



(12) 发明专利申请

(10) 申请公布号 CN 114467279 A

(43) 申请公布日 2022. 05. 10

(21) 申请号 202080068132.1

(22) 申请日 2020.07.29

(30) 优先权数据

62/881,025 2019.07.31 US

(85) PCT国际申请进入国家阶段日

2022.03.28

(86) PCT国际申请的申请数据

PCT/US2020/044086 2020.07.29

(87) PCT国际申请的公布数据

W02021/021942 EN 2021.02.04

(71) 申请人 奇跃公司

地址 美国佛罗里达州

(72) 发明人 J·坎贝尔 D·奥利尚斯基

M·L·克尔

(74) 专利代理机构 北京市中咨律师事务所

11247

专利代理师 于静 牛南辉

(51) Int.Cl.

H04L 9/08 (2006.01)

G06F 16/58 (2006.01)

G06F 3/041 (2006.01)

G06N 5/02 (2006.01)

H04W 12/02 (2006.01)

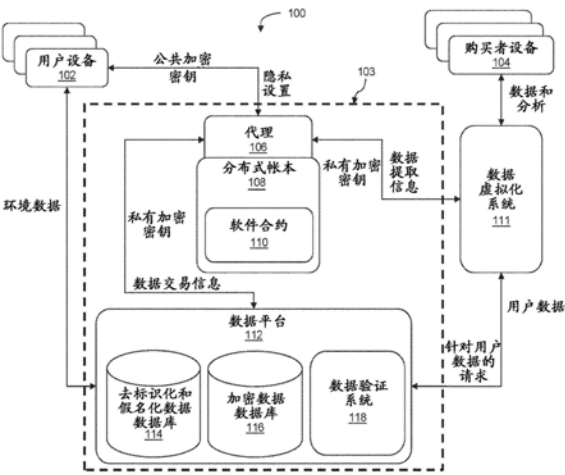
权利要求书17页 说明书31页 附图12页

(54) 发明名称

使用分布式账本用于增强现实的用户数据管理

(57) 摘要

在此公开了用于使用分布式账本来设置、访问和修改用户隐私设置的系统和方法。在一方面，系统可以搜索先前存储的软件合约，以基于访问特定用户的用户数据的请求来定位与用户相关联的软件合约的最新的版本。然后，系统确定允许共享用户数据。该系统向数据虚拟化平台发送从数据平台提取经加密的用户数据的指令。然后，系统可以向数据验证系统提供私有加密密钥和与软件合约相关联的细节，以验证私有加密密钥和用户数据是否匹配。然后系统向数据虚拟化平台发送私有加密密钥，使得数据虚拟化平台可以解密经加密的用户数据。



1. 一种用户设备, 包括:
 - 一个或多个计算机可读存储设备, 其被配置为存储计算机可执行指令;
 - 头戴式显示器;
 - 传感器, 其被配置为检测所述用户设备的周围环境;
 - 分布式账本管理器, 其包括分布式账本和被配置为读取和写入所述分布式账本的软件;
 - 数据平台, 其包括一个或多个数据库;
 - 网络接口; 以及
 - 一个或多个硬件计算机处理器, 其与所述一个或多个计算机可读存储设备通信以执行所述计算机可执行指令以使所述用户设备:
 - 接收与第一用户相关联的隐私设置;
 - 向分布式账本管理器发送所述隐私设置;
 - 从所述分布式账本管理器接收与所述第一用户相关联的第一公共加密密钥;
 - 经由所述传感器收集与所述用户设备相关联的环境数据;
 - 基于所述第一公共加密密钥, 加密所述环境数据;
 - 用元数据来语义标记经加密的环境数据, 其中, 所述元数据至少指示关于所述用户设备的标识信息; 以及
 - 向数据平台发送被语义标记的经加密的环境数据, 其中, 所述数据平台包括一个或多个数据库。
2. 根据权利要求1所述的设备, 其中, 由所述分布式账本管理器至少部分地基于所述隐私设置来生成所述公共加密密钥。
3. 根据权利要求1-2中任一项所述的设备, 其中, 所述传感器包括以下中的一个或多个: 加速度计, 相机, 以及GPS传感器。
4. 根据权利要求1-3中任一项所述的设备, 其中, 所述元数据未被加密。
5. 一种用户设备, 包括:
 - 一个或多个计算机可读存储设备, 其被配置为存储计算机可执行指令;
 - 头戴式显示器;
 - 网络接口; 以及
 - 一个或多个硬件计算机处理器, 其与所述一个或多个计算机可读存储设备通信以执行所述计算机可执行指令以使所述用户设备:
 - 接收与第一用户相关联的隐私设置;
 - 经由所述网络接口向分布式账本管理器发送所述隐私设置以用于存储在分布式账本上;
 - 经由所述网络接口从所述分布式账本管理器接收与所述第一用户相关联的第一公共加密密钥;
 - 经由所述传感器收集与所述用户设备相关联的环境数据, 其中, 所述传感器被配置为检测所述用户设备的周围环境;
 - 基于所述第一公共加密密钥, 加密所述环境数据;
 - 用元数据来语义标记经加密的环境数据, 其中, 所述元数据至少指示关于所述用户设

备的标识信息;以及

经由所述网络接口向数据平台发送被语义标记的经加密的环境数据,其中,所述数据平台包括一个或多个数据库。

6. 根据权利要求5所述的设备,其中,由所述分布式账本管理器至少部分地基于所述隐私设置来生成所述公共加密密钥。

7. 根据权利要求5-6中任一项所述的设备,其中,所述传感器包括以下中的一个或多个:加速度计,相机,以及GPS传感器。

8. 根据权利要求5-7中任一项所述的设备,其中,所述元数据未被加密。

9. 一种方法,包括:

接收与第一用户相关联的隐私设置;

向分布式账本管理器发送所述隐私设置,其中,所述分布式账本管理器包括分布式账本和被配置为读取和写入所述分布式账本的软件;

从所述分布式账本管理器接收与所述第一用户相关联的第一公共加密密钥;

经由传感器收集与所述用户设备相关联的环境数据,其中,所述传感器被配置为检测所述用户设备的周围环境;

基于所述第一公共加密密钥,加密所述环境数据;

用元数据来语义标记经加密的环境数据,其中,所述元数据至少指示关于所述用户设备的标识信息;以及

向数据平台发送被语义标记的经加密的环境数据,其中,所述数据平台包括一个或多个数据库。

10. 根据权利要求9所述的方法,其中,由所述分布式账本管理器至少部分地基于所述隐私设置来生成所述公共加密密钥。

11. 根据权利要求9-10中任一项所述的方法,其中,所述传感器包括以下中的一个或多个:加速度计,相机,以及GPS传感器。

12. 根据权利要求9-11中任一项所述的方法,其中,所述元数据未被加密。

13. 一种系统,包括:

一个或多个计算机可读存储设备,其被配置为存储:

计算机可执行指令;

与用户相关联的隐私设置;

软件合约,其中,所述软件合约至少部分地基于所述隐私设置;

与所述用户相关联的私有加密密钥,其中,每个用户被分配一个私有加密密钥;

与所述用户相关联的公共加密密钥,其中,每个用户被分配一个公共加密密钥;以及

与所述用户相关联的用户数据;

网络接口;以及

一个或多个硬件计算机处理器,其与所述一个或多个计算机可读存储设备通信以执行所述计算机可执行指令以使所述系统:

经由所述网络接口从第一设备接收与所述用户中的第一用户相关联的第一隐私设置;

至少部分地基于所述第一隐私设置来创建第一软件合约,其中,所述第一软件合约被配置为实现所述第一隐私设置;

创建并加密与所述第一用户相关联的第一私有密钥；

存储第一软件合约和经加密的第一私有密钥；

创建与所述第一用户相关联的第一公共密钥；以及

经由所述网络接口向所述第一设备发送所述第一公共密钥，其中，所述第一设备被配置为收集第一用户数据并用第一元数据来语义标记所述第一用户数据。

14. 根据权利要求13所述的系统，其中，所述第一软件合约是智能合约。

15. 根据权利要求14所述的系统，其中，所述第一软件合约和经加密的第一私有密钥被存储在分布式账本中。

16. 根据权利要求13-15中任一项所述的系统，还包括：

数据平台，其包括一个或多个数据库；

其中，所述一个或多个硬件计算机处理器还被配置为使所述系统：

从所述第一设备接收第一用户数据，其中，用一个或多个语义标记来语义标记所述第一用户数据；

将第一用户数据存储在所述数据平台中，其中，所述数据平台与所述分布式账本分离；

计算并分配哈希标识值给所述第一用户数据；以及

在分布式账本中编码所述一个或多个语义标记和所述哈希标识值。

17. 根据权利要求13-16中任一项所述的系统，其中，所述第一隐私设置被加密。

18. 根据权利要求13-17中任一项所述的系统，其中，所述第一用户数据至少部分地基于由所述第一设备所收集的环境数据。

19. 根据权利要求13-18中任一项所述的系统，其中，所述第一用户数据被加密。

20. 根据权利要求13-19中任一项所述的系统，其中，所述第一元数据包括指示收集所述第一用户数据的日期和时间、收集所述第一用户数据的所述设备、以及所述数据是第一用户数据的指示的数据。

