通过网络来提供。所述方法可以包括通过第一计算设备的处理器来确定许多私钥中的第一私钥，其中第一私钥对应于第一公钥，并且第一公钥被分配给许多实体中的第一实体。所述方法可以包括通过第一计算设备的处理器来使用第一私钥和所述一个或多个解密算法中的至少一个解密算法来对加密的数据进行解密，其中解密的数据

通过对加密的数据进行解密来获得。所述方法可以包括提供所述解密的数据的一部分以供处理引擎处理，其中第二计算设备包括处理引擎。所述方法可以包括接收由处理引擎所生成的处理结果，其中处理结果涉及所述解密的数据的部分。所述方法可以包括通过网络来将处理结果提供给第一实体。

[0009] 在一些实施例中，所述方法可以进一步包括，在提供所述解密的数据的部分以供处理引擎处理之前，通过第一计算设备的处理器来对用于处理的解密的数据进行排队。

[0010] 所述方法可以进一步包括：在接收加密的数据之前，接收对第一加密算法的下载请求，其中下载请求跨越网络被从第三计算设备接收；以及经由网络将第一加密算法提供给第三计算设备。下载请求可以包括超文本传输协议请求。所述方法可以包括将一个或多个加密算法作为一个或多个加密子程序存储在第一计算设备的存储器中，其中提供第一加密算法包括提供所述一个或多个加密子程序中的第一加密子程序，其中第一加密子程序包括第一加密算法。第一加密子程序可以包括运行时解释的指令。

[0011] 在一些实施例中，所述方法可以包括将所述解密的数据和所述加密的数据中的至少一个存储在第一计算设备可访问的存储档案中。所述方法可以包括：通过网络接收未加密的数据，其中未加密的数据与加密的数据相关；以及提供未加密的数据的一部分以供处理引擎处理，其中未加密的数据的部分提供有所述解密的数据的部分。

[0012] 在一些实施例中，所述方法可以进一步包括通过网络接收待对加密的数据执行的处理的类型的指示，其中处理的类型的指示通过由第一实体所控制的第三计算设备来提供。处理的类型可以包括信用卡授权和后端检查中的至少一个。加密的数据可以包括信用卡信息、医疗历史信息、社会安全号、银行账号以及驾驶执照号中的一个或多个。加密的数据可以通过网络从由第一实体所控制的第三计算设备来提供，并且第一实体也许不能对加密的数据进行加密。

[0013] 在一个方面，本公开内容描述了包括以下各项的方法：将一个或多个加密算法存储在第一计算设备的存储器中；跨越网络将一个或多个加密算法中的第一加密算法提供给请求者；以及将一个或多个解密算法存储在第一计算设备的存储器中，其中所述一个或多个解密中的每个相应的加密算法都被配置为对使用所述一个或多个加密算法中的至少一个加密算法先前加密的数据进行解密。所述方法可以包括接收处理请求，其中处理请求包括加密的数据、非加密的数据以及要被执行的处理的类型的指示，其中处理请求通过网络从由实体所控制的第二计算设备来提供，并且加密的数据使用第一加密算法被加密。所述方法可以包括：通过第一计算设备的处理器来确定加密的数据与实体相关联；通过第一计算设备的处理器来确定所述一个或多个解密算法中的第一解密算法；通过第一计算设备的处理器来使用第一解密算法对加密的数据进行解密，其中解密的数据通过对加密的数据进行解密来获得；通过第一计算设备的处理器来确定被配置为使用处理的类型来处理解密的数据的处理引擎；以及经由第二网络将解密的数据的一部分和未解密的数据的一部分提供给第三计算设备，其中第三计算设备包括处理引擎。所述方法可以包括从第三计算设备接收处理结果，以及将处理结果提供给第二计算设备。

[0014] 在一些实施例中，第一加密算法可以是非对称加密算法。所述方法可以进一步包括：通过第一计算设备的处理器来将公钥分配给实体；将公钥提供给第二计算设备，其中加密的数据使用公钥被加密；以及将私钥存储在第一计算设备的存储器中。私钥可以与公

钥配对，并且对加密的数据进行解密可以包括使用私钥进行解密。

[0015] 在本公开内容的一个方面，方法可以包括：将一个或多个加密算法作为一个或多个加密子程序存储在第一计算设备的存储器中；经由网络接收对所述一个或多个加密子程序中的第一加密子程序的下载请求；经由网络提供第一加密子程序；以及经由网络接收处理请求，其中处理请求包括加密的数据，其中加密的数据使用第一加密子程序被加密。所述方法可以包括：通过第一计算设备的处理器来确定加密的数据与实体相关联；通过第一计算设备的处理器来确定第一解密算法，其中第一解密算法被配置为对加密的数据进行加密；通过第一计算设备的处理器来使用第一解密算法对加密的数据进行解密，其中解密的数据通过对加密的数据进行解密来获得；所述方法可以包括：通过第一计算设备的处理器来确定用于处理解密的数据的处理引擎；经由第二网络将解密的数据的一部分提供给第二计算设备，其中第二计算设备包括处理引擎；从第二计算设备接收处理结果；以及跨越网络将处理结果提供给第三计算设备，其中第三计算设备被实体控制。

[0016] 可以从第三计算设备接收处理请求。处理结果可以包括批准和拒绝中的至少一个的指示。可以从由终端用户所控制的第四计算设备接收下载请求，其中第四计算设备不同于第二计算设备和第三计算设备。

[0017] 在一个方面，本公开内容描述了一种方法，其包括：接收由服务提供商分配以供实体使用的公钥，其中服务提供商维护与公钥配对的私钥；通过第一计算设备的处理器来确定包括公钥的交互程序；为终端用户提供交互程序，其中交互程序被配置为使得第二计算设备的处理器能够使用公钥来对数据进行加密，其中第二计算设备被终端用户控制；所述方法可以包括：跨越第一网络从第二计算设备接收加密的数据，其中第二计算设备的处理器使用公钥对加密的数据进行加密了；跨越第二网络将加密的数据转发到服务提供商，其中服务提供商被配置为确定私钥并且对加密的数据进行加密，以及第一计算设备无法访问未加密的数据；以及从服务提供商接收与加密的数据的解密相关的处理结果。

[0018] 交互程序可以是移动计算设备应用，并且第二计算设备可以是移动计算设备，其中移动计算设备应用被配置为安装在第二计算设备的处理器上。

[0019] 交互程序可以包含指令，所述指令当被执行时，使第二计算设备的处理器使用公钥来对数据进行加密。交互程序可以包含指令，所述指令当被执行时，使第二计算设备的处理器从实体和服务提供商中的一个下载加密子程序。交互程序可以包括能够在互联网浏览器应用内被呈现的指令。所述方法可以进一步包括将结果信息提供给第二计算设备，其中结果信息被配置用于呈现在第二计算设备的显示屏上。

[0020] 在一个方面，本公开内容描述了包括接收一个或多个加密算法和公钥的方法，其中一个或多个加密算法被配置为使用公钥来对数据进行加密以获得加密的数据，其中加密的数据被配置为使用与公钥配对的私钥被解密，并且一个或多个加密算法和公钥由服务提供商通过网络来提供，其中服务提供商分配了公钥以供实体使用，并且服务提供商存储私钥。所述方法可以包括：通过第一计算设备的处理器来生成包括所述一个或多个加密算法和公钥的移动设备应用；提供移动设备应用以供通过网络下载；以及接收加密的数据，其中数据由移动计算设备的处理器通过一个或多个加密算法和公钥被加密，其中移动设备应用被安装在移动计算设备上。所述方法可以包括将加密的数据转发到第二计算设备，其中第二计算设备被服务提供商控制，并且服务提供商被配置为对加密的数据进行解密以获得

解密的数据，以及管理所述解密的数据的处理以获得处理结果。所述方法可以包括从第二计算设备接收处理结果。

[0021] 在一些实施例中，所述方法可以进一步包括：通过第三计算设备的处理器来生成结果信息，其中结果信息是基于处理结果的；以及经由网络将结果信息提供给在移动计算设备上执行的移动设备应用。第一计算设备可以是第三计算设备。

[0022] 所述方法可以进一步包括将处理类型的指示提供给第二计算设备，其中处理类型与加密的数据相关联，并且服务提供商基于处理类型来管理解密的数据的处理。

附图说明

[0023] 通过参考一下说明并结合附图，本公开的上述和其它目的、方面、特征和优点将更加明显和容易理解，其中：

[0024] 图 1 是用于实现源自客户的信息的客户端加密的示例系统的框图；

[0025] 图 2A 是用于在支付处理环境中实现源自客户的信息的客户端加密的示例系统的框图；

[0026] 图 2B 是通过系统（诸如图 2A 的系统）实现客户端加密的示例操作流程的泳道图；

[0027] 图 3 是用于提供和使用实现信息的客户端加密的无线计算设备应用的示例操作流程的泳道图；

[0028] 图 4 是用于实现源自客户的信息的客户端加密的示例方法的流程图；

[0029] 图 5 是用于采集和操纵销售点的交易数据的示例网络环境的框图；

[0030] 图 6 是计算设备和移动计算设备的框图。

[0031] 根据与附图相结合的下述详细说明，本公开的特征和优点将变得明显，其中在相同的标符自始至终标识相应的元件。在附图中，相同的标号通常指示相同的，功能相似的和 / 或结构相似的元件。

具体实施方式

[0032] 中间方可以从终端用户接收信息。中间方可以将至少一部分信息传递到后端服务提供商进行处理。对信息的访问和 / 或暴露可能引起中间方的潜在义务。

[0033] 总的来说，本公开的系统和方法使得实体能够从终端用户获得信息，并且在不暴露潜在净荷信息的情况下将至少一部分信息传递给后端服务提供商。实体或中间方可以使得由终端用户操作的计算设备来加密传输之前的信息。实体可以通过中间方将加密信息发送到后端服务提供商，其中信息可能被解密。因为实体和中间方接受加密信息，而非可解释的，可由人呈现的和 / 或明文信息，实体可以向终端用户保证信息是安全的。类似地，中间方可以向后端服务提供商保证信息是安全的。此外，由于有关加密信息的存储的安全风险可能较低，实体和 / 或中间方可以存储信息以异步处理从终端用户接收的信息。总的来说，与中间方合作的实体可以通过实体自身成员，可以访问实体或中间方的系统的第三方来减轻不希望的暴露接收的信息的风险，以及利用获得的安全性来管理信息处理。

[0034] 在一些示例中，本公开的系统和方法可以被部署以用于支付系统。支付系统（例如中间方服务器）可以从实体接收加密的信用卡信息，诸如信用卡号和信用校验值 (CVV)，

以及与信用卡公司核实卡号的用户被授权从实体进行购买。因为实体无法访问，解释或者呈现信用卡信息（例如，作为文本信息等），实体可以将加密的信息存储在长期存储器（例如光盘，硬驱动）中，并且依然符合由诸如支付卡行业（PCI）数据安全标准（DSS）的标准所述的某些要求。在一些示例中，本公开的系统和方法可以在健康保险系统中部署，从而使得保密病人信息在电子系统间安全地传递。本公开的系统和方法可以针对背景调查服务被部署。背景核对所需的保密信息，诸如个人社会保障号可以在电子系统间安全的传递，直到信息到达授权用户。本文中所面熟的系统和方法的应用并于限于上述示例，但是可以在任意数量的环境中部署，如将被本领域技术人员所理解的。背景的内容不被认为是作为现有技术的内容的许可。