21. 一种方法，包括：

从第一设备接收与多个用户中的第一用户相关联的第一隐私设置，其中，所述多个用户中的每个用户与隐私设置、公共加密密钥和私有加密密钥相关联；

至少部分地基于所述第一隐私设置来创建第一软件合约，其中，所述第一软件合约被配置为实现所述第一隐私设置；

创建并加密与所述第一用户相关联的第一私有密钥；

存储第一软件合约和经加密的第一私有密钥；

创建与所述第一用户相关联的第一公共密钥；以及

向所述第一设备发送所述第一公共密钥，其中，所述第一设备被配置为收集第一用户数据并用第一元数据来语义标记所述第一用户数据。

22. 根据权利要求21所述的方法，其中，所述第一软件合约是智能合约。

23. 根据权利要求22所述的方法，其中，所述第一软件合约和经加密的第一私有密钥被存储在分布式账本中。

24. 根据权利要求21-23中任一项所述的方法，还包括：

接收第一用户数据，其中，用一个或多个语义标记来语义标记所述第一用户数据；

将第一用户数据存储在数据平台中，其中，所述数据平台与所述分布式账本分离并且

包括一个或多个数据库；

计算并分配哈希标识值给所述第一用户数据；以及

在分布式账本中编码所述一个或多个语义标记和所述哈希标识值。

25. 根据权利要求21-24中任一项所述的方法，其中，所述第一隐私设置被加密。

26. 根据权利要求21-25中任一项所述的方法，其中，所述第一用户数据至少部分地基于由所述第一设备所收集的环境数据。

27. 根据权利要求21-26中任一项所述的方法，其中，所述第一用户数据被加密。

28. 根据权利要求21-27中任一项所述的方法，其中，所述第一元数据包括指示收集所述第一用户数据的日期和时间、收集所述第一用户数据的所述设备、以及所述数据是第一用户数据的指示的数据。

29. 一种系统，包括：

一个或多个计算机可读存储设备，其被配置为存储：

计算机可执行指令；

与用户相关联的隐私设置；

软件合约，其中，所述软件合约至少部分地基于所述隐私设置；以及

与所述用户相关联的私有加密密钥，其中，每个用户被分配一个私有加密密钥；

数据虚拟化平台，其包括被配置为显示用户数据的用户界面；

数据平台，其被配置为存储与所述用户相关联的用户数据；

数据验证系统，其被配置为确定私有加密密钥是否与经加密的用户数据匹配，以使得能够用所述私有加密密钥来解密所述用户数据；

网络接口；以及

一个或多个硬件计算机处理器，其与所述一个或多个计算机可读存储设备通信以执行所述计算机可执行指令以使所述系统：

经由所述网络接口从所述数据虚拟化平台接收用于访问第一用户数据的请求，其中，所述第一用户数据与第一用户相关联；

搜索所述软件合约以定位所述软件合约中的与所述第一用户相关联的第一软件合约的最新版本；

基于所述搜索，至少部分地基于所述第一软件合约确定所述第一用户数据被允许共享；

准备并经由所述网络接口向所述数据虚拟化平台发送从所述数据平台提取所述第一用户数据的指令；

经由所述网络接口从所述数据平台接收所述第一用户数据已被加密并发送到所述数据虚拟化平台的确认，其中，所述确认包括所发送的所述第一用户数据的描述；

在接收到所述确认后，访问与所述第一用户相关联的第一私有加密密钥和所述第一软件合约；

经由所述网络接口向所述数据验证系统发送所述第一私有加密密钥和与所述第一软件合约相关联的细节；

经由所述网络接口从所述数据验证系统接收所述第一私有加密密钥和所述第一用户数据匹配的指示；以及

基于所接收的所述第一私有加密密钥和所述第一用户数据匹配的指示,经由所述网络接口向所述数据虚拟化平台发送所述第一私有加密密钥,以使得所述数据虚拟化平台能够解密从所述数据平台所接收的经加密的第一用户数据。

30. 根据权利要求29所述的系统,其中,包括所述第一私有加密密钥的所述私有加密密钥被存储在分布式账本中。

31. 根据权利要求29-30中任一项所述的系统,其中,包括所述第一软件合约的所述软件合约是智能合约。

32. 根据权利要求29-31中任一项所述的系统,其中,包括所述第一软件合约的所述软件合约被存储在分布式账本中。

33. 根据权利要求29-32中任一项所述的系统,其中,所述一个或多个硬件计算机处理器还被配置为使所述系统:

生成第二私有加密密钥;

生成并存储包括所述第二私有加密密钥的第二软件合约;以及

经由所述网络接口向所述数据平台发送所述第一私有加密密钥和第二私有加密密钥,以使得所述数据平台能够用所述第一私有加密密钥来解密所述第一用户数据并用所述第二私有加密密钥来重新加密所述第一用户数据。

34. 根据权利要求33所述的系统,其中,所述第二软件合约还存储被发送到所述数据虚拟化平台的所述第一用户数据的所述描述。

35. 根据权利要求29-34中任一项所述的系统,其中,至少部分地基于所述第一软件合约被确定为被允许共享的所述第一用户数据还至少部分地基于与访问所述数据虚拟化平台的购买者设备相关联的账户,其中,所述购买者设备与用于访问第一用户数据的请求相关联。

36. 一种方法,包括:

从数据虚拟化平台接收用于访问第一用户数据的请求,其中,所述第一用户数据与第一用户相关联,其中,所述数据虚拟化平台包括被配置为显示用户数据的用户界面;

搜索软件合约以定位所述软件合约中的与所述第一用户相关联的第一软件合约的最新版本,其中,所述软件合约至少部分地基于隐私设置;

基于所述搜索,至少部分地基于所述第一软件合约确定所述第一用户数据被允许共享;

准备并向所述数据虚拟化平台发送从数据平台提取所述第一用户数据的指令,其中,所述数据平台被配置为存储与所述用户相关联的用户数据;

从所述数据平台接收所述第一用户数据已被加密并被发送至所述数据虚拟化平台的确认,其中,所述确认包括被发送的所述第一用户数据的描述;

在接收到所述确认后,访问与所述第一用户相关联的第一私有加密密钥和所述第一软件合约;

向数据验证系统发送所述第一私有加密密钥和与所述第一软件合约相关联的细节,其中,所述数据验证系统被配置为确定私有加密密钥是否与经加密的用户数据匹配,以使得能够用所述私有加密密钥来解密所述用户数据;

从所述数据验证系统接收所述第一私有加密密钥和所述第一用户数据匹配的指示;以

及

基于所接收的所述第一私有加密密钥和所述第一用户数据匹配的指示,向所述数据虚拟化平台发送所述第一私有加密密钥,以使得所述数据虚拟化平台能够解密从所述数据平台所接收的经加密的第一用户数据。

37. 根据权利要求36所述的方法,其中,包括所述第一私有加密密钥的所述私有加密密钥被存储在分布式账本中。

38. 根据权利要求36-37中任一项所述的方法,其中,包括所述第一软件合约的所述软件合约是智能合约。

39. 根据权利要求36-38中任一项所述的方法,其中,包括所述第一软件合约的所述软件合约被存储在分布式账本中。

40. 根据权利要求36-39中任一项所述的方法,还包括:

生成第二私有加密密钥;

生成并存储包括所述第二私有加密密钥的第二软件合约;以及

向所述数据平台发送所述第一私有加密密钥和所述第二私有加密密钥,以使得所述数据平台能够用所述第一私有加密密钥来解密所述第一用户数据,并用所述第二私有加密密钥来重新加密所述第一用户数据。

41. 根据权利要求40所述的方法,其中,所述第二软件合约还存储被发送到所述数据虚拟化平台的所述第一用户数据的所述描述。

42. 根据权利要求36-41中任一项所述的方法,其中,至少部分地基于所述第一软件合约被确定为被允许共享的所述第一用户数据还至少部分地基于与访问所述数据虚拟化平台的购买者设备相关联的账户,其中,所述购买者设备与用于访问第一用户数据的请求相关联。

43. 一种系统,包括:

一个或多个计算机可读存储设备,其被配置为存储:

计算机可执行指令;

与用户相关联的隐私设置;

软件合约,其中,所述软件合约至少部分地基于所述隐私设置;以及

与所述用户相关联的公共加密密钥,其中,每个用户被分配一个公共加密密钥;

数据虚拟化平台,其包括被配置为显示用户数据的用户界面;

数据平台,其被配置为存储与所述用户相关联的用户数据;

网络接口;以及

一个或多个硬件计算机处理器,其与所述一个或多个计算机可读存储设备通信以执行所述计算机可执行指令以使所述系统:

经由所述网络接口从所述数据虚拟化平台接收用于访问第一用户数据的请求,其中,所述第一用户数据与第一用户相关联;

搜索所述软件合约以定位所述软件合约中的与所述第一用户相关联的第一软件合约,其中,所述第一软件合约是最新的版本;

基于所述搜索,至少部分地基于所述第一软件合约确定所述第一用户数据被允许共享,其中,所述第一用户数据包括来自一个或多个第三方服务的第一第三方数据;

准备并经由所述网络接口向所述数据虚拟化平台发送从所述一个或多个第三方服务提取所述第一第三方数据的指令；

经由所述网络接口从所述数据虚拟化平台接收所述第一第三方数据已被所述数据虚拟化平台成功取得的通知；

在接收到所述通知后，从所述第一软件合约取得第一公共加密密钥；以及

经由所述网络接口向所述数据虚拟化平台发送所述第一公共加密密钥，以使得所述数据虚拟化平台能够加密所述第三方数据并发送至所述数据平台以用于存储。

44. 根据权利要求43所述的系统，其中，包括所述第一公共加密密钥的所述公共加密密钥被存储在分布式账本中。

45. 根据权利要求43-44中任一项所述的系统，其中，包括所述第一软件合约的所述软件合约是智能合约。

46. 根据权利要求43-45中任一项所述的系统，其中，包括所述第一软件合约的所述软件合约被存储在分布式账本中。

47. 根据权利要求43-46中任一项所述的系统，其中，所述第三方数据包括社交媒体数据。

48. 根据权利要求43-47中任一项所述的系统，其中，所述一个或多个硬件计算机处理器还被配置为使所述系统：

在接收到所述通知后，存储描述与第三方数据的取得相关联的细节的数据。

49. 根据权利要求48所述的系统，其中，描述与第三方数据的取得相关联的细节的所述数据包括与所述第三方数据的提取、处理、剖析或标记、以及加密相关的信息。

50. 根据权利要求43-49中任一项所述的系统，其中，至少部分地基于所述第一软件合约被确定为被允许共享的所述第一用户数据还至少部分地基于与访问所述数据虚拟化平台的购买者设备相关联的账户，其中，所述购买者设备与用于访问第一用户数据的所述请求相关联。

51. 一种方法，包括：

从数据虚拟化平台接收用于访问第一用户数据的请求，其中，所述第一用户数据与第一用户相关联，其中，所述数据虚拟化平台包括被配置为显示用户数据的用户界面；

搜索软件合约以定位所述软件合约中的与所述第一用户相关联的第一软件合约，其中，所述第一软件合约是最新的版本；

基于所述搜索，至少部分地基于所述第一软件合约确定所述第一用户数据被允许共享，其中，所述第一用户数据包括来自一个或多个第三方服务的第一第三方数据；

准备并向所述数据虚拟化平台发送从所述一个或多个第三方服务提取所述第一第三方数据的指令；

从所述数据虚拟化平台接收所述第一第三方数据已被所述数据虚拟化平台成功取得的通知；

在接收到所述通知后，从所述第一软件合约取得第一公共加密密钥；以及

向所述数据虚拟化平台发送所述第一公共加密密钥，以使得所述数据虚拟化平台能够加密所述第三方数据并发送至数据平台以用于存储。

52. 根据权利要求51所述的方法，其中，包括所述第一公共加密密钥的所述公共加密密

钥被存储在分布式账本中。

53. 根据权利要求51-52中任一项所述的方法, 其中, 包括所述第一软件合约的所述软件合约是智能合约。

54. 根据权利要求51-53中任一项所述的方法, 其中, 包括所述第一软件合约的所述软件合约被存储在分布式账本中。

55. 根据权利要求51-54中任一项所述的方法, 其中, 所述第三方数据包括社交媒体数据。

56. 根据权利要求51-55中任一项所述的方法, 还包括:

在接收到所述通知后, 存储描述与第三方数据的取得相关联的细节的数据。

57. 根据权利要求56所述的方法, 其中, 描述与第三方数据的取得相关联的细节的所述数据包括与所述第三方数据的提取、处理、剖析或标记、以及加密相关的信息。

58. 根据权利要求51-57中任一项所述的方法, 其中, 至少部分地基于所述第一软件合约被确定为被允许共享的所述第一用户数据还至少部分地基于与访问所述数据虚拟化平台的购买者设备相关联的账户, 其中, 所述购买者设备与用于访问第一用户数据的请求相关联。

59. 一种数据平台, 包括:

一个或多个计算机可读存储设备, 其被配置为存储:

计算机可执行指令;

与用户相关联的公共加密密钥, 其中, 每个用户被分配一个公共加密密钥;

与所述用户相关联的用户数据; 以及

与所述用户数据相关联的标识值;

分布式账本管理器, 其包括分布式账本和被配置为读取和写入所述分布式账本的软件;

网络接口; 以及

一个或多个硬件计算机处理器, 其与所述一个或多个计算机可读存储设备通信以执行所述计算机可执行指令以使所述数据平台:

经由所述网络接口从第一设备接收所述用户数据中的第一用户数据, 其中, 所述第一用户数据包括被加密并且用第一元数据来语义标记的数据;

在所述一个或多个计算机可读存储设备中存储所述第一用户数据;

计算用于所述第一用户数据的标识值, 其中, 所述标识值基于哈希算法;

将所述标识值分配给所述第一用户数据;

在所述一个或多个计算机可读存储设备中存储所计算的标识值; 以及

经由所述网络接口向所述分布式账本管理器发送交易数据, 其中, 所述交易数据包括所计算的标识值、所述第一元数据、以及与所述第一用户数据从所述第一用户设备到所述数据平台的传递相关的信息。

60. 根据权利要求59所述的数据平台, 其中, 所述第一元数据包括指示收集所述第一用户数据的日期和时间、收集所述第一用户数据的所述设备、以及所述数据是第一用户数据的指示的数据。

61. 根据权利要求59-60中任一项所述的数据平台, 其中, 基于与所述第一用户相关联的

第一公共加密密钥加密所述第一用户数据。

62. 根据权利要求59-61中任一项所述的数据平台,其中,所述分布式账本管理器被配置为将所述交易数据编码到分布式账本中。

63. 根据权利要求59-62中任一项所述的数据平台,其中,所述第一用户数据至少部分地基于由所述第一设备所收集的环境数据。

64. 一种方法,包括:

从第一设备接收第一用户数据,其中,所述第一用户数据包括被加密并且用第一元数据来语义标记的数据;

在所述一个或多个计算机可读存储设备中存储所述第一用户数据;

计算用于所述第一用户数据的标识值,其中,所述标识值基于哈希算法;

将所述标识值分配给所述第一用户数据;

在所述一个或多个计算机可读存储设备中存储所计算的标识值;以及

经由所述网络接口向分布式账本管理器发送交易数据,其中,所述交易数据包括所计算的标识值、所述第一元数据、以及与所述第一用户数据从所述第一用户设备到所述数据平台的传递相关的信息,其中,所述分布式账本管理器包括分布式账本和被配置为读取和写入所述分布式账本的软件。

65. 根据权利要求64所述的方法,其中,所述第一元数据包括指示收集所述第一用户数据的日期和时间、收集所述第一用户数据的所述设备、以及所述数据是第一用户数据的指示的数据。

66. 根据权利要求64-65中任一项所述的方法,其中,基于与所述第一用户相关联的第一公共加密密钥加密所述第一用户数据。

67. 根据权利要求64-66中任一项所述的方法,其中,所述分布式账本管理器被配置为将所述交易数据编码到分布式账本中。

68. 根据权利要求64-67中任一项所述的方法,其中,所述第一用户数据至少部分地基于由所述第一设备所收集的环境数据。

69. 一种数据平台,包括:

一个或多个计算机可读存储设备,其被配置为存储:

可执行指令;

与用户相关联的用户数据;以及

数据虚拟化平台,其包括配置为显示用户数据的用户界面;

数据验证系统,其被配置为确定私有加密密钥是否与经加密的用户数据匹配,以使得能够用所述私有加密密钥来解密所述用户数据;

网络接口;以及

一个或多个硬件计算机处理器,其与所述一个或多个计算机可读存储设备通信以执行所述计算机可执行指令以使所述数据平台:

经由所述网络接口从所述数据虚拟化平台接收用于访问第一用户数据的至少一部分的第一请求,其中,所述第一用户数据与第一用户相关联;

在接收到所述第一请求后,至少部分地基于所述第一请求在所述一个或多个计算机可读存储设备中定位所述第一用户数据,其中,所述第一用户数据是先前从第一设备接收并

在接收后被存储的；

经由所述网络接口向所述数据虚拟化平台发送所述第一用户数据的至少一部分，其中，所述第一用户数据被加密并用第一元数据来语义标记；以及

经由所述网络接口向数据验证系统发送所述第一用户数据的所述至少一部分到所述数据虚拟化平台的成功传输的确认以及描述所述第一用户数据的哪一部分被发送的信息，其中，所述数据验证系统被配置为验证所述第一用户数据的所述至少一部分和与所述第一用户匹配相关联的第一私有加密密钥匹配。

70. 根据权利要求69所述的数据平台，其中，所述第一元数据包括指示收集所述第一用户数据的日期和时间、收集所述第一用户数据的所述设备、以及所述数据是第一用户数据的指示的数据。

71. 根据权利要求69-70中任一项所述的数据平台，其中，基于与所述第一用户相关联的第一公共加密密钥来加密所述第一用户数据。

72. 根据权利要求69-71中任一项所述的数据平台，其中，由所述数据验证系统执行的验证匹配包括：确定所述第一私有加密密钥能够解密所述第一用户数据的所述至少一部分。

73. 根据权利要求69-72中任一项所述的数据平台，还包括：

分布式账本管理器，其包括分布式账本和被配置为读取和写入所述分布式账本的软件；

其中，所述一个或多个硬件计算机处理器还被配置为使所述数据平台：

经由所述网络接口从所述分布式账本管理器接收所述第一私有加密密钥和第二私有加密密钥，其中，所述第一私有加密密钥和所述第二私有加密密钥与所述第一用户相关联；

在所述一个或多个计算机可读存储设备中定位所述第一用户数据，其中，所述第一用户数据是先前从第一设备接收并在接收后被存储的；

用所述第一私有加密密钥来解密所述第一用户数据；

用所述第二私有加密密钥来加密被解密的第一用户数据；以及

在所述一个或多个计算机可读存储设备中存储用所述第二私有加密密钥加密的所述第一用户数据。

74. 根据权利要求69-73中任一项所述的数据平台，其中，所述一个或多个硬件计算机处理器还被配置为使所述数据平台：

经由所述网络接口从所述数据虚拟化平台接收用于访问通用用户数据的第二请求，其中，所述通用用户数据包括与所述用户数据相关联的去标识化和假名化的数据，并且不能用于标识所述用户中的任何用户；

至少部分地基于所述请求，在所述一个或多个计算机可读存储设备中定位所述通用用户数据；以及

经由所述网络接口向所述数据虚拟化平台发送所述通用用户数据的至少一部分。

75. 根据权利要求69-74中任一项所述的数据平台，其中，所述数据平台还包括所述数据验证系统。

76. 根据权利要求69-75中任一项所述的数据平台，其中，所述第一请求至少部分地基于与所述第一用户相关联的第一软件合约。

77. 根据权利要求69-76中任一项所述的数据平台,其中,被发送的所述第一用户数据的所述至少一部分至少部分地基于与所述第一用户相关联的第一软件合约。

78. 根据权利要求69-77中任一项所述的数据平台,其中,被发送的所述第一用户数据的所述至少一部分至少部分地基于与访问所述数据虚拟化平台的购买者设备相关联的账户,其中,所述购买者设备与用于访问第一用户数据的所述请求相关联。