[0035] 现在参考图 1，示出并描述了用于实现源自客户的信息的客户端加密的系统 100。系统 100 包括与后端处理系统 110 通信的中间方服务器 105。中间方服务器 105 可以与实体服务器 115a、115b（统称为 115）通信。每个实体服务器 115 可以与由终端用户操作的客户端计算设备，诸如移动计算设备 120a、120b、120c 和个人计算设备 122a、122b 和 122c 通信。

[0036] 在操作中，实体可以通过中间方持有账户。在一些实现方式中，中间方可以提供对可以由计算设备上的处理器执行的安全性相关子程序的库 125 的访问。库 125 可以包括用在可以用于传输敏感信息的客户端计算设备 120、122 上的加密子程序。子程序的库 125 可以位于中间方服务器 105 上或者与其相关联。当登陆其账户时，实体服务器 115 可以访问库 125。在一些实现方式中，实体服务器 115 可以通过其账号获得子程序的库 125 的备份。实体可以将库 125 的备份存储在其相应的实体服务器 115 上。

[0037] 在一些实现方式中，子程序的库 125 可以是 Javascript 库，虽然可以使用具有其它编程语言的子程序的库。在一些实现方式中，库 125 的子程序可以在 web 浏览器，诸如加州的 Mozilla Corporation of Mountain View 提供的 Mozilla Firefox™，加州的 Google, Inc. of Mountain View 提供的 Google Chrome™，或者加州的 Apple Inc. of Cupertino 提供的 Safari™ 中执行。在一些实现方式中，库 125 的子程序可包括在由实体提供以用于用户安装的移动设备应用中（例如智能手机、平板电脑或其它移动计算设备）。

[0038] 在一些实现方式中，每个实体账户可以包括可以和非对称加密算法（例如 RSA、Diffie-Hellman 秘钥交换协议（DSS）、数字签名标准、ElGamal、Paillier）一起使用的密钥对的公钥（public key）的备份。公钥作为基数 64 编码串，十六进制编码串或任何其它格式可以是可用的。实体可以将公钥备份到任何实体可以使用的计算机程序中。在一些实现方式中，当实体通过中间方打开账户时，中间方服务器 105 可以将公钥备份传送到相应的实体服务器 115。

[0039] 在操作中，在一些实现方式中，在客户端设备 120、122 处的用户可以访问与实体相关联的 web 站点。用户可以访问与实体的 web 站点相关联的统一资源定位符（URL）。客户计算设备 120、122 可以通过计算机网络做出超文本传输协议（HTTP）请求来访问 web 站点。

[0040] 作为响应，实体服务器 115 可以将 web 页面传输到客户计算设备 120、122 进行显示。客户计算设备 120、122 可以使用 web 浏览器来观看 web 页面。web 页面可以包括超文本标记语言（HTML）。

[0041] 在一些实现方式中，实体的 web 页面可以包括表格。表格可以包括接受来自客户计算设备 120、122 的用户的信息的字段。在一些实现方式中，一部分字段被配置为接收诸如用户账单地址、信用卡号、信用卡到期日和 / 或信用卡安全码（例如信用校验值，或 CVV）的信息。在一些实现方式中，一部分字段被配置为接收诸如用户家庭地址，出生日期，驾驶执照号和社会安全码的信息。在一些实现方式中，部分字段被配置为接收与个人健康历史相关的信息。在一些实现方式中，部分字段被配置为接收诸如用户姓名、账号密码和联系人信息（例如邮寄地址、e-mail 地址、手机号）的信息。

[0042] 在一些实现方式中，一个或多个字段可以被配置为接收敏感信息。如果信息是保密的（例如只是仅有指定方本该访问的信息的工业和 / 或专业标准），则信息是敏感的。如果一方因为信息暴露而承担处理信息的监管义务，则信息是敏感的。如果一方由于信息处理和 / 或信息暴露而招致潜在义务，信息可以是敏感的。

[0043] Web 页面可以标识被配置为接收敏感信息的字段，从而标识接收到的信息应该被加密的字段。在一些实现方式中，web 页面可以包括被配置为接收敏感信息的 HTML 标识字段。在一些实现方式中，web 页面可以包括脚本标签。脚本标签可以识别加密相关的 web 页面可以使用的子程序的库 125 以及库 125 的位置。Web 页面可以包括由中间方服务器 105 提供的公钥的备份。

[0044] Web 页面可以包括用户可以激活的控制以将表格字段中提供的信息提交给实体服务器 115（例如，“提交”按钮）的控制。库 125 的处理子程序可以响应于提交控制的激活开始在客户端计算设备 120、122 上的 web 浏览器中执行。该处理子程序可以挂钩到 web 页面的提交处理中。

[0045] 在一些实现方式中，处理子程序可以从随机数生成器（例如通过开放资源库可用的生成器）获得值。处理子程序可以处理该值以获得和对称加密算法，诸如高级加密标准 (AES) 或数据加密标准 (DES) 一起使用的加密秘钥。Web 页面可以访问库 125 的加密子程序以使用加密秘钥（这里也称作“对称加密秘钥”）加密可以接收敏感信息的字段内的值。

[0046] 在一些实现方式中，web 页面可以包括具有相同字段的两个表格。一个表格可以对用户隐藏（例如，没有显示）。隐藏表格中的信息可以是将要传输到实体服务器 115 的信息。显示的表格中的 HTML 可以指示字段是否被配置为接收敏感信息。处理子程序可以分析 HTML 以识别字段值用于加密。如果字段未被配置为接收敏感信息，字段中的值可以备份到隐藏表格的对应字段中。如果字段被配置为敏感信息，字段中的值可以被加密，并且加密的值可以被插入到隐藏表格的相应字段中。在一些实现方式中，客户端计算设备 120、122 的用户可能没有发现键入的值变化成其加密的相对物，这可以避免用户的部件上的警报或混淆。

[0047] 在一些实现方式中，web 页面可以包括单个表格。该表格可以具有于接收敏感信息的字段相对应的隐藏字段。在一些实现方式中，只有一个隐藏字段或者其对应的可见字段可以被激活（例如，如果可见字段是激活的，则隐藏字段不可以被配置为接收值，反之亦然）。库 125 的加密子程序可以加密接收敏感信息的字段中的值。处理子程序可以取消激活字段，激活相应的隐藏字段，并且将加密值插入隐藏字段中。可见字段可以以例如灰色出现。在一些实现方式中，客户端计算设备 120、122 用户可能没有发现键入的值变化成其加密的相对物。

[0048] 在一些实现方式中，web 页面可以包括可以被隐藏和 / 或禁用的表格。Web 页面可以包括可以显示和 / 或实现表格的代码。在一些实现方式中，如果客户端计算设备 120、122 上的 web 浏览器不能执行显示和 / 或实现隐藏表格的代码（例如不能运行 Javascript），表格可以保持隐藏和 / 或禁用。在一些实现方式中，不能执行特定编程语言的代码的 web 浏览器可能不能够接收用户通过其键入敏感信息（例如，信用卡号）的 web 页面。在一些实现方式中，web 页面可以包括指示要求执行特定编程语言的能力的 noscript 标签。

[0049] 库 125 的加密子程序可以根据非对称加密算法（例如，RSA）加密对称加密秘钥。加密子程序可以通过接收 web 页面内的秘钥被配置。web 页面可以发送对称加密秘钥到将使用公钥加密的加密子程序。

[0050] Web 页面可以编码字段的加密值，字段的非加密值，以及加密的对称加密秘钥。在一些实现方式中，web 页面可以通过将信息序列化来编码信息。用于序列化的示例格式包括基数 54 或十六进制（基数 16），虽然可以使用其它格式。客户端计算设备 120、122 可以将信息发送到实体服务器 115。

[0051] 在其它操作中，客户端计算设备 122（例如，移动设备）可以下载和安装包括用于将用户信息和其它数据提供给实体服务器 115 中的一个的算法的移动设备应用。例如，用户可以下载移动设备应用以从维护实体服务器 115 的特定批发商实体购买产品。在此情况下，移动设备应用可以包括用于加密敏感信息以传输到实体服务器 115 的一个或多个算法（如上所述，与基于 web 浏览器的模型相关）。例如，移动设备应用可以包括分配给中间服务器 105 的（例如库 125 的）批发商的公钥和 / 或加密算法。在其它实施方式中，移动设备应用可以包含用于从中间方服务器 105 检索信息（诸如加密算法和 / 或公钥信息）的代码，诸如加密算法和 / 或公钥信息。移动设备应用可以从用户接收数据，加密信息的至少一部分，以及以和如上所述与基于浏览器的模型相关的相似的方式将信息提供给实体服务器 115。

[0052] 实体服务器 115 可以存储从客户端计算设备 120、122 接收的信息。在一些实现方式中，实体服务器 115 可以不接收可解释的，可读的和 / 或可呈现的表格（例如，明文）中的敏感信息。将加密的信息存储在永久内存中（例如，硬驱动，光盘）呈现较低的安全风险以及可以在信息安全标准中保持。因此，可以不迫使实体服务器 115 立即将信息发送到后端系统 110 进行处理。

[0053] 终端用户信息的存储可以是实现异步处理。例如，实体服务器 115 可以将加密信息排队，并且确定用户的信息可以以哪个顺序处理（例如优先权或其它度量）。因此，客户端加密将导致实体服务器 115 有更大的灵活性来管理从客户端计算设备 120、122 接收到的信息。

[0054] 实体服务器 115 可以将客户端计算设备 120、122 的信息发送到中间方服务器 105 进行处理。实体服务器 115 可以指示将对信息执行的处理的类型。在一些实现方式中，实体服务器 115 可以通过 HTTP 请求，诸如 POST 请求发送信息。在一些实现方式中，实体服务器 115 可以向中间方服务器 105 做出应用程序界面 (API) 调用。

[0055] 在一些实现方式中，实体服务器 115 可以包括可与非对称加密算法一起使用的密钥对的私钥 (private key) 的备份，其对应于中间方服务器 105 已提供给账户持有者（例如，实体服务器 115) 的公钥。中间方服务器 105 可以使用私钥解密加密的数据（例如表格

字段的值或由移动应用采集的值)。在一些实现方式中,加密的值不可以在没有私钥的情况下解密。在一些实现方式中,客户端计算设备 120、122 和实体服务器 115 均不能访问私钥。

[0056] 通过访问经由表格接收的可解释的(例如可呈现的,明文等)版本的全部信息,中间方服务器 105 可以处理信息。处理可以创建结果。在一些实现方式中,中间方服务器 105 可以与后端系统 110(例如与第三方相关联)来处理信息。

[0057] 例如,中间方服务器 105 可以与后端处理系统 110(诸如,例如信用卡公司服务器)通信,已授权信用卡号使用所请求的金额数量(例如,商品或服务的价格)。如果所使用的信用卡号由信用卡公司服务器授权,中间方服务器 105 可以将“核准”的结果返回实体服务器 115。如果该卡号未被授权,则中间方服务器 105 可以返回“拒绝”的结果。在一些实现方式中,该结果可以包括拒绝的理由(例如资金不足、无效的信用卡号、无效的 CVV)。