79. 一种方法,包括:

从数据虚拟化平台接收用于访问第一用户数据的至少一部分的第一请求,其中,所述第一用户数据与第一用户相关联,其中,所述数据虚拟化平台包括被配置为显示用户数据的用户界面;

在接收到所述第一请求后,至少部分地基于所述第一请求在一个或多个计算机可读存储设备中定位所述第一用户数据,其中,所述第一用户数据是先前从第一设备接收并在接收后被存储的;

向所述数据虚拟化平台发送所述第一用户数据的至少一部分,其中,所述第一用户数据被加密并用第一元数据来语义标记;以及

向数据验证系统发送所述第一用户数据的所述至少一部分到所述数据虚拟化平台的成功传输的确认以及描述所述第一用户数据的哪一部分被发送的信息,其中,所述数据验证系统被配置为验证所述第一用户数据的所述至少一部分和与所述第一用户匹配相关联的第一私有加密密钥匹配,以及其中,所述数据验证系统还被配置为确定私有加密密钥是否与经加密的用户数据匹配,以使得所述用户数据能够用所述私有加密密钥来解密。

80. 根据权利要求79所述的方法,其中,所述第一元数据包括指示收集所述第一用户数据的日期和时间、收集所述第一用户数据的所述设备、以及所述数据是第一用户数据的指示的数据。

81. 根据权利要求79-80中任一项所述的方法,其中,基于与所述第一用户相关联的第一公共加密密钥加密所述第一用户数据。

82. 根据权利要求79-81中任一项所述的方法,其中,由所述数据验证系统执行的验证匹配包括:确定所述第一私有加密密钥能够解密所述第一用户数据的所述至少一部分。

83. 根据权利要求79-82中任一项所述的方法,还包括:

从分布式账本管理器接收所述第一私有加密密钥和第二私有加密密钥,其中,所述第一私有加密密钥和所述第二私有加密密钥与所述第一用户相关联,以及其中,所述分布式账本管理器包括分布式账本和被配置为读取并写入所述分布式账本的软件;

在所述一个或多个计算机可读存储设备中定位所述第一用户数据,其中,所述第一用户数据是先前从第一设备接收并在接收后被存储的;

用所述第一私有加密密钥来解密所述第一用户数据;

用所述第二私有加密密钥来加密被解密的第一用户数据;以及

在所述一个或多个计算机可读存储设备中存储用所述第二私有加密密钥加密的所述第一用户数据。

84. 根据权利要求79-83中任一项所述的方法,还包括:

从所述数据虚拟化平台接收用于访问通用用户数据的第二请求,其中,所述通用用户数据包括与所述用户数据相关联的去标识化和假名化的数据,并且不能用于标识所述用户

中的任何用户；

至少部分地基于所述请求，在所述一个或多个计算机可读存储设备中定位所述通用用户数据；以及

向所述数据虚拟化平台发送所述通用用户数据的至少一部分。

85. 根据权利要求79-84中任一项所述的方法，其中，所述数据平台还包括所述数据验证系统。

86. 根据权利要求79-85中任一项所述的方法，其中，所述第一请求至少部分地基于与所述第一用户相关联的第一软件合约。

87. 根据权利要求79-86中任一项所述的方法，其中，被发送的所述第一用户数据的所述至少一部分至少部分地基于与所述第一用户相关联的第一软件合约。

88. 根据权利要求79-87中任一项所述的方法，其中，被发送的所述第一用户数据的所述至少一部分至少部分地基于与访问所述数据虚拟化平台的购买者设备相关联的账户，其中，所述购买者设备与用于访问第一用户数据的所述请求相关联。

89. 一种数据虚拟化平台，包括：

一个或多个计算机可读存储设备，其被配置为存储：

计算机可执行指令；

与用户相关联的私有加密密钥，其中，每个用户被分配一个私有加密密钥；以及

与所述用户相关联的用户数据；

分布式账本管理器，其包括分布式账本和被配置为读取和写入所述分布式账本的软件；

数据平台，其包括一个或多个数据库；

网络接口；以及

一个或多个硬件计算机处理器，其与所述一个或多个计算机可读存储设备通信以执行所述计算机可执行指令以使所述数据虚拟化平台：

经由所述网络接口从所述分布式账本管理器接收所述私有加密密钥中的第一私有加密密钥，其中，所述第一私有加密密钥与第一用户相关联；

经由所述网络接口从所述分布式账本管理器接收从所述数据平台取得所述用户数据中的第一用户数据的指令，其中，所述第一用户数据与第一用户相关联；

基于所接收的指令，准备并经由所述网络接口向所述数据平台发送针对所述第一用户数据的第一请求；

基于所述第一请求，经由所述网络接口从所述数据平台接收所述第一用户数据，其中，所述第一用户数据被加密；

用所述第一私有加密密钥和从所述数据平台接收的所述第一用户数据来解密所述第一用户数据；

处理被解密的第一用户数据，以对所述第一用户数据进行去标识化和假名化；以及

通过验证不可能基于去标识化和假名化的第一用户数据而标识所述第一用户，确定所处理的第一用户数据。

90. 根据权利要求89所述的数据虚拟化平台，其中，所述一个或多个硬件计算机处理器还被配置为：

经由所述网络接口从所述分布式账本管理器接收所述私有加密密钥中的第二私有加密密钥,其中,所述第二私有加密密钥与第二用户相关联;

经由所述网络接口从所述分布式账本管理器接收从所述数据平台取得所述用户数据中的第二用户数据的第一指令,其中,所述第二用户数据与第二用户相关联;

基于所接收的第一指令,准备并经由所述网络接口向所述数据平台发送针对所述第二用户数据的第二请求;

基于所述第二请求,经由所述网络接口从所述数据平台接收所述第二用户数据,其中,所述第二用户数据被加密;

用所述第二私有加密密钥和从所述数据平台接收的所述第二用户数据来解密所述第二用户数据;

处理被解密的第二用户数据,以对所述第二用户数据进行去标识化和假名化;以及

通过验证不可能基于去标识化和假名化的第二用户数据而标识所述第二用户,确定所处理的第二用户数据。

91. 根据权利要求90所述的数据虚拟化平台,其中,所述一个或多个硬件计算机处理器还被配置为:

验证不可能基于去标识化和假名化的第一用户数据而标识所述第一用户。

92. 根据权利要求89-91中任一项所述的数据虚拟化平台,其中,所述一个或多个硬件计算机处理器还被配置为:

在电子用户界面上显示所处理的第一用户数据。

93. 根据权利要求89-92中任一项所述的数据虚拟化平台,其中,所述一个或多个硬件计算机处理器还被配置为:

经由所述电子用户界面接收第二指令,以终止所述所处理的第一用户数据的使用;以及

基于所接收的第二指令,删除与所述第一用户相关联的任何数据,包括所述所处理的第一用户数据和第一私有加密密钥。

94. 根据权利要求89-93中任一项所述的数据虚拟化平台,其中,所述一个或多个硬件计算机处理器还被配置为:

进一步处理所处理的第一用户数据以创建经分析的第一用户数据,其中,所述经分析的第一用户数据包括具有被应用于所述数据的一个或多个分析工具的所处理的第一用户数据,其中,所述一个或多个分析工具包括以下中的一个或多个:聚合,预分析,和情境化;

用元数据对所述经分析的第一用户数据进行编码,其中,所述元数据至少指示所述经分析的第一用户数据与第一用户相关联;以及

监控经分析的第一用户数据以防止从所述数据虚拟化平台未经授权地导出所述经分析的第一用户数据的一些或全部。

95. 根据权利要求94所述的数据虚拟化平台,其中,所述一个或多个硬件计算机处理器还被配置为:

从所述数据虚拟化平台接收发送分析数据的第三请求,其中,所述分析数据包括与由所述数据虚拟化平台运行的分析相关联的结果和与所述第一用户相关联的数据;以及

基于所述第三请求,发送与由所述数据虚拟化平台运行的所述分析相关联的数据,而

不发送与所述第一用户相关联的所述数据。

96. 根据权利要求95所述的数据虚拟化平台, 其中, 所述一个或多个硬件计算机处理器还被配置为:

经由所述电子用户界面接收第三指令, 以终止所述所处理的第一用户数据的使用; 以及

基于所接收的第三指令, 删除与所述第一用户相关联的任何数据, 包括所述所处理的第一用户数据和第一私有加密密钥。

97. 根据权利要求89-96中任一项所述的数据虚拟化平台, 其中, 取得第一用户数据的指令至少部分地基于与所述第一用户相关联的第一软件合约。

98. 根据权利要求89-97中任一项所述的数据虚拟化平台, 其中, 取得第一用户数据的指令至少部分地基于与访问所述数据虚拟化平台的购买者设备相关联的账户, 其中, 所述购买者设备是与用于访问第一用户数据的所述请求相关联。

99. 一种方法, 包括:

从分布式账本管理器接收私有加密密钥中的第一私有加密密钥, 其中, 所述第一私有加密密钥与第一用户相关联, 以及其中, 所述分布式账本管理器包括分布式账本和被配置为读取和写入所述分布式账本的软件;

从所述分布式账本管理器接收从数据平台取得用户数据中的第一用户数据的指令, 其中, 所述第一用户数据与第一用户相关联, 以及其中, 所述数据平台包括一个或多个数据库;

基于所接收的指令, 准备并向所述数据平台发送针对所述第一用户数据的第一请求;