[0058] 在另一个示例中,中间方服务器 105 可以与后端处理系统 110 通信(诸如例如背景调查服务)以校验个人的身份。中间方服务器 105 可以解密信息。在一些实现方式中,中间方服务器 105 可以将明文的识别信息发送到用于背景调查服务的服务器。在一些实现方式中,中间方服务器 105 可以根据用于保护中间方服务器 105 和后端处理系统 110 之间的信息的加密算法来加密识别信息。

[0059] 在一些示例中,中间方服务器 105 可以将个人姓名,过去 5 年中的居住地址,社会保障号,对开账户号和驾驶执照号发送到后端处理系统 110 用于背景调查服务。后端处理系统 110 可以确定接收到的信息与个人存储在其数据库中的信息一致,并将“已证实”的结果返回到中间方服务器 105。如果接收到的信息与数据库信息不一致,背景调查服务可以返回“未证实”的结果。

[0060] 在任一这些示例中,中间 web 服务器 105 可以将来自后端处理系统 110(例如,信用卡公司服务器,背景调查服务器)的结果发送到实体服务器 115。实体服务器 115 可以发送具有结果或结果指示(例如已证实 / 未证实、已授权 / 未授权)的 web 页面以在客户计算设备 120、122 上显示。例如,实体服务器 115 可能引起报警机构提醒客户计算设备 122 该结果信息。

[0061] 实体服务器 115 可以灵活地确定应何时以及如何采集信息(例如,表格数量,经由任意给定的表格或移动信息登录页采集的信息,通过表格或者移动信息登录页共同获得的信息组织等)以及哪种信息应该被加密。在一些实现方式中,在实体服务器 115 从浏览器表格或移动应用接收到信息时,实体服务器 115 可以将另一表格发送到客户端计算设备 120、122 或者使得在移动应用内呈现另一个信息登录页面。表格或登录页面可以包含从以前发送的表格请求不同信息的不同字段。

[0062] 在 HTML 表格的情况下,表格可以包括识别可以接收敏感信息的不同字段的 HTML 标签或者编码标记。例如,实体服务器 115 可以发送向网站登记用户的表格。实体服务器 115 可以发送不同的表格以实现接收商品和 / 或服务的用户支付信息。在移动应用的情况下,数据登录页面可以被配置为标识指定接收敏感信息的信息字段。在一些实现方式中,至少一部分信息可以使用存储的数据自动填充。例如,使用 web 浏览器 cookie 采集用户数据或者从与移动设备应用相关联的用户账户检索用户数据。替换地,基于用于提供的信息(例如,用户名和密码等),表格或者移动应用数据登录字段的一部分可以通过具有存储的用户信息的实体服务器 115 自动聚集。

[0063] 现在参照图 2A，显示并描述了用于在支付处理情境下启用源于客户端的信息的差异客户端加密的示范性系统 200 的方框图。在操作中，由消费者控制的客户端计算设备 220 可用于经由网络从实体订购商品和 / 或服务。在订货时，消费者可将信息输入到 web 页面上的表格中。举例而言，表格可包括关于消费者姓名、电话号码、送货地址、账单地址、信用卡号码和信用卡验证值的栏位。

[0064] 消费者可激活控制器来将表格数据 225 提交给实体服务器 215（例如，商家服务器）。在控制器激活时，由 web 浏览器访问的加密子程序可在客户端计算设备 220 上执行。在一些实现方式中，加密子程序可将诸如信用卡号码和 / 或卡验证值之类的信息加密。在一些实现方式中，加密子程序可能不会将诸如消费者姓名、电话号码、送货地址，和 / 或账单地址之类的信息加密。

[0065] 在一些实现方式中，web 浏览器可将表格数据 225（包括非加密的消费者姓名、电话号码、送货地址，和 / 或账单地址）发送给实体服务器 215。实体服务器 215 可访问非加密的信息和 / 或将非加密的信息储存在，例如，永久存储器中。在一些实现方式中，web 浏览器可将表格数据 225 内的加密信息 230，诸如，信用卡信息发送给实体服务器 215。实体服务器 215 可访问加密信息 230 和 / 或将加密信息 230 储存在，例如，永久存储器中。在一些实现方式中，举例而言，实体服务器 215 可将加密信息 230 储存在硬盘驱动器或光盘上。

[0066] 因为实体服务器 215 缺少加密密钥来将加密信息 230 解密，所以实体服务器 215 可能不会获得加密信息 230 的纯文本值。在一些实现方式中，不能访问信用卡信息的纯文本值可使实体服务器 215 能够储存加密信息 230，而不用担心加密信息 230 可被未授权方解密并恢复。

[0067] 实体服务器 215 可将表格数据 225（包括非加密信息以及加密信息 230 的至少一部分）发送给中间方服务器 205（例如，支付网关）。中间服务器 205 可运行所订购商品和 / 或服务的交易。例如，中间服务器 205 可确定消费者是否可为商品和 / 或服务付款。中间服务器 205 可通过将加密的信用卡信息解密来由加密信息 230 恢复信用卡信息。中间服务器 205 可请求后端处理系统 210（例如，信用卡网络中的信用卡公司服务器）确定消费者是否可以使用关于订单中的数量的信用卡信息。例如，中间服务器 205 可将信用卡数据 235 转发给后端处理系统 210。在一些实现方式中，信用卡数据 235 可以经由安全信息，例如，对后端处理系统 210 加密和 / 或提供，以保护信用卡数据 235 免受未经授权的访问。

[0068] 后端处理系统 210 可接收信用卡数据 235 并分析信用卡数据 235 以确定消费者是否可以使用关于订单中的数量的信用卡信息。后端处理系统 210 可将验证结果 240a（例如，核准、拒绝等）回传给中间服务器 205。中间服务器 205 可将从后端处理系统 210 获得的验证结果 240b 转发给实体服务器 215。实体服务器 215 可使验证结果 240b 格式化以在客户端计算设备 220 上显示。例如，实体服务器 215 可提供包含验证结果 240 的 web 页面信息 245 供消费者在客户端计算设备 220 上查看。

[0069] 图 2B 是通过系统（诸如，图 2A 的系统）用于启用客户端加密的示例操作流程 250 的泳道图。操作流程 250 示出在中间服务器 205、实体服务器 215、客户端计算设备 220，和后端处理服务器 210 之间传递的示例信息，如参照图 2A 所述。在一些实现方式中，操作流程 250 可用于处理并验证在线供应商的支付信息。操作流程 250，在一些实现方式中，可用于处理并鉴定健康信息网络上的患者信息。在一些实现方式中，操作流程 250 可用于处理

并验证背景信息，以实现调查的目的。

[0070] 在一些实现方式中，操作流程 250 从通过在客户端计算设备 220 上执行的 web 浏览器访问在线实体 web 站点 (252) 开始。例如，用户可使用 web 浏览器应用程序来浏览 web 站点。用户可访问 web 站点，例如，以请求信息（例如，患者信息、背景调查信息等）。在其它示例中，用户可访问 web 站点来购买商品或服务。

[0071] 响应于访问请求表格 web 页面（例如，订单页、患者信息页、个人信息识别页等），实体服务器 215，在一些实现方式中，提供浏览器可呈现的信息，包括用于将敏感信息加密的公钥 (254)。浏览器可呈现的信息，例如，可包括可填写的表格，或包括可见表格和隐藏表格的一组可填写的表格。可填写的表格的栏位的至少一部分，例如，可被配置为接收敏感信息。

[0072] 在一些实现方式中，浏览器可呈现的信息包括用于下载由中间服务器 205 提供的加密算法的指令。在一些实现方式中，客户端计算设备 220 经由在线实体服务器 215 从中间服务器 205 下载加密算法 (256)。在其它实施方式中，客户端计算设备 220 直接从中间服务器 205 下载加密算法（图未示）。尽管被示为在接收到包括公钥的浏览器可呈现的信息之后执行，但是，在一些实现方式中（未示出），web 浏览器 220 先前可能已经从中间服务器 205 接收到加密算法。例如，客户端计算设备 220 可能在登录进入与实体服务器 215 相关联的用户账户时已经接收到加密算法。加密算法，在一些实现方式中，可能与公钥相关联。例如，中间服务器 205 可将特定加密算法与分配给特定实体的特定公钥相关联。

[0073] 在一些实现方式中，客户端计算设备 220（例如，在浏览器应用程序内执行的脚本语言或其它浏览器可执行的语言内）使用加密算法和公钥将用户数据加密 (258)。例如，加密算法可被编程到浏览器可执行的语言中，诸如，Javascript 编程语言。在一些实现方式中，加密算法识别被配置为接受敏感信息的一个或多个栏位，并将输入到那些栏位中的信息加密。

[0074] 在一些实现方式中，客户端计算设备将数据，包括加密数据传送给实体服务器 215(260a)。加密算法或另一种算法，例如，可将数据传送给实体服务器 215。加密数据，在一些实现方式中，与未加密数据分开提供给实体服务器 215（例如，独立传输）。除了加密之外，在一些实现方式中，加密的和，可选地，未加密的数据可由客户端计算设备 220 经由安全连接，诸如，安全套接层 (SSL) 连接提供给实体服务器 215。

[0075] 在一些实现方式中，实体服务器 215 将加密数据和，可选地，未加密数据（例如，识别信息，诸如，用户姓名和邮政编码）的一部分转发给中间服务器 205(260b)。在一些实现方式中，实体服务器 215 将加密数据排列，用于之后传送给中间服务器 205，而非立即转发数据。除了转发加密数据之外，在一些实现方式中，实体服务器将加密数据的副本储存在本地，例如，作为临时备份，以防对中间服务器 205 的初始请求失败或用于实现交易历史的目的。若实体服务器 215 将加密数据储存在本地，则在一些实现方式中，实体服务器 215 将信息储存在安全存储区，诸如，安全数据库内。

[0076] 在一些实现方式中，加密数据在中间服务器 205 处被解密 (262)。中间服务器 205，例如，可将在线实体与和发给实体服务器 215 的公钥配对的私钥匹配。在一些实现方式中，私钥至少部分基于实体服务器 215 的传输签名（例如，互联网协议 (IP) 地址、域名服务器 (DNS) 等）来识别。私钥，在一些实现方式中，至少部分基于来自实体服务器 215 的传输物

内所含的标头信息来识别。例如，传输算法可将识别信息嵌入到由实体服务器 215 提供给中间服务器 205（例如，步骤 260b 中）的传输物内。在一些实现方式中，公钥自身或识别公钥的识别符与加密信息一起传送。

[0077] 在将加密信息解密时，在一些实现方式中，中间服务器 205 储存信息的至少一部分 (264)。信息可储存用于例如审计目的。

[0078] 数据，在一些实现方式中，排列供数据处理用 (266)。视数据类型（例如，信用卡信息、患者信息、背景验证信息等）而定，数据可排列到一些后端服务器之一中，包括后端服务器 210。后端服务器 210，在一些实现方式中，可以是医疗系统服务器、信用卡服务器、电子支付处理服务器、执法服务器，或政府部门服务器。

[0079] 在一些实现方式中，数据在某个时间点上由中间服务器 205 转发给后端服务器 210 以供处理 (268)。在一些实现方式中，数据在传送给后端服务器 210 之前被加密。数据，在一些实现方式中，经由安全传输或经由安全网络连接提供给后端服务器 210。