基于所述第一请求, 从所述数据平台接收所述第一用户数据, 其中, 所述第一用户数据被加密;

用所述第一私有加密密钥和从所述数据平台接收的所述第一用户数据来解密所述第一用户数据;

处理被解密的第一用户数据, 以对所述第一用户数据进行去标识化和假名化; 以及

通过验证不可能基于去标识化和假名化的第一用户数据而标识所述第一用户, 确定所处理的第一用户数据。

100. 根据权利要求99所述的方法, 还包括:

从所述分布式账本管理器接收所述私有加密密钥中的第二私有加密密钥, 其中, 所述第二私有加密密钥与第二用户相关联;

从所述分布式账本管理器接收从所述数据平台取得所述用户数据中的第二用户数据的第一指令, 其中, 所述第二用户数据与第二用户相关联;

基于所接收的第一指令, 准备并向所述数据平台发送针对所述第二用户数据的第二请求;

基于所述第二请求, 从所述数据平台接收所述第二用户数据, 其中, 所述第二用户数据被加密;

用所述第二私有加密密钥和从所述数据平台接收的所述第二用户数据来解密所述第二用户数据;

处理被解密的第二用户数据, 以对所述第二用户数据进行去标识化和假名化; 以及

通过验证不可能基于去标识化和假名化的第二用户数据而标识所述第二用户,确定所处理的第二用户数据。

101. 根据权利要求100所述的方法,其中,所述一个或多个硬件计算机处理器还被配置为:

验证不可能基于去标识化和假名化的第一用户数据而标识所述第一用户。

102. 根据权利要求99-101中任一项所述的方法,还包括:

在电子用户界面上显示所处理的第一用户数据。

103. 根据权利要求99-102中任一项所述的方法,还包括:

经由所述电子用户界面接收第二指令,以终止所述所处理的第一用户数据的使用;以及

基于所接收的第二指令,删除与所述第一用户相关联的任何数据,包括所述所处理的第一用户数据和第一私有加密密钥。

104. 根据权利要求99-103中任一项所述的方法,还包括:

进一步处理所述所处理的第一用户数据以创建经分析的第一用户数据,其中,所述经分析的第一用户数据包括具有被应用于所述数据的一个或多个分析工具的所处理的第一用户数据,其中,所述一个或多个分析工具包括以下中的一个或多个:聚合,预分析,和情境化;

用元数据编码所述经分析的第一用户数据,其中,所述元数据至少指示所述经分析的第一用户数据与第一用户相关联;以及

监控经分析的第一用户数据以防止从所述数据虚拟化平台未经授权地导出所述经分析的第一用户数据的一些或全部。

105. 根据权利要求104所述的方法,还包括:

从所述数据虚拟化平台接收发送分析数据的第三请求,其中,所述分析数据包括与由所述数据虚拟化平台运行的分析相关联的结果和与所述第一用户相关联的数据;以及

基于所述第三请求,发送与由所述数据虚拟化平台运行的所述分析相关联的数据,而不发送与所述第一用户相关联的所述数据。

106. 根据权利要求105所述的方法,还包括:

经由所述电子用户界面接收第三指令,以终止所述所处理的第一用户数据的使用;以及

基于所接收的第三指令,删除与所述第一用户相关联的任何数据,包括所述所处理的第一用户数据和第一私有加密密钥。

107. 根据权利要求99-106中任一项所述的方法,其中,取得第一用户数据的指令至少部分地基于与所述第一用户相关联的第一软件合约。

108. 根据权利要求99-107中任一项所述的方法,其中,取得第一用户数据的指令至少部分地基于与访问所述数据虚拟化平台的购买者设备相关联的账户,其中,所述购买者设备与用于访问第一用户数据的所述请求相关联。

109. 一种数据虚拟化平台,包括:

一个或多个计算机可读存储设备,其被配置为存储:

计算机可执行指令;以及

与用户相关联的用户数据;

分布式账本管理器,其包括分布式账本和被配置为读取和写入所述分布式账本的软件;

网络接口;以及

一个或多个硬件计算机处理器,其与所述一个或多个计算机可读存储设备通信以执行所述计算机可执行指令以使所述数据虚拟化平台:

经由所述网络接口从所述分布式账本管理器接收从一个或多个第三方服务中的第一第三方服务取得第三方数据的第一指令,其中,所述第三方数据与第一用户相关联;

基于所述指令,从与所述第一用户相关联的所述第一第三方服务取得第三方数据;

处理所述第三方数据以用元数据编码所述第三方数据,其中,所述元数据指示从其取得所述第三方数据的所述第三方服务并且所述第三方数据与所述第一用户相关联;

将第三方数据与先前取得的与所述第一用户相关联的数据相结合;以及

经由所述网络接口向所述分布式账本管理器发送所取得的第三方数据的通知,其中,所述通知包括取得所述第三方数据的时间和从其取得所述第三方数据的所述服务。

110. 根据权利要求109所述的数据虚拟化平台,其中,所述一个或多个第三方服务包括社交媒体服务。

111. 根据权利要求109-110中任一项所述的数据虚拟化平台,其中,取得第三方数据的指令包括与所述第一第三方服务相关联的第一用户账户信息。

112. 根据权利要求109-111中任一项所述的数据虚拟化平台,其中,取得第三方数据的指令包括关于如何执行对所述第一第三方服务的至少一个API调用的指令。

113. 根据权利要求109-112中任一项所述的数据虚拟化平台,其中,所述一个或多个硬件计算机处理器还被配置为:

处理所述第三方数据以移除所述数据虚拟化平台不需要的任何额外信息。

114. 根据权利要求109-113中任一项所述的数据虚拟化平台,其中,所述一个或多个硬件计算机处理器还被配置为:

处理所述第三方数据以将所述数据格式化为所述数据虚拟化平台所优选的配置。

115. 一种数据虚拟化平台,包括:

从分布式账本管理器接收从一个或多个第三方服务中的第一第三方服务取得第三方数据的第一指令,其中,所述第三方数据与第一用户相关联,其中,所述分布式账本管理器包括分布式账本以及被配置为读取和写入所述分布式账本的软件;

基于所述指令,从与所述第一用户相关联的所述第一第三方服务取得第三方数据;

处理所述第三方数据以用元数据编码所述第三方数据,其中,所述元数据指示从其取得所述第三方数据的所述第三方服务并且所述第三方数据与所述第一用户相关联;

将第三方数据与先前取得的与所述第一用户相关联的数据相结合;以及

向所述分布式账本管理器发送所取得的第三方数据的通知,其中,所述通知包括取得所述第三方数据的时间和从其取得所述第三方数据的所述服务。

116. 根据权利要求115所述的方法,其中,所述一个或多个第三方服务包括社交媒体服务。

117. 根据权利要求115-116中任一项所述的方法,其中,取得第三方数据的所述指令包

括与所述第一第三方服务相关联的第一用户账户信息。

118. 根据权利要求115-117中任一项所述的方法, 其中, 取得第三方数据的所述指令包括关于如何执行对所述第一第三方服务的至少一个API调用的指令。

119. 根据权利要求115-118中任一项所述的方法, 还包括:

处理所述第三方数据以移除所述数据虚拟化平台不需要的任何额外信息。

120. 根据权利要求115-119中任一项所述的方法, 还包括:

处理所述第三方数据以将所述数据格式化为所述数据虚拟化平台所优选的配置。

使用分布式账本用于增强现实的用户数据管理

[0001] 相关申请的交叉引用

[0002] 本申请要求于2019年7月31日提交的题为“USER DATA MANAGEMENT FOR AUGMENTED REALITY USING A DISTRIBUTED LEDGER”的美国专利申请第62/881,025号的优先权,其全部内容通过引用并入本文。

[0003] 有限版权声明

[0004] 该专利文件的公开内容的一部分包含受版权保护的材料。版权所有者不反对任何人传真复制出现在美国专利和商标局专利文件或记录中的专利文件或专利公开,但除此之外保留所有版权。

技术领域

[0005] 本公开涉及用于安全数据存储、传输和访问的系统和方法,并且特别涉及用于基于规则的数据存储、传输和访问的系统和方法。该系统和方法可以用于增强、混合或虚拟现实环境中。

背景技术

[0006] 公司收集关于其用户或客户的大量用户数据。例如,该用户数据可用于构建计算机模型、定向广告、或统计分析。公司收集和出售该用户数据以获取利润,这可能以用户隐私为代价,并且可能是在用户不知情的情况下。最近,收集和出售用户数据的许多公司要么以误导性方式出售数据,要么被盗取数据并随后在黑市上出售的第三方侵犯或入侵。

发明内容

[0007] 在此公开了用于使用分布式账本设置、访问和修改用户隐私设置的系统和方法。在一方面,系统可以接收与用户相关联的隐私设置,并且至少部分地基于隐私设置来创建软件合约。然后系统可以创建私有密钥和公共密钥。该系统可以将软件合约和私有密钥存储在分布式账本中,并将公共密钥发送到被配置为收集用户数据并采用元数据对用户数据进行语义标记的设备。

[0008] 在另一方面,系统可以从数据虚拟化平台接收访问针对特定用户的用户数据的请求。然后,系统可以搜索先前存储的软件合约以定位与用户相关联的软件合约的最新的版本,并且基于搜索确定允许共享的用户数据。然后系统可以向数据虚拟化平台发送关于如何从数据平台提取用户数据的指令。然后,系统可以从数据平台接收用户数据被发送到数据虚拟化平台的确认,并且然后系统可以访问与用户相关联的软件合约和私有加密密钥。然后系统可以向数据验证系统发送私有加密密钥和与软件合约相关联的细节,并且然后从数据验证系统接收私有加密密钥和用户数据匹配的指示。然后,基于所接收的私有加密密钥与用户数据匹配的指示,向数据虚拟化平台发送私有加密密钥,使得数据虚拟化平台可以解密从数据平台所接收的经加密的用户数据。