[0080] 在一些实现方式中，数据在后端服务器 210 处经处理 (270) 以获得结果。视数据类型和 / 或后端服务器 210 的类型而定，结果可改变。例如，若后端服务器 210 是信用卡支付处理服务器，则结果可包括状态消息（例如，核准、拒绝等）。

[0081] 在一些实现方式中，后端服务器 210 将与处理用户数据有关的结果提供给中间服务器 205(272a)。例如，医疗系统服务器可提供与患者请求服务、手续或药物治疗的审查许可 (clearance) 有关的“核准”结果。

[0082] 中间服务器 205，在一些实现方式中，将结果转发给实体服务器 215(272b)。在一些实现方式中，中间服务器 205 储存结果用于实现审计目的（例如，连同之前在步骤 264 储存的用户数据）。

[0083] 在接收到结果时，在一些实现方式中，实体服务器 215 对结果进行处理 (274)。处理，在一些实现方式中，可包括将结果与前一请求，例如，购买商品的请求相关联。若，例如，信用卡信息已经被授权，则实体服务器 215 可发起对客户端计算设备 220 的用户的商品交付。

[0084] 在一些实现方式中，基于步骤 274 的处理结果，实体服务器 215 将与结果有关的信息提供给客户端计算设备 220(276)。例如，在接收到信用卡信息已经被拒绝的指示时，实体服务器 215 可在客户端计算设备 220 上执行的 web 浏览器应用程序内呈现关于拒绝的消息。

[0085] 在用户数据传输（步骤 260a）和结果处理（步骤 274）之间常常有大量时间（例如，数分钟、数小时、一天等）流逝。在这种情况下，在一些实现方式中，实体服务器 215 识别与用户相关联的联系人信息（例如，电子邮件地址、发短信的电话号码、社交媒体帐号信息等），而不是将与结果有关的信息提供给客户端计算设备 220（例如，浏览器应用程序内）。实体服务器 215，进一步参照示例，可使用联系人信息将与结果有关的信息提供给用户。

[0086] 尽管被示为特定的一系列步骤，但是在一些实现方式中，可实施更多或更少的步骤，或可以不同的顺序来执行所述步骤中的一个或多个。例如，在一些区域中，信用卡支付可能直到订单发货日才会被处理。在这种情况下，实体服务器 215 第一次可将加密用户数据提供给中间服务器 205(260b) 以验证信用卡信息是有效的，且第二次（例如，数小时或数日之后）用于发起支付处理。

[0087] 此外，在一些实现方式中，储存在中间服务器 205 的信用卡信息可被访问，用于重新使用，例如，基于后续交易期间提供的识别信息。例如，顾客在后续购买时，可在支付表格（例如，包括敏感和公开数据的可填写的表格）内选择“有记录的”信用卡。在一些实现方式中，随后传送的用户数据（例如，由客户端计算设备 220 发送给实体服务器 215，在此其被转发给中间服务器 205）可包括信用卡号码的一部分（银行信息号码 (BIN) 加上最后四位数字），或由实体服务器 215 辨认的旗标、标签，或编码。例如，在步骤 254 内提供的浏览器可呈现的信息内，实体服务器 215 可为客户端计算设备 220 提供可用于识别特定的“存档”信用卡（例如，最后四位数字为 7890 的美国运通卡）的部分编码的信用卡信息。在选择“存档”信用卡时，通过步骤 260a 传送的用户数据可包括用于识别所选的“存档”信用卡的文字美国运通和 7890 或另一个识别码（例如，唯一的识别符）。在步骤 260b，作为响应，实体服务器 215 可将用于识别“存档”信用卡的信息转发给中间服务器 205。中间服务器 205 可使用识别信息来检索存档的信用卡信息。可选地，响应于辨认出在步骤 260a 传送的用户数据中接收的“存档”信用卡识别信息，实体服务器 215 可将加密的信用卡信息存档并将（仍加密的）信用卡信息转发给中间服务器 205。对操作流程 250 的其它修改是可能的。

[0088] 图 3 是用于提供并使用启用信息的客户端加密的无线计算设备应用程序的示例操作流程 300 的泳道图。操作流程 300 示出在移动计算设备 302（例如，诸如，参照图 1 所述的客户端计算设备 122）、应用程序商店 304、实体服务器 306（例如，诸如，参照图 1 所述的实体服务器 115）和中间服务器 308（例如，诸如，参照图 1 所述的中间服务器 105）之间传递的示例信息。在一些实现方式中，操作流程 300 可用于提供并利用隶属于在线供应商的移动应用程序，用于购买经由实体服务器 306 处理的商品和服务。操作流程 300，在一些实现方式中，可用于提供并利用隶属于保健系统的移动应用程序，用于认证健康信息网络上的患者信息。在一些实现方式中，操作流程 300 可用于提供并利用隶属于执法系统的移动应用程序，用于验证背景信息以实现调查目的。

[0089] 在一些实现方式中，操作流程 300 从中间服务器 308 为实体服务器 306 提供公共加密密钥和一种或多种加密算法 (310) 开始。公共加密密钥，例如，可与由中间服务器 308 保存的私有加密密钥配对。公共加密密钥，例如，可用于使用加密算法中的一种或多种将数据加密。在中间服务器处，可使用由中间服务器 308 保存的配对的私有加密密钥和一种或多种解密算法来将加密数据解密。在一些实现方式中，公钥对实体服务器 306 是唯一的。例如，中间服务器 308 可将不同的公钥分配给利用中间服务器 308 的服务来安全传送和处理敏感数据的每一个实体。

[0090] 在一些实现方式中，实体服务器 306 可将中间服务器 308 提供的公钥和至少一种安全算法捆绑到移动设备应用程序中 (312)。例如，被给予公钥和一种或多种安全算法的开发者可将加密算法纳入到收集和安全传送用户数据的应用程序中。可选地，移动设备应用程序可被配置为在敏感数据加密时从实体服务器 306 或中间服务器 308 请求公共加密密钥和安全算法中的一者或多者。

[0091] 在开发移动设备应用程序时，实体可提供移动应用程序供用户在应用程序商店消费 (314)。例如，为 iPhone™ 平台开发的移动设备应用程序可用于通过 Apple 应用程序商店来下载，而为 Android™ 平台开发的移动设备应用程序可用于通过 Google 应用程序商店来下载。在其它实施方式中，应用程序可用于直接下载和安装，例如，经由实体服务器 306。

[0092] 终端用户可从应用程序商店 304 下载实体应用程序，安装在移动计算设备 302 上 (316)。例如，实体可提供 web 站点上的信息供用户下载应用程序。应用程序，在一些示例中，可以是用于商业实体购物的应用程序、用于经由保健组织实体来管理患者信息的应用程序，或用于经由人力资源支撑实体来管理候选者的背景信息的应用程序。

[0093] 在用户使用移动计算设备 302 与安装的移动设备应用程序互动时，在一些实现方式中，用户可输入传送给实体服务器 306 的敏感信息。例如，用户可被展示以包括一个或多个用于输入与订单、信息请求，或认证请求有关的数据的信息栏位的用户界面。在将信息提供给实体服务器 306 之前，移动计算设备，在一些实现方式中，将数据的至少一部分用之前由中间服务器 308 提供给实体服务器 306 的公共密钥和至少一种安全算法加密 (318)。

[0094] 在一些实现方式中，加密数据由移动计算设备 302 传送给实体服务器 306(320a)。移动设备应用程序，在一些实现方式中，被编程以与实体通信。加密数据，例如，可经由安全或非安全传输提供给实体服务器 306。

[0095] 实体服务器 306，作为响应，可将用户数据的至少一部分，包括加密数据，转发给中间服务器 308(320b)。中间服务器 308 可将用户数据解密，例如，使用私有加密密钥和解密算法 (322)。如之前参照图 2B 的步骤 262 到 272 所述，例如，数据可储存用于实现审计目的并提供给后端服务器以供处理。后端服务器可将结果提供给与处理之前加密的数据有关的中间服务器 308。

[0096] 在一些实现方式中，中间服务器 308 将与数据处理有关的结果提供给实体服务器 306。结果，例如，可使用交易识别符、用户信息的一部分，或与移动计算设备的终端用户有关的识别符被识别供实体服务器 306 辨认。例如，在转发供处理的加密用户数据 (320b) 时，中间服务器 308 可接收唯一的交易识别符。可选地，响应于加密用户数据的接收，中间服务器 308 可为实体服务器 306 提供与加密数据有关的唯一的交易识别符。

[0097] 在一些实现方式中，与结果有关的信息可提供给终端用户的移动账户 (326)。例如，使用移动计算设备 302，终端用户可经由移动设备应用程序接收结果信息。

[0098] 尽管被示为特定的一系列步骤，但是在一些实现方式中，可实施更多或更少的步骤，或可以不同的顺序来执行所述步骤中的一个或多个。对操作流程 300 的其它修改是可能的。

[0099] 图 4 是使客户端能对来自客户的信息进行加密的方法 400 的流程图。例如，方法 400 可以由中间服务器来实施，例如参照图 1 描述的中间服务器 105。

[0100] 在一些实现方式中，所述方法首先提供用于加密用户数据的加密算法 (402)。例如，加密算法可以提供给实体以便加密敏感信息。

[0101] 在一些实现方式中，给实体分配与加密算法一起使用的公钥 (404)。例如，公钥可以与加密算法结合使用。在一些实现方式中，公钥与分配器（例如，中间服务器）所保持的私匙配对。

[0102] 在一些实现方式中，接收了使用公钥和加密算法进行加密的加密的用户数据 (406)。例如，实体服务器可以转发在客户端计算设备使用加密算法和公钥时被加密的加密的数据。在一些实现方式中，未加密的用户数据和加密的用户数据一样可以被包括在同一次传输中。

[0103] 在一些实现方式中，与加密的用户数据相关的实体被确定 (408)。例如，在加密的

用户数据的传输中可以具有对实体进行标识的标识符（例如，在传输数据包报头中或者在具有加密的数据的未加密的数据中）。又如，可以按照传输的来源（例如，互联网协议（IP）地址、DNS 服务器等）标识实体。在一些实现方式中，公钥或者与公钥对应的标识符具有加密的用户数据。可以基于公钥来标识实体或者与实体相关的私匙。

[0104] 在一些实现方式中，与实体相关的私匙被确定（410）。在一些实现方式中，单个公钥已经被分配给实体。在这种情况下，在步骤 408 中被标识的实体可以用于唯一地标识私匙。在一些实现方式中，如果两个或更多个公钥已经被分配给实体，那么可以分析额外的信息来标识私匙。例如，当标识与处理请求匹配的私匙时可以考虑信息的来源（例如，移动设备应用与 web 页面）、请求的处理类型（例如，信用卡处理与个人背景验证等）或传输的信息来源（例如，实体网关、IP 地址、DNS 名称等）。

[0105] 在一些实现方式中，使用私匙和解密算法对加密的用户数据进行解密（412）。在一些实现方式中，解密的数据可以被存储用于审计目的。

[0106] 在一些实现方式中，将解密的用户数据排队以便使用处理引擎进行处理（414）。例如，基于信息的来源、与信息相关的实体和 / 或与请求的处理类型相关的传输内的标识符，将解密的用户数据排队以便使用一个或多个后端处理服务器进行处理。在一些实现方式中，后端处理系统为第三方所有，例如，信用卡公司。在其它实施方式中，由同一实体控制中间服务器和后端处理器。如果后端处理器立即可供使用，那么解密的用户数据可以被传输用于处理而非排队。

[0107] 在一些实现方式中，将解密的用户数据提供给处理引擎（416）。在一些实现方式中，与加密的用户数据一起传输的一部分未加密的用户数据同样可以被供应到处理引擎，例如，以便用作标识信息，从而给请求提供背景（例如，名字、邮政编码等）。在一些实现方式中，解密的用户数据通过安全传输被提供给处理引擎。在提供解密的用户数据到处理引擎之前，例如，可以用处理引擎可识别的格式来加密数据。又如，解密的用户数据可以通过安全的通信连接被提供给处理引擎。

[0108] 在一些实现方式中，接收来自处理引擎的处理结果（418）。处理结果中包含的信息可以在布尔值（例如，批准 / 拒绝等）与多元媒体响应（例如，指纹的图像数据、照片、文字数据等）之间变化。例如，处理结果可以根据请求的处理类型的变化而变化。处理结果可以被实时接收（即，在解密的用户数据已经被提供给处理引擎不久之后）或稍后接收。在一些实现方式中，基于事务标识符、用户标识符、实体标识符和 / 或请求时间戳的一个或多个可识别包含结果的传输。在一些实现方式中，在接收处理结果时，处理结果与特定的处理请求匹配。

[0109] 在一些实现方式中，将处理结果提供给实体（420）。在一些实现方式中，在使处理结果与处理请求进行匹配时，可以对响应方法进行标识以便将信息中继转发给请求实体。例如，实体可以具有专用服务器、网关、传输代码、传输类型或者用于接收处理结果的其它偏好。在一些实现方式中，处理结果或处理结果的可用性指示可以通过传真来发送、公布，或者登记在由中间系统替实体维护的账户中。在一些实现方式中，在包含处理结果的传输中可以提供一部分请求信息，例如，以便使处理结果与实体的请求之间能匹配上。

[0110] 在一些实现方式中，除提供处理结果之外，方法 400 可以包括将处理结果、与处理结果有关的信息（例如，接收的时间戳、转发给实体的时间戳、成功转发给实体的指示等）

存储在长期储存区中。例如，这些信息可以被存储用于审计目的。

[0111] 尽管按照特定的一系列步骤进行说明，但是在一些实现方式中，可以实施更多或更少的步骤，或者可以按照不同的顺序来执行一个或多个步骤。运作流程 400 的其它修改形式是可行的。

[0112] 如图 5 所示，图示并描述了供客户端加密和安全传输数据的示例性云计算环境 500 的实现方式。云计算环境 500 可以包括一个或多个资源提供商 502a、502b、502c（统称为 502）。每个资源提供商 502 可以包括计算资源。在一些实现方式中，计算资源可以包括用于处理数据的任何硬件和 / 或软件。例如，计算资源可以包括能执行算法的硬件和 / 或软件、计算机程序和 / 或计算机应用。在一些实现方式中，示例性计算资源可以包括应用服务器和 / 或具有储存和检索能力的数据库。在云计算环境 500 中，每个资源提供商 502 可以连接到任何其它的资源供应商 502。在一些实现方式中，资源提供商 502 可以通过计算机网络 508 连接上。每个资源提供商 502 可以通过计算机网络 508 连接至一个或多个计算设备 504a、504b、504c（统称为 504）。

[0113] 云计算环境 500 可以包括资源管理器 506。资源管理器 506 可以通过计算机网络 508 连接至资源提供商 502 和计算设备 504。在一些实现方式中，资源管理器 506 可以辅助一个或多个资源提供商 502 提供计算资源到一个或多个计算设备 504。资源管理器 506 可以从特定的计算设备 504 接收对计算资源的请求。资源管理器 506 可以识别能提供计算设备 504 所请求的计算资源的一个或多个资源提供商 502。资源管理器 506 可以选择资源提供商 502 来提供计算资源。资源管理器 506 可以辅助资源提供商 502 与特定的计算设备 504 之间的连接。在一些实现方式中，资源管理器 506 可以建立特定的资源提供商 502 与特定的计算设备 504 之间的连接。在一些实现方式中，资源管理器 506 可以以请求的计算资源来将计算设备 504 重定向到特定的资源提供商 502。

[0114] 图 6 示出了可以用于实施本公开中描述的技术的计算设备 600 和移动计算设备 650 的示例。计算设备 600 旨在表示各种形式的数字计算机，例如，笔记本电脑、台式电脑、工作站、个人数字助理、服务器、刀片式服务器、大型主机和其它合适的计算机。移动计算设备 650 意在代表各种形式的移动设备，例如个人数字助理、移动电话、智能手机和其它类似的计算设备。本文示出的组件、它们的连接和关系以及它们的功能仅仅意味着示例，且并非意味着限制。

[0115] 计算设备 600 包括处理器 602、存储器 604、存储设备 606、连接到存储器 604 和多重高速扩展端口 610 的高速接口 608、以及连接到低速扩展端口 614 和存储设备 606 的低速接口 612。处理器 602、存储器 604、存储设备 606、高速接口 608、高速扩展端口 610 和低速接口 612 的每一个使用多种总线互连，并且可以安装在共同的主板上或者以其它适当的方式被安装。处理器 602 可以处理用于在计算设备 600 中执行的指令，包括存储在存储器 604 中或者存储在存储设备 606 上用于在外部输入 / 输出设备（例如连接到高速接口 608 的显示屏 616）上显示用于 GUI 的图形信息的指令。在其它实现方式中，适当的情况下多个处理器和 / 或多个总线可以与多个存储器和多种存储器一起使用。另外，可以连接多个计算设备，其中每个计算设备提供必要操作的一部分（例如服务器组、一组刀片式服务器或多处理器系统）。

[0116] 存储器 604 在计算设备 600 内存储信息。在一些实现方式中，存储器 604 是一个

或多个易失性存储器装置。在一些实现方式中，存储器 604 是一个或多个非易失性存储器装置。存储器 604 还可以是另一种形式的计算机可读的介质，例如磁盘或光盘。

[0117] 存储设备 606 能为计算设备 600 提供大容量存储。在一些实现方式中，存储设备 606 可以是或者包括计算机可读的介质，例如软盘设备、硬盘设备、光盘设备或磁带设备、闪速存储器或其它类似的固态存储设备或设备阵列（包括存储区域网或其它配置中的设备）。指令可以存储在信息载体中。指令当被一个或多个处理设备（例如处理器 602）执行时实施一种或多种方法，例如上述方法。指令还可以通过一个或多个存储设备来存储，例如计算机可读的介质或机器可读的介质（例如存储器 604、存储设备 606 或处理器 602 上的存储器）。

[0118] 高速接口 608 管理计算机设备 600 的高带宽密集型操作，而低速接口 612 管理低带宽密集型操作。这种功能分配只是一个示例。在一些实现方式中，高速接口 608 耦接到存储器 604、显示屏 616（例如通过图形处理器或图形加速器）并且耦接到高速扩展端口 610，高速扩展端口可以接收多种扩展卡（未示出）。在该实施方式中，低速接口 612 连接到存储设备 606 和低速扩展端口 614。可以包括多种通信端口（例如 USB、蓝牙®、以太网、无线以太网）的低速扩展端口 614 可以，例如通过网络适配器耦接到一个或多个输入 / 输出设备（例如键盘、指向设备、扫描仪）或者诸如交换机或路由器的网络设备。

[0119] 计算设备 600 可以实现为多种不同的形式，如附图所示。例如，计算设备可以实现为标准服务器 620，或一组这种服务器的好几倍。此外，计算设备可以实现为个人计算机，例如，笔记本电脑 622。计算设备还可以实现为机架服务器系统 624 的一部分。可替代地，来自计算设备 600 的组件可以与例如移动计算设备 650 的移动设备（未示出）中的其它组件结合。每个这种设备可以包括计算设备 600 和移动计算设备 650 的一个或多个，并且整个系统可以是由彼此通信的多个计算设备组成的。

[0120] 除其它组件之外，移动计算设备 650 包括处理器 652、存储器 664、例如显示屏 654 的输入 / 输出设备、通信接口 666 和收发器 668。移动计算设备 650 还可以具有存储设备，例如，微型驱动器或其它设备，以便提供额外存储。处理器 652、存储器 664、显示屏 654、通信接口 666 和收发器 668 的每一个使用多种总线互连，并且几个组件可以安装在共同的主板上，或者以其它方式安装，视具体情况而定。

[0121] 处理器 652 可以执行移动计算设备 650 中的指令，包括存储在存储器 664 中的指令。处理器 652 可以实现为芯片的芯片集，这种芯片集包括分开的多个模拟和数字处理器。例如，处理器 652 可以提供用于协调移动计算设备 650 的其它组件，例如，控制用户接口、移动计算设备 650 运行的应用以及移动计算设备 650 的无线通信。

[0122] 处理器 652 可以通过控制接口 658 以及与显示屏 654 连接上的显示接口 656 与用户通信。显示屏 654 可以是例如 TFT（薄膜晶体管液晶显示屏）显示屏或 OLED（有机发光二极管）显示屏或者其它合适的显示技术。显示接口 656 可以包括用于驱动显示屏 654 以便向用户呈现图形和其它信息的适当电路。控制接口 658 可以接收来自用户的命令并且将命令进行转化以便提交到处理器 652。此外，外部接口 662 可以提供与处理器 652 进行通信，以便使移动计算设备 650 能与其它设备进行近场通信。在一些实现方式中，外部接口 662 可以提供用于例如有线通信，在其它实施方式中，外部接口可以提供用于无线通信，并且还可以使用多个接口。

[0123] 存储器 664 在移动计算设备 650 中存储信息。存储器 664 可以实现为一个或多个计算机可读的介质、易失性存储设备或非易失性存储设备。扩展存储器 674 还可以通过扩展接口 672 提供给并连接到移动计算设备 650，所述扩展接口可以包括例如 SIMM（单列直插式内存模块）卡接口。扩展存储器 674 可以为移动计算设备 650 提供额外的存储空间，或者还可以为移动计算设备 650 存储应用或其它信息。特别地，扩展存储器 674 可以包括用于实施或补充上述方法的指令，并且同样可以包括安全信息。因此，例如，扩展存储器 674 可以作为安全模块提供给移动计算设备 650，并且可以编写有允许安全使用移动计算设备 650 的指令。此外，安全应用连同额外的信息一起可以经由 SIMM 卡来提供，例如，以不可非法侵入的方式在 SIMM 卡上放置识别信息。

[0124] 如上所述，存储器可以包括，例如，闪速存储器和 / 或 NVRAM 存储器（非易失性随机存取存储器）。在一些实现方式中，指令存储在信息载体中，这些指令当被一个或多个处理设备（例如，处理器 652）执行时实施一种或多种方法，例如上述的这些方法。指令还可以由一个或多个存储设备来存储，例如，一个或多个计算机可读的介质或机器可读的介质（例如，存储器 664、扩展存储器 674 或处理器 652 上的存储器）。在一些实现方式中，例如，可以通过收发器 668 或外部接口 662 在传播的信号中接收指令。