[0009] 在另一方面,系统可以从数据虚拟化平台接收访问与特定用户相关联的用户数据

的请求。然后,系统可以搜索先前存储的软件合约以定位与用户相关联的软件合约,并基于搜索确定允许共享的用户数据。在一些方面,用户数据可以包括来自一个或多个第三方服务的第三方数据。然后,系统可以准备并向数据虚拟化平台发送关于如何从一个或多个第三方服务提取第三方数据的指令,并从数据虚拟化平台接收第三方数据已被数据虚拟化平台成功取得的通知。在接收到通知后,系统可从软件合约取得公共加密密钥,并向数据虚拟化平台发送公共加密密钥,使得数据虚拟化平台可加密第三方数据,并向数据平台发送用于存储的第三方数据。

[0010] 在此描述的增强现实、虚拟现实和混合现实系统仅作为示例并且不应被解释为将实施例或方面限制于所描述的特定技术。因此,应当理解,尽管在此描述了增强现实、虚拟现实和混合现实系统,但是实施例和公开可以应用于收集或生成数据的任何消费电子设备。

[0011] 本说明书中描述的主题的一个或多个实现方式的细节在附图和以下描述中阐述。其它特征、方面和优点将从描述、附图和权利要求中变得显而易见。该概要和以下详细描述均不旨在定义或限制本公开主题的范围。下面参考可用作本公开的附加概要的所附权利要求描述了本公开的附加实施例。

附图说明

[0012] 图1示出用户数据交易系统的示例并且包括系统的组件之间的交互和数据传输的示例。

[0013] 图2A示出用于为用户创建或更新隐私设置的示例方法的流程图。

[0014] 图2B-2C示出用于为用户创建或更新隐私设置的示例方法的泳道流程图。

[0015] 图3示出用于定位、发送和解密用户数据的示例方法的流程图。某些附加的或替代的框在图4、6A和6B中描绘。

[0016] 图4示出用于生成新的私有加密密钥并采用新的私有加密密钥重新加密用户数据的方法的流程图。某些附加的或替代的步骤在图3中描绘。

[0017] 图5示出用于采用从一个或多个第三方服务取得的社交媒体数据来丰富用户数据的方法的流程图。某些附加的或替代的步骤在图6B中描绘。

[0018] 图6A示出了用于验证、处理和监控用户数据的方法的流程图。某些附加的或替代的步骤在图3中描绘。

[0019] 图6B示出用于处理对去标识化和假名化的用户数据的请求的方法的示例的流程图。某些附加的或替代的步骤在图3和5中描绘。

[0020] 图7A示出空间计算设备或可穿戴显示系统的示例。

[0021] 图7B示意性地示出用户数据交易系统的一个实施例。

[0022] 图8示出可以实现在此讨论的某些方法的计算机系统。

[0023] 在整个附图中,参考数字可以重新用于指示参考元件之间的对应关系。提供附图以说明在此描述的示例实施例并且不旨在限制本公开的范围。

具体实施方式

[0024] 概述

[0025] 空间计算设备以及向公司的用户或客户提供此类设备的公司可以收集与此类用户相关的用户数据,其可以包括环境数据或基于空间计算设备的周围环境的数据。用户将在空间计算设备上生成并与之交互的用户数据的类型可能比当今许多其它平台或服务上可用的数据更加敏感和有价值。例如,用户数据更敏感,因为它可能提供关于用户环境(例如,用户的家、卧室、办公室、附近人的脸和身体等)和用户的个人身份(例如,用户的关于产品、人员、地点、用户个人标识数据等的个人偏好)的信息。用户数据还可以提供关于用户的身体能力的信息(例如,用户是否需要眼镜,或者用户可能需要的处方、用户的身高、用户的体重、用户的步幅、用户的身体看起来如何等)。在一些示例中,用户数据可以提供关于用户健康的信息(例如,心跳、通过用户皮肤对用户血液的分析等)。可能希望以提供对如何使用用户数据的控制的方式来保护该信息。对于空间计算设备或相关联的系统来说,允许用户控制该信息的保护级别可能是有利的,使得用户基于用户的个人隐私偏好来控制数据收集和/或用户数据的共享。例如,在一些实施例,用户可以提供可更新的隐私设置,该可更新的隐私设置可以被存储在不可变的分布式账本上,其中对隐私设置的附加更改可以被添加到新的存储位置,并且还可以查看先前的隐私设置。

[0026] 通过使用支持软件合约(例如,智能合约等)的公共密钥密码术和公共分布式账本技术(例如,区块链、比特币、以太坊、缠结(Tangle)等),用户可以保持对自己数据的控制和隐私。例如,用户可以控制他们的数据(例如从他们那里收集的用户数据)是否可用或完全共享,管理谁可以访问它,管理数据的哪些部分可以被访问或共享,管理数据的哪些部分可以对谁访问,以及用户可以从提供对一些或全部数据的访问中受益。此外,这里描述的系统和方法还可以促进此类服务的提供商(例如,收集或收集用户数据的公司、受雇管理用户数据的第三方公司等)与选择使用收集用户数据的设备的人之间的信任。

[0027] 软件合约(例如,智能合约、以太坊智能合约、图灵(Turing)完备的智能合约等)和密钥密码术的组合可以提供可以扩展(scale)以包括最多产的数据集的解决方案。在此所述的系统和方法可以提供一种用户友好的方式来维持对用户的用户数据的访问、控制。

[0028] 在一些实施例中,密钥密码术(例如,公共密钥密码术等)可以被配置为生成一对加密密钥:用于平台的每个用户的公共密钥和私有密钥。公共密钥可以公开共享,但私有密钥旨在仅由用户控制。密钥密码术的一个益处可以包括数据机密性,使得将用户数据保密。例如,用户可以使用他们之前生成的公共密钥来加密他们的用户数据,并且只有该用户能够在稍后的时间点使用他们的私有密钥来解密用户数据。密钥密码术的另一个益处可以包括数据真实性,用户可以使用他们的私有密钥对某些数据进行数字签名,以便证明他们授权该数据。

[0029] 分布式账本与软件合约支持相结合,可以提供无需许可、无需信任、抗审查且不可变的账本,该账本可被配置为跟踪账户余额状态并促进智能合约从一个有效状态到另一个有效状态的转换。分布式账本(有时称为共享账本或分布式账本技术或DLT,并且还可以包括缠结和其它形式的分布式存储)可以是在地理上分布在多个站点、国家或机构的复制、共享和同步数字数据的共识。分布式账本设计的一种形式是区块链系统,其可以是公共的,也可以是私有的。账本可以分布在对等网络中,并且可以包括分布在多个节点(设备)上的分布式数据库、有向无环图(DAG)或其它数据结构。如上所述,数据机密性和真实性可以由分布式账本提供,并且也可以经由密钥密码术在分布式账本的上下文之外使用。在信息安全

的上下文中,分布式账本还可以提供改进的数据完整性和不可否认性。公共分布式账本技术的一个益处可以包括,例如,通过确保数据不会在未许可的情况下被操纵,从而实现数据完整性。公共分布式账本技术的另一个益处可以包括,例如,数据可用性和可访问性,其中用户可以通过互联网用户连接和访问分布式账本上的数据。例如,中央组织不能阻止或授予任何一方对分布式账本的特殊权限。公共分布式账本技术的另一个益处可以包括例如抗审查。例如,中央组织无法控制谁可以和不可以在区块链上存储数据。

[0030] 目前,分布式账本技术具有其局限性。例如,该技术可能很昂贵(例如,交易费用可能很高),不完全安全(例如,51%攻击、链分叉的可能性等),不完全可扩展,并且比采用数据库的传统集中式服务要慢。分布式账本技术的改进正在进行中,并可能影响在此所述的系统和方法。当前对分布式账本技术的限制不应被解释为对在此描述的系统和方法的限制。

[0031] 对分布式账本技术的改进将转化为对在此描述的系统和方法的改进。例如,一些改进可能包括:较低的交易费用、提高的安全性(例如,实现区块链终结性、抵抗51%攻击、限制分叉的可能性等)、提高的可扩展性(例如,通过使用和实施分片、不同的共识机制等)、或可以直接或间接改进在此描述的系统和方法的其它新特征或益处。

[0032] 目前,由于在分布式账本上存储大量数据可能是昂贵或繁琐的,因此希望实现一种解决方案,该解决方案将数据存储在有数据库的安全服务器上,但可以将用户的隐私设置存储在分布式账本上。然而,应该理解,随着分布式账本技术改进,用户的隐私设置和用户数据都可以经由分布式账本进行存储和访问。

[0033] 此外,对人类可用且易于学习的计算机用户界面的设计可能具有挑战性。本公开的交互式 and 动态用户界面的各种实施例是重要的研究、开发、改进、迭代和测试的结果。该非平凡的发展导致在此描述的用户界面可以提供显著的认知和人体工程学效率以及优于先前系统的优势。交互式 and 动态用户界面包括改进的人机交互,其可以为用户提供减少的心理工作量、改进的决策制定、减少的工作压力等。例如,与在此描述的交互式用户界面的用户交互可以提供资源相关性或数据转换、关系的优化显示,并且可以使用户能够比以前的系统更快速地访问、导航、评估和消化此类信息。

[0034] 在此所述的系统和方法的一个益处是数据平台的运营商、与空间计算设备相关联的服务、以及收集用户数据的任何相关服务将无法直接访问用户数据,因为数据将被加密并运营商将没有适当的密钥来解密用户数据。例如,此类实现方式的益处是,在侵犯期间,如果用户数据被盗,基于加密,在没有正确的密钥情况下,用户数据几乎不可能被解密。此外,如果政府实体向运营商传唤用户数据,运营商将无法解密用户数据并遵守此类传唤。这将使运营商避免泄露此类敏感用户数据的公共关系问题。

[0035] 在一些情况下,用户必须相信托管他们的用户数据的人不会以任何方式修改或错误处理用户数据。由于用户可以在上传其用户数据之前将其用户数据的哈希存储到区块链,因此很容易验证他们的用户数据是否被篡改。例如,可以确定上传的用户数据的新哈希值,并将其与存储的哈希值进行比较。因此,在此描述的系统和方法的另一个益处是可以存在验证程序来验证用户数据是否被修改。

[0036] 在一些实施例中,如果用户丢失或忘记了他们的私有密钥,则可以使用私有密钥恢复选项。例如,使用一系列双因素身份验证机制(例如,电子邮件、Facebook、SMS、电话、给

朋友打电话等),用户能够跨不同设备取得与其账户相关联的私有密钥的访问。这将允许同一用户在不同的设备和不同的平台上登录。

[0037] 在一些实施例中,可能存在赞助或托管用户数据的实体单方面破坏或阻止对用户数据的访问的问题。然而,在一些实施例中,可以实现去中心化的云存储解决方案(例如,Sia、Storj、Filecoin和/或IPFS)。加密的用户数据可以被存储在去中心化的云上,并且赞助或托管实体几乎无法控制存储的用户数据。

[0038] 此外,在一些实施例中,尽管用户可以允许通过第三方访问用户数据并且此类用户数据可能只能被临时访问,但是第三方仍然可能滥用用户数据。在一些实施例中,可以实现去中心化的类似托管(escrow)的机制来解决处理不当的用户数据的争议。在用户授予第三方访问用户的用户数据的许可之后,接收或访问用户数据的第三方将被要求质押(stake)一定数量的硬币、代币或资金,以保证不会滥用用户数据(例如,与其他未授权的第三方共享或出售用户数据,对用户数据免受侵犯或未授权的访问的保护不充分或疏忽等)。如果用户声称用户授予访问许可的第三方违反了预配置的隐私协议,例如,去中心化自治组织(DAO)可以决定谁有过错(例如,OpenZeppelin和Aragon提供平台允许DAO做出此类决定)。例如,如果决定存在隐私侵犯的行为,第三方质押的代币可以被烧毁或删除,或发送给用户。这会激励第三方不要错误处理用户数据。可替代地,任何第三方都可以被授权持有他们拥有的很大一部分资金。如果第三方侵犯了与第三方进行交易的任何用户的隐私,如果第三方有过错,则DAO可以做出决定。如果第三方有过错,所有质押的资金被烧毁或删除,或在受影响的用户之间共享。这将激励第三方不要破坏任何用户的信任,因为如果质押金额足够大,可能会损害第三方。

[0039] 在一些实施例中,分布式系统通常被设计为容错的。因此,如果集群中的节点中的一个节点出现故障,则系统在最终用户眼中仍保持完整功能。然而,如果节点继续正常运行,就像它正确运行一样,但无意中执行了不同的功能,则它可能损害数据的完整性和/或影响用户的体验。例如,考虑到此类行为不端的节点被称为拜占庭(byzantine)容错。尽管有许多不同形式的共识协议,但权益证明(PoS)和工作量证明(PoW)是最常见的两种,因为它们考虑了拜占庭容错。例如,如果行为不端的矿工(miner)想要比网络的其它部分更快地计算区块的话,则PoW通过迫使行为不端的矿工花费大量的计算资源来解释拜占庭容错。与其试图攻击网络,攻击者(例如,行为不端的矿工等)可以通过支持网络作为公平的矿工来赚更多的钱。在另一个示例中,如果矿工想要生成区块,则PoS通过迫使矿工质押大量资金来解释拜占庭容错。如果另一个矿工或不同的完整节点尝试验证对应的区块链并看到其中一个矿工行为不端并计算了不正确的区块,则他们将向网络的其余部分发出信号。与其试图攻击网络,攻击者(例如,行为不端的矿工等)可以通过支持网络作为公平的矿工来赚更多的钱。

[0040] 在一些实施例中,在此描述的架构可以支持取决于用户的传感器数据的对象识别器(OR)。在一些示例中,如果空间计算设备提供商在提供商的服务器上托管第三方OR,则提供商必须能够在某个时间点解密用户的数据。这意味着如果没有直接访问用户数据的提供商,任何外部OR都无法运行。在另一个示例中,如果提供商选择让第三方在他们自己的服务器上运行OR,并让用户控制哪些第三方可以访问用户的用户数据,则用户可以具有允许第三方访问用户的用户数据的选项,而提供商永远无法解密用户数据。

[0041] 示例用户数据交易系统

[0042] 图1示出用户数据交易系统100的示例并且包括系统的组件之间的交互和数据传输的示例。例如,用户数据交易系统100的内部组件或系统如何交互,以及在组件或系统之间传输什么数据。代理106、分布式账本108和软件合约110可以与在此描述的代理、分布式账本和软件合约相同(例如,关于其它实施例和示例),是用户数据交易系统100的组件或系统。此外,所述的系统和组件可以包括一个组件或多个组件。在此描述的组件并非详尽无遗,而只是可以实现哪些组件的示例。一些组件可以被组合,而其它组件可以被移除或替换为类似的组件。此外,一些组件可以是一个系统的一部分,或多个系统的一部分,它们相互连接并协同工作以实现相同的类似功能。

[0043] 示例代理

[0044] 在一些实施例中,代理106可以与各种系统进行电子通信,该系统可以包括分布式账本108、数据平台112、数据虚拟化系统111和用户设备102(例如,蜂窝电话、平板计算机、电子阅读器、智能手表、头戴式增强、虚拟或混合现实显示系统、可穿戴显示系统、图7A的可穿戴显示系统1000等)。在一些实施例中,代理106可以包括经由局域网或经由互联网连接的多个系统。此外,在一些实施例中,例如,代理106或其部分可以位于用户设备102、数据平台112、数据虚拟化系统111或购买者设备104上。例如,包括代理106和数据平台112的用户数据隐私系统103可以包括以隐私为中心的数据存储解决方案。以隐私为中心的数据存储解决方案可以是私有的、公共的、或私有组件和公共组件的组合。在一些实施例中,可以通过使用应用编程接口(API)调用从以隐私为中心的数据存储解决方案(或其组件)访问数据或信息(例如,用户数据等)。代理106可以确定它从各种系统接收到什么信息以处理和存储在分布式账本(例如,区块链、缠结等)中。

[0045] 在一些实施例中,代理106可以从各种系统接收数据或指令,它可以用来生成软件合约110(例如,智能合约等)并将软件合约110存储在分布式账本108中。例如,代理106可以从用户设备102接收隐私设置指令,然后代理106可以处理指令并生成捕获隐私设置指令的智能合约,并且然后代理106可以将智能合约写入区块链。由包括代理106的各种系统发送和接收的数据类型将关于图2-6中的流程图进行更详细的描述。

[0046] 除了在分布式账本108上生成和存储软件合约110之外,代理106还可以生成私有密钥和公共密钥。如在此所讨论的,密钥密码术(例如,公共密钥密码术等)可以被配置为生成一对加密密钥:用于平台的每个用户的公共密钥和私有密钥。公共密钥可以公开共享,但私有密钥旨在仅由用户控制。密钥密码术的一个益处可以包括数据机密性,使得将用户数据保密。例如,用户可以使用他们之前生成的公共密钥来加密他们的用户数据,并且只有该用户将能够在稍后的时间点使用他们的私有密钥来解密用户数据。密钥加密的另一个益处可以包括数据真实性,其中用户可以使用他们的私有密钥对一些数据进行数字签名,以便证明他们授权了这些数据。私有密钥和公共密钥可以存储在分布式账本108或软件合约110中,并与为其生成密钥的用户相关联。可以从分布式账本108或软件合约110中取得私有密钥和公共密钥,并将其发送到本文更详细描述的各种系统。例如,可以将私有密钥发送到数据虚拟化系统111、数据平台112、和/或用户设备102或从其接收。

[0047] 代理106可以读取存储在分布式账本108中的软件合约110,以生成基于反映在该用户的关联软件合约110中的特定用户的共享设置来提取数据的指令。此类指令可以被发

送到数据虚拟化系统111,例如,使得数据虚拟化系统111可以从数据平台112或经由存储相关数据的一个或多个第三方服务取得相关数据。

[0048] 在一些实施例中,关于哪些数据被各种系统访问或传输的数据传输或交易信息可以由数据虚拟化系统111或数据平台112发送到代理106。例如,数据虚拟化系统111或数据平台112可以取得/访问或修改它从一个或多个第三方服务(例如,社交网络、文件存储服务等)或数据平台接收的用户数据,并且信息的此类取得/访问和修改可以被跟踪和监控。还可以总结和描述取得/访问和修改信息,并且然后将其发送到代理106以进行任何进一步处理并存储在分布式账本108上。例如,该信息可用于跟踪或监控谁访问了什么类型的数据以及何时访问。