[0125] 移动计算设备 650 可以通过通信接口 666 进行无线通信，所述通信接口在必要时可以包括数字信号处理电路。通信接口 666 可以提供用于多种模式或协议下的通信，除了别的以外，例如，GSM 语音电话（全球移动通信系统）、SMS（短消息服务）、EMS（增强型短信服务）或 MMS（多媒体信息服务）、CDMA（码分多址）、TDMA（时分多址）、PDC（个人数字蜂窝电话）、WCDMA（宽带码分多址）、CDMA2000 或 GPRS（通用分组无线服务）。例如，使用射频通过收发器 668 可以实现这种通信。此外，可以进行短波通信，例如，使用蓝牙®、Wi-Fi™ 或其它的这种收发器（未示出）。此外，GPS（全球定位系统）收发器模块 670 可以提供额外的与导航及定位相关的无线数据到移动计算设备 650，视情况而定，移动计算设备 650 上运行的应用可以使用这些信息。

[0126] 移动计算设备 650 还可以使用音频解码器 660 进行声音通信，所述音频解码器可以接收来自用户的语音信息并且将其转换成可使用的数字信息。音频解码器 660 同样可以产生可听见的声音给用户，比如，通过例如在移动计算设备 650 的听筒中的扬声器产生声音。这种声音可以包括来自语音电话的声音，可以包括录制的声音（例如语音消息、音乐文件等），并且还可以包括在移动计算设备 650 上运行的应用所产生的声音。

[0127] 移动计算设备 650 可以实现为多种不同形式，如附图所示。例如，移动计算设备可以实现为移动电话 680。移动计算设备还可以实现为智能电话 682、个人数字助理或其它类似移动设备的一部分。

[0128] 本文描述的系统和技术的多种实施方式可以实现为数字电子电路、集成电路、专用 ASIC（专用集成电路）、计算机硬件、固件、软件和 / 或它们的组合。这些实施方式可以包括一个或多个计算机程序中的实施方式，包括至少一个可编程处理器、至少一个输入设备以及至少一个输出设备的可编程系统可执行并且 / 或者可编译这些计算机程序，所述可编程处理器可以被专用地或通用地连接以便接收来自存储系统的数据和指令，并且发送数据和指令到所述存储系统。

[0129] 这些计算机程序（也被称为程序、软件、软件应用或代码）包括用于可编程处理器

的机器指令，并且可以在高层次的过程编程语言和/或面向对象编程语言中实施，并且/或者在汇编语言/机器语言中实施。本文中使用的术语“机器可读的介质”和“计算机可读的介质”指的是用于提供机器指令和/或数据到可编程处理器的任何计算机程序产品、装置和/或设备（例如，磁盘、光盘、存储器、可编程逻辑器件(PLD)），包括接收机器指令作为机器可读的信号的机器可读的介质。术语“机器可读的信号”指的是用于提供机器指令和/或数据到可编程的处理器的任何信号。

[0130] 为了提供与用户进行交互，本文描述的系统和技术可以在计算机上实施，所述计算机具有显示设备（例如，CRT（阴极射线管）或LCD（液晶显示屏）监视器）以及键盘和指向设备（例如，鼠标或轨迹球），所述显示设备用于向用户显示信息，并且用户通过指向设备可以向计算机提供输入。同样可以使用其它类型的设备来提供与用户的交互，例如，提供给用户的反馈可以是任何形式的传感反馈（例如，视觉反馈、听觉反馈或触觉反馈），并且能够以任何方式接收来自用户的输入，包括声音输入、语音输入或触觉输入。

[0131] 本文描述的系统和技术可以实现为计算系统，所述计算系统包括后端组件（例如，作为数据服务器），或者所述计算系统包括中间件组件（例如，应用服务器），或者所述计算系统包括前端组件（例如，具有图形用户接口的客户端计算机，或者用户可以与本文描述的系统和技术的实施方式交互的web浏览器）或者这些后端组件、中间件组件或前端组件的任意组合。系统的组件可以通过任何形式或数字数据通信（例如，通信网络）的介质互连。通信网络的示例包括局域网(LAN)、宽带网(WAN)和互联网。

[0132] 计算系统可以包括客户端和服务器。客户端和服务器一般彼此距离较远并且通常通过通信网络交互。由于在各个计算机上运行并且彼此具有客户端-服务器关系的计算机程序而出现了客户端和服务器的关系。

[0133] 根据本文描述的系统的结构、功能和装置以及方法，在一些实现方式中，提供了用于收集并操作事务数据的装置和方法。由于已经描述了用于客户端加密以及安全传输用户数据的方法和装置的实施方式，本领域技术人员现在会明白，可以使用整合本发明的概念的其它实施方式。因此，本发明不应当局限于某些实施方式，而是应当仅由以下权利要求书的精神和范围来限制。

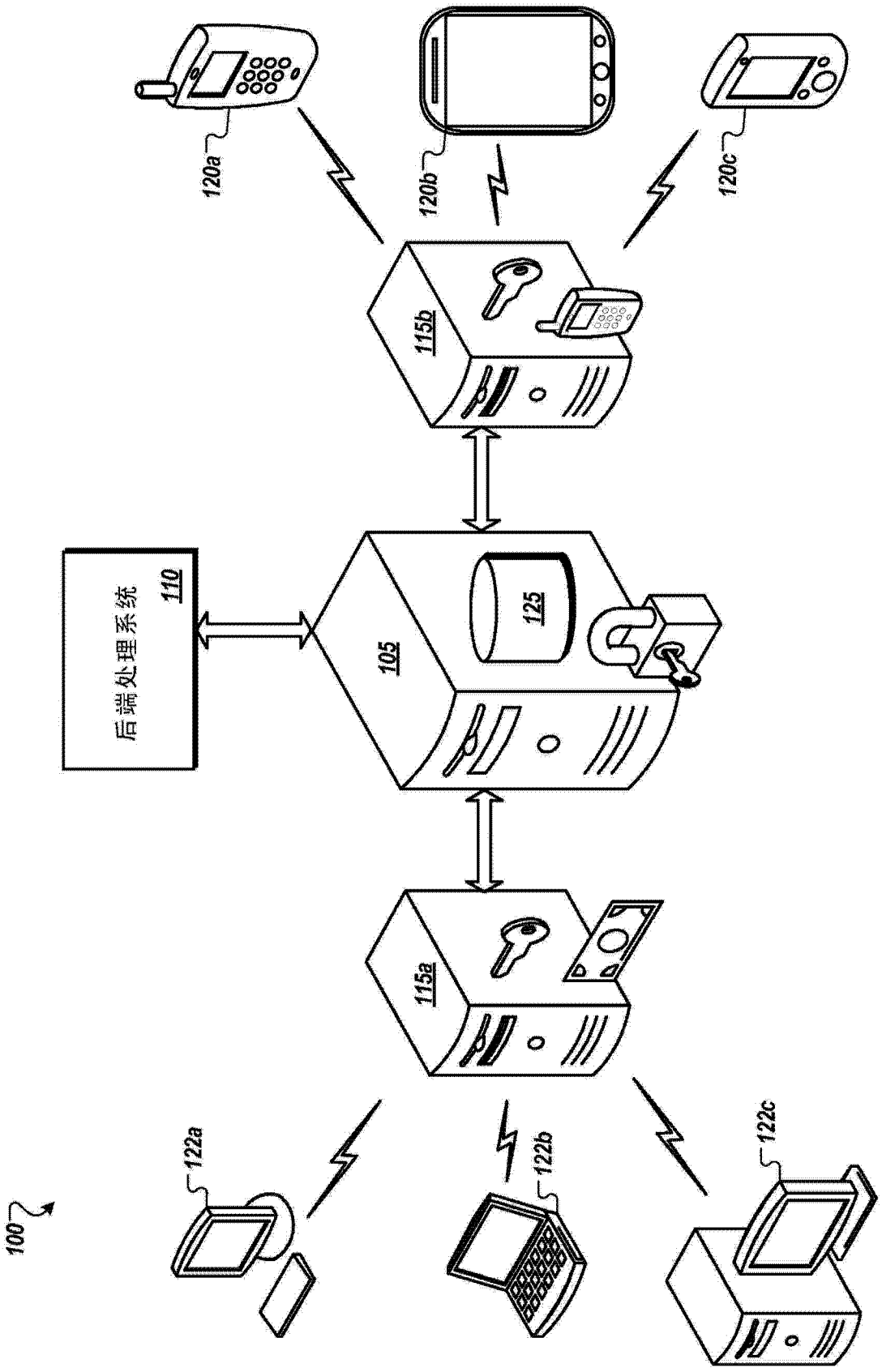

120a
120b
120c
115b
后端处理系统
110
105
125
115a
122a
122b
122c
100

图 1

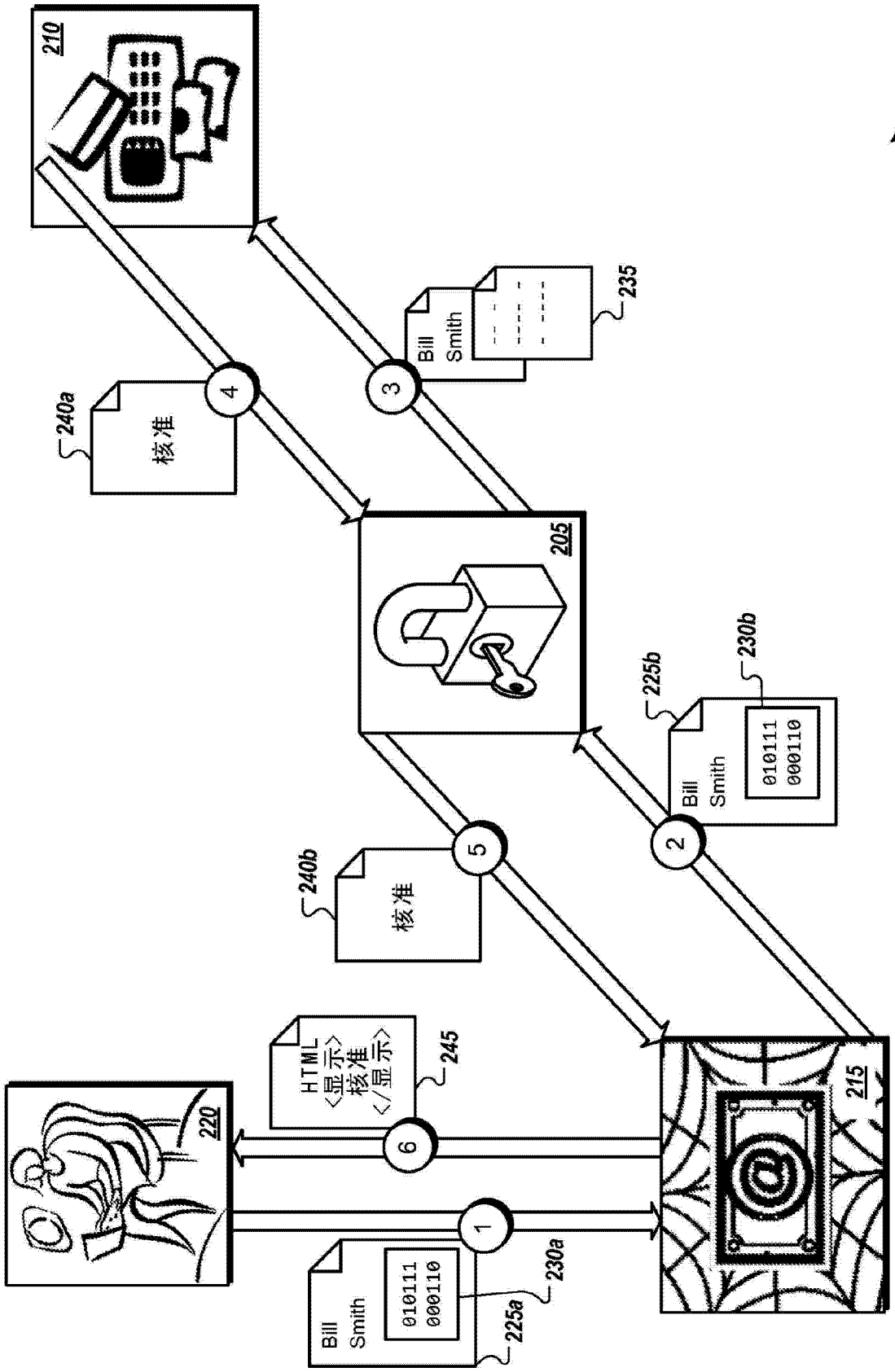

200
210
235
Bill
Smith
240a
核准
4
3
205
225b
230b
Bill
Smith
010111
000110
2
240b
核准
5
HTML
<显示>
核准
</显示>
245
220
6
215
1
Bill
Smith
010111
000110
230a
225a

图 2A

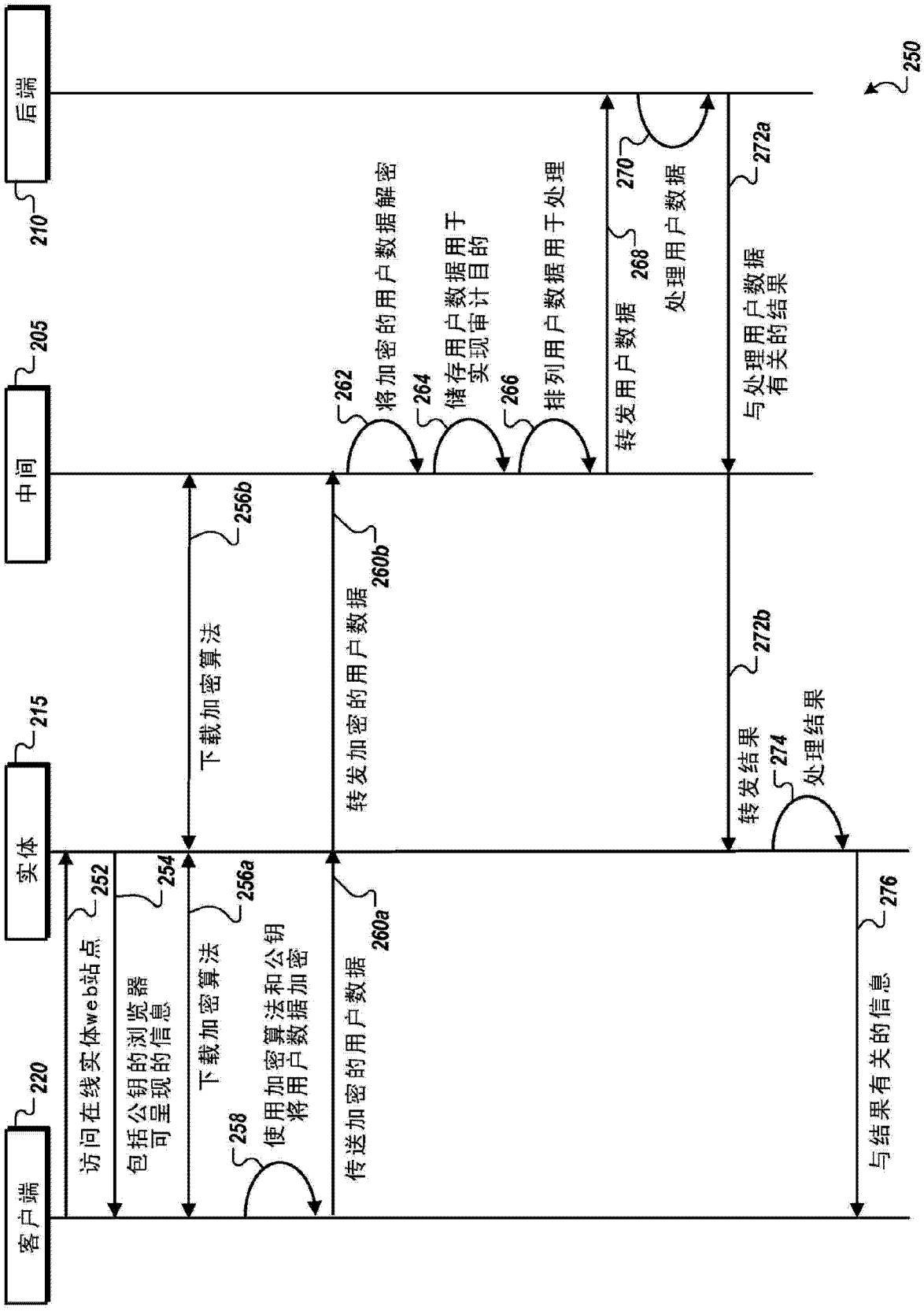

客户端
220
实体
215
中间
205
后端
210
250
访问在线实体web站点
252
包括公钥的浏览器
可呈现的信息
254
下载加密算法
256a
使用加密算法和公钥
将用户数据加密
258
传送加密的用户数据
260a
下载加密算法
256b
转发加密的用户数据
260b
将加密的用户数据解密
262
储存用户数据用于
实现审计目的
264
排列用户数据用于处理
266
转发用户数据
268
处理用户数据
270
与处理用户数据
有关的结果
272a
转发结果
272b
处理结果
274
与结果有关的信息
276

图 2B

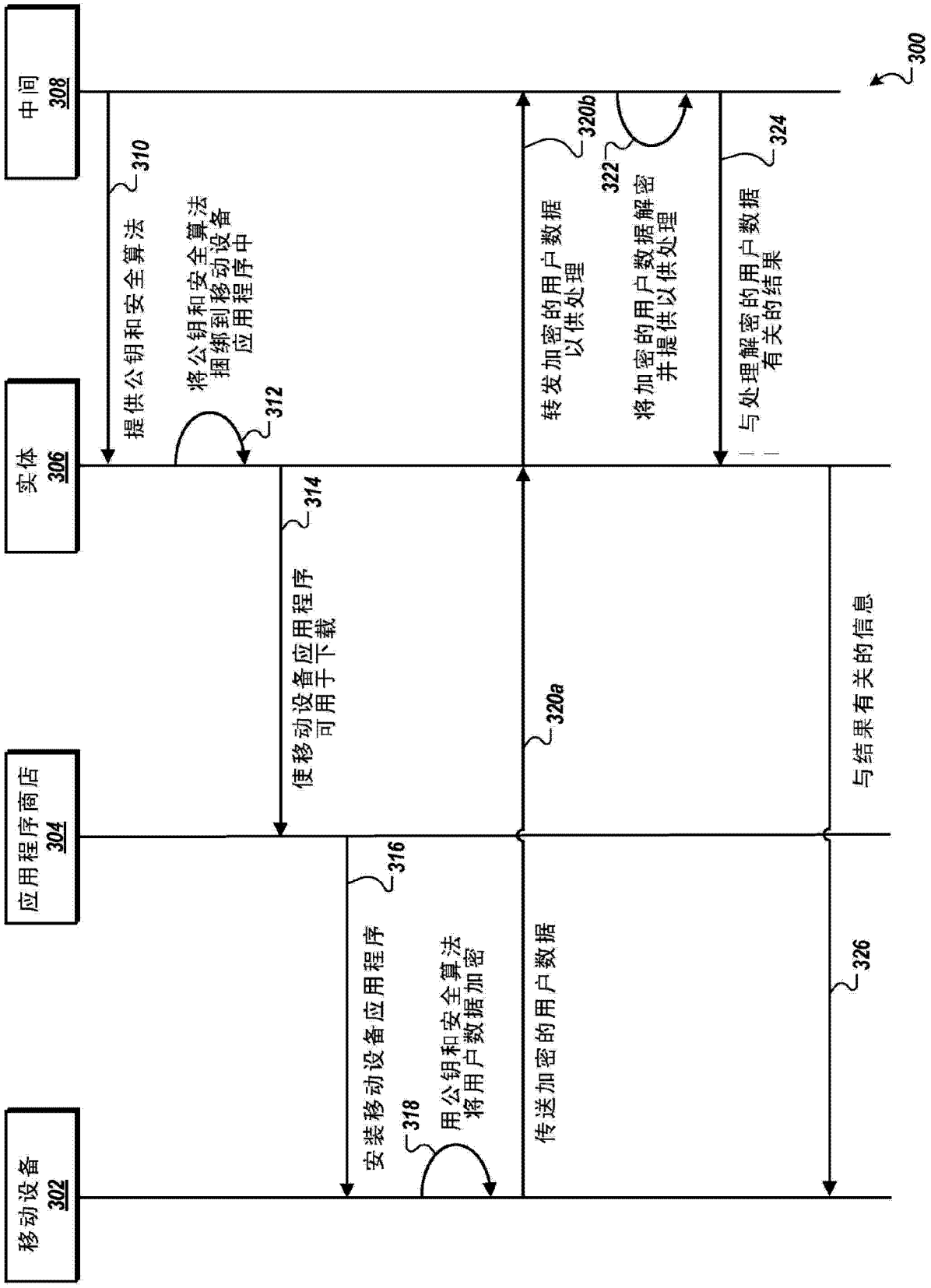

移动设备
302
应用程序商店
304
实体
306
中间
308
300
提供公钥和安全算法
310
将公钥和安全算法
捆绑到移动设备
应用程序中
312
使移动设备应用程序
可用于下载
314
安装移动设备应用程序
316
用公钥和安全算法
将用户数据加密
318
320a
传送加密的用户数据
转发加密的用户数据
以供处理
320b
将加密的用户数据解密
并提供以供处理
322
与处理解密的用户数据
有关的结果
324
与结果有关的信息
326

图 3

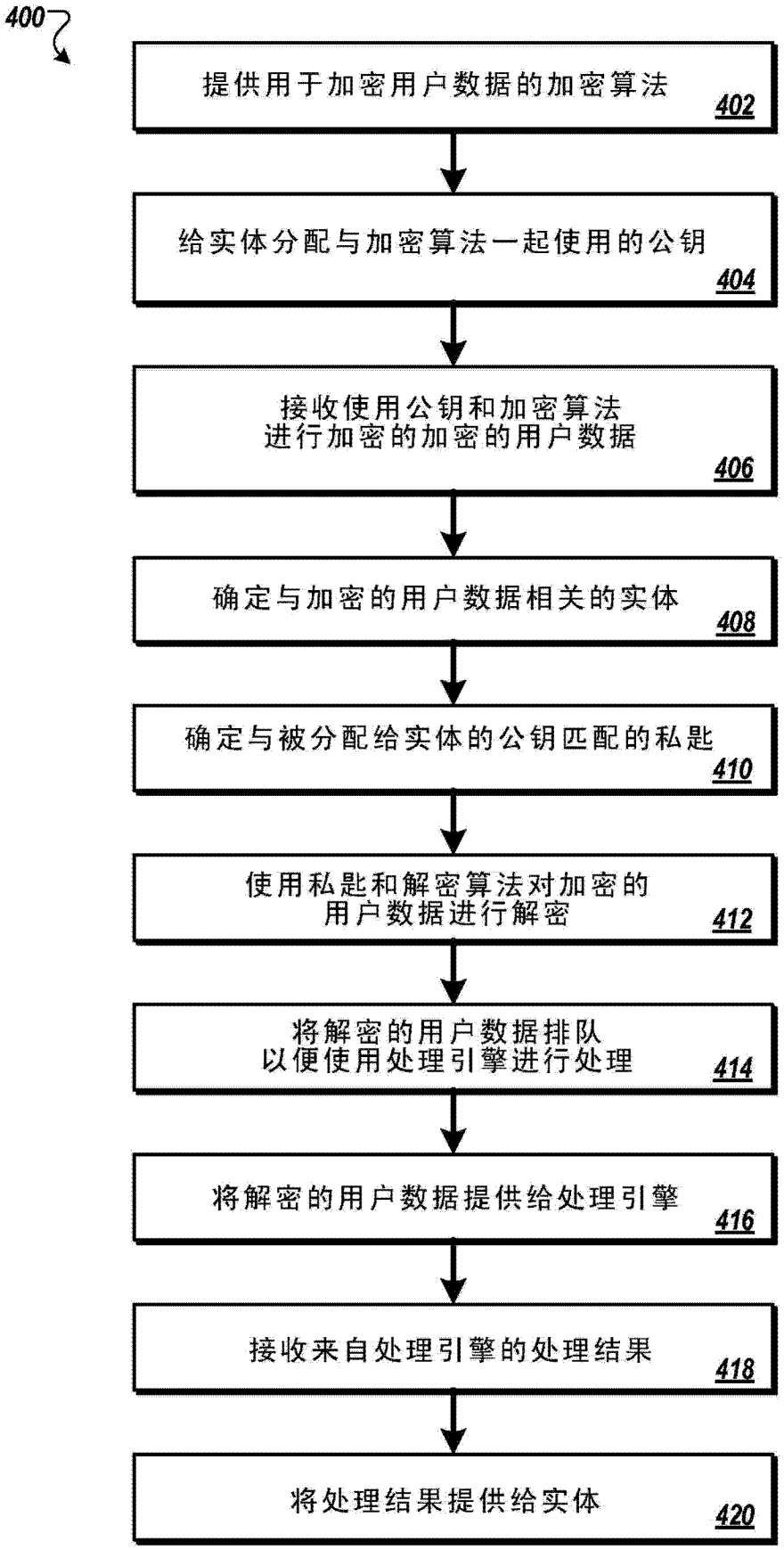

400
提供用于加密用户数据的加密算法
402
给实体分配与加密算法一起使用的公钥
404
接收使用公钥和加密算法
进行加密的加密的用户数据
406
确定与加密的用户数据相关的实体
408
确定与被分配给实体的公钥匹配的私匙
410
使用私匙和解密算法对加密的
用户数据进行解密
412
将解密的用户数据排队
以便使用处理引擎进行处理
414
将解密的用户数据提供给处理引擎
416
接收来自处理引擎的处理结果
418
将处理结果提供给实体
420

图 4

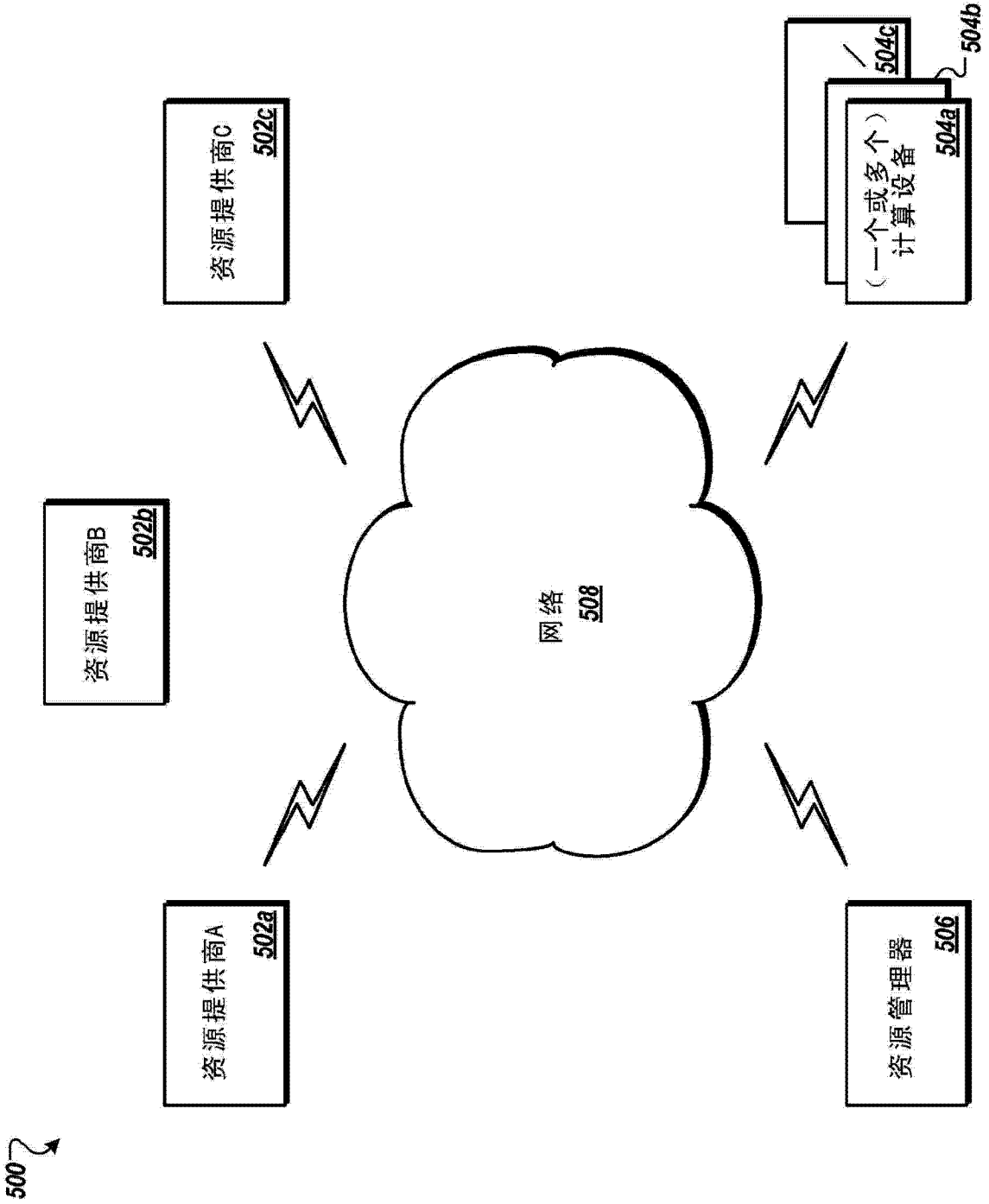

500
资源提供商A
502a
资源提供商B
502b
资源提供商C
502c
网络
508
资源管理器
506
（一个或多个）
计算设备
504a
504b
504c

图 5

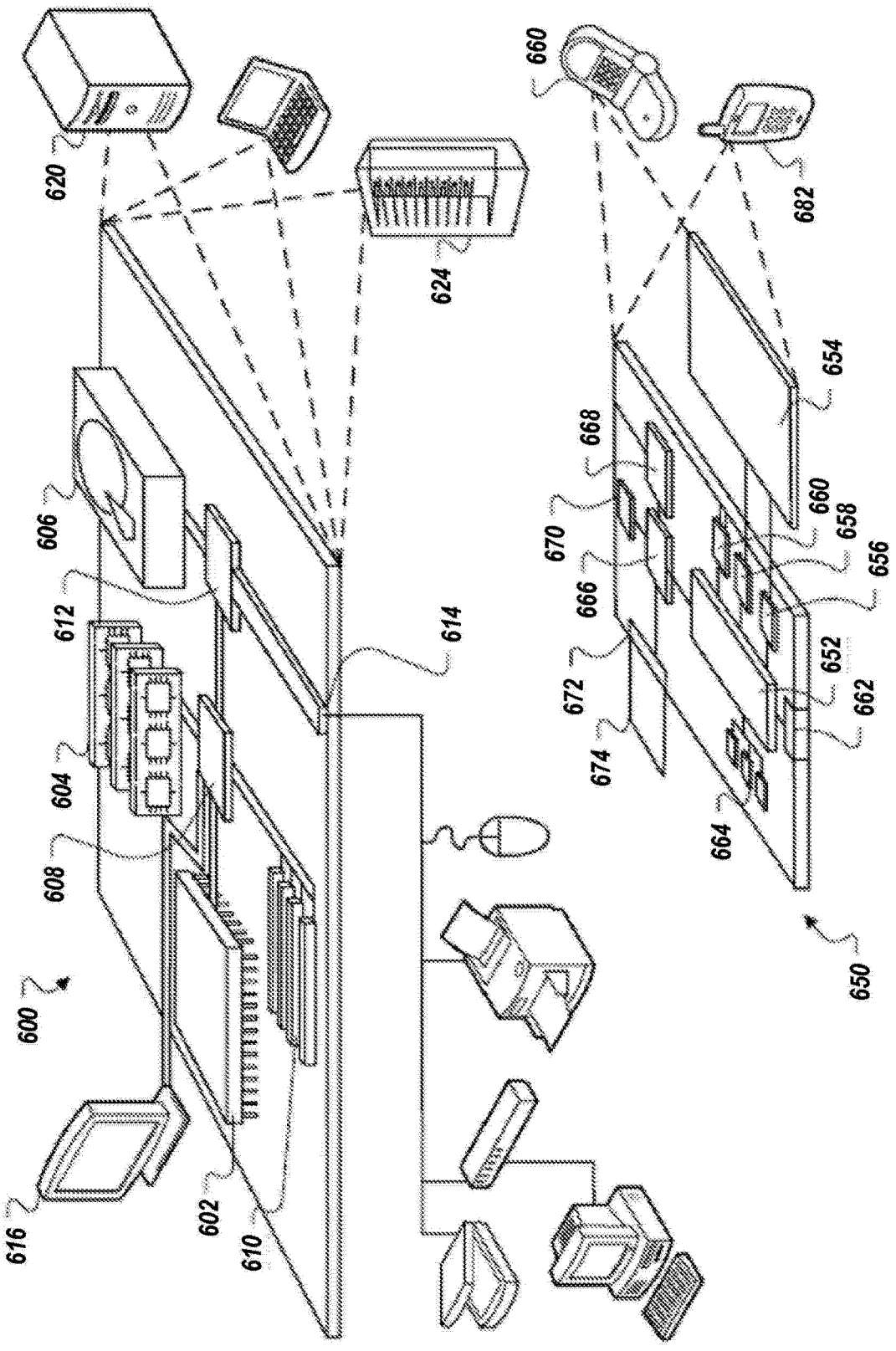

620
624
660
682
654
668
660
658
656
670
666
652
672
662
674
664
650
606
612
614
604
608
600
602
610
616

图 6