[0049] 在实现方式中,代理106(或代理106的一个或多个方面)可以包括“虚拟计算环境”或在“虚拟计算环境”中实现。如在此所使用的,术语“虚拟计算环境”应广义地解释为包括例如由一个或多个处理器(例如,如下文在图8的示例中描述)执行以实现在此描述的模块或功能的一个或多个方面的计算机可读程序指令。此外,在该实现方式中,代理106的一个或多个模块或引擎可以被理解为包括虚拟计算环境的一个或多个规则引擎,其响应于由虚拟计算环境接收到的输入,执行规则或其它程序指令以修改虚拟计算环境的操作。例如,从用户设备102接收的请求可以被理解为修改虚拟计算环境的操作以使代理106生成软件合约110、公共密钥或私有密钥,或执行其它操作。此类功能可以包括响应于输入并且根据各种规则来修改虚拟计算环境的操作。例如,由虚拟计算环境实现的其它功能(如在整个本公开中所述)可以进一步包括对虚拟计算环境的操作的修改,例如,虚拟计算环境的操作可以取决于由代理106从数据平台112收集的信息而改变。虚拟计算环境的初始操作可以理解为虚拟计算环境的建立。在一些实现方式中,虚拟计算环境可以包括一个或多个虚拟机或计算系统的其它仿真。在一些实现方式中,虚拟计算环境可以包括托管(host)计算环境,该托管计算环境包括可以远程访问并且可以根据需要快速供应的物理计算资源的收集(通常称为“云”计算环境)。

[0050] 分布式账本

[0051] 分布式账本108可以是代理106的一部分或单独的系统。分布式账本108可以被配置为存储一个或多个软件合约110、多个私有密钥和公共密钥、关于哪些数据被各种系统访问或传输的数据传输或交易信息,和/或任何其它相关信息(例如,何时访问数据,与访问相关联的账户,访问的数据属于谁,访问数据的适当许可是否适当,使用哪个公共密钥或私有密钥访问数据等)。

[0052] 与软件合约支持相结合的分布式账本可以提供无需许可、无需信任、抗审查和不可变的账本,该账本可以被配置为跟踪账户余额的状态并促进软件合约110从一个有效状态到另一个有效状态的转换。软件合约110(例如,智能合约、以太坊智能合约、图灵完备的智能合约等)和密钥密码术的组合可以提供可以扩展以包括最多产的数据集的解决方案。在此所述的系统和方法可以提供一种用户友好的方式来维持对用户的用户数据的访问和/或控制。

[0053] 在一些实施例中,关于哪些数据被各种系统访问或传输的数据传输或交易信息可以被存储在分布式账本108中。例如,数据虚拟化系统111可以取得/访问或修改它从一个或多个第三方服务(例如,社交网络、文件存储服务等)或数据平台112接收的用户数据,并且

可以跟踪和监控此类取得/访问和修改信息。取得/访问和修改信息也可以被总结和描述,并且然后发送到代理106以进行任何进一步的处理和存储在分布式账本108上。例如,该数据传输或交易信息可用于跟踪或监控谁访问了什么类型的用户数据以及何时访问。

[0054] 尽管现有技术中分布式账本的某些实现方式可能存在效率低下(例如,对区块链的各个区块的较慢写入),但与传统数据库或分布式数据库相比,该技术很快得到改进,效率低下将是最小的或根本不存在。因此,应当理解,尽管在此的实施例和示例公开了用于处理和存储用户数据的数据平台112,但分布式账本108可用于结合数据平台112或代替数据平台112来存储此类用户数据。

[0055] 在一些实施例中,可以实现私有区块链或分布式账本。当在企业之间构建保证完整性的安全服务时,私有分布式账本非常有用。例如,三个公司之间的股票结算服务可以使用私有分布式账本,因此这三个公司可以访问相同的信息,而不必彼此信任。可替代地,银行可以拥有私有分布式账本,以实现更安全、更快速的支付转移。在构建去中心化的面向消费者的产品时,一个目标可以是构建用户不必信任服务提供商的系统。最终用户应该能够看到谁访问他们的数据以及访问频率。用户应该具有同步轻(light)节点或全节点的能力,并自己验证交易。当与另一个地址进行交易时,用户应该能够看到他们的交易历史,并自己决定是否信任某个地址。

[0056] 软件合约

[0057] 在一些实施例中,软件合约110是自动执行合约,其中两方之间的协议条款被直接写入代码行。代码和其中包含的协议存在于分布式、去中心化的分布式账本网络中。例如,软件合约110可以允许可信交易和协议在不同的匿名方之间执行,而不需要中央机构、法律系统或外部执行机制。它们使交易具有可追溯性、透明性和不可逆性。虽然标准合约概述了关系的条款(通常是法律可以强制执行的),但软件合约110强制执行与密码代码的关系。例如,软件合约110是完全按照它们被编程的方式执行的程序。

[0058] 在一些实施例中,用户通过他们各自的设备102可以更新用户的个人隐私设置。一旦接收/访问更新,代理106然后将准备新的软件合约110并将其保存到分布式账本108。应该理解,基于分布式账本的技术(例如,区块链等),许多旧版本的用户软件合约可能会在各种位置(例如区块链的区块)中出现和可查看/可访问。因此,希望代理106能够区分哪个软件合约110是最新的版本。例如,代理106可以处理软件合约110,其具有指示正在保存的软件合约110的版本的字母数字标识符。在另一个示例中,每个软件合约110可以包括日期。在另一个示例中,每个软件合约110可以包括对先前软件合约的参考(reference),使得在审查所有软件合约后,分布式账本108上的某些位置不会进行审查或分析(例如,基于所包括的参考,或因为在较新的区块中找到了软件合约,并且本质上是更新的,因此不需要搜索较旧的区块)。

[0059] 在一些实施例中,可以使用软件合约110并且软件合约110可以包括旨在以数字方式促进、验证或执行协议的协商或执行的计算机协议。软件合约110可以允许在没有第三方的情况下执行可信的交易,其可以是可追踪的和不可逆的。许多类型的合约条款可以部分或完全自动执行、自动强制执行、或两者兼而有之。软件合约110可以提供优于传统合约法律的安全性并减少与合约化相关联的其它交易成本。软件合约110的一个示例是智能合约。下面提供了智能合约110的Solidity编程语言中的伪代码示例:

```
[0060]   pragma solidity^0.4.18;
[0061]   contract SmartContract{
[0062]     struct UserData{
[0063]       string URI;
[0064]       string metadata;
[0065]       string hash;
[0066]     }
[0067]     struct AcceptedBuyer{
[0068]       address acceptedBuyer;
[0069]       string key;
[0070]     }
[0071]     //属于选择共享其数据的用户的地址列表
[0072]     address[] userAddresses;
[0073]     //包含用户同意与其共享数据的实体的结构列表,以及只有该实体才//能访问的
解密密钥
[0074]     mapping (address=>AcceptedBuyer[]) acceptedBuyers;
[0075]     //想要访问用户数据但尚未被用户授予权限的实体列表
[0076]     mapping (address=>address[]) pendingBuyers;
[0077]     //指向URI的结构列表,其中存储了经加密的数据以及用户愿意公开//的一些元
数据;实体可以使用元数据来找出他们想要访问的用户数据
[0078]     mapping (address=>UserData[]) userData;
[0079]   }
```

[0080] 以下示例流程示出数据库如何能够基于用户设置的隐私设置采用加密数据运行。示例流程有助于示出系统在被使用和操作时的一些优势。应当理解,未明确提及的其它流程可以基于在此阐述的公开而生成或存在。

[0081] 关于加密密钥,示例流程可以包括以下内容。在该示例中,智能合约充当小型数据库,每次用户添加或移除有权访问用户数据的授权方列表时,该小型数据库都会不断被更新。例如,用户的私有密钥可以在认证过程之后安全地被转移到对应的用户设备(例如,102)。然后第三方可以经由分布式账本交易请求访问用户的环境数据。用户可以免费或付费拒绝或授予对其环境数据的访问许可。例如,用户可以要求对用户的环境数据的统一的预付费、订阅费,或者可以引入用户的环境数据的竞价平台。现在,例如,假设用户允许访问用户的环境数据,并且第三方进行了适当的支付或同意。当用户通过使用空间计算设备生成新的环境数据时,空间计算设备将经加密的数据(例如,在经加密的数据数据库116中)存储到数据平台(例如,112),并更新软件合约110的状态以指示新数据已被生成或存储。然后,当第三方查询软件合约110以取得解密密钥和从何处取得用户的环境数据的文件位置的列表时。用户可以稍后从软件合约中移除第三方(例如,通过创建新的软件合约来替换旧的软件合约等)以移除对用户的环境数据的访问。

[0082] 此外,在另一个示例流程中,即使可能存在存储在数据平台(例如,112)上的传感器数据,数据平台的运营商也将无法解密数据,因为运营商将无权访问必要的密钥。例如,

可以为用户生成非对称私有密钥,并可以安全地传输到用户的空间计算设备。还可以生成短时对称文件加密密钥。由空间计算设备生成的用户传感器数据(例如,环境数据或其他用户数据)使用短时对称文件进行加密,并且还计算用户传感器数据的哈希值。经加密的传感器数据被存储在数据平台上(例如,由空间计算设备的卖方来操作),并取得统一资源标识符(URI)。空间计算设备查询分布式账本上的软件合约,以取得对传感器数据感兴趣的所有未决第三方的列表。

[0083] 在一些实施例中,空间计算设备可以周期性地将分布式账本的轻节点同步到用户设备102。轻节点或轻量(lightweight)节点可能不会下载完整的分布式账本。相反,轻节点下载区块头(header)只是为了验证交易的真实性。轻节点易于维护和在系统上运行。用户选择用户希望向哪些第三方授予它们的传感器数据的许可。作为授予许可的交换,资金、积分、信用等的立即转移,或者第三方和用户之间的订阅模型可以在分布式账本上进行。对于第三方,空间计算设备使用提供的公共密钥对对称文件加密密钥进行加密。所有加密密钥以及第三方地址都针对接受的第三方进行存储。用户将URI、传感器数据的哈希值、和一些元数据添加到软件合约。每次生成更多传感器数据时,都可以重复该组步骤。所有接受的第三方都可以查询软件合约,使用他们的私有密钥来取得短时对称文件加密密钥,然后下载传感器数据并对其进行解密。每当用户想要更改有权访问其传感器数据的人员时,用户只需更新用户的隐私设置。更新用户隐私设置将触发用户设备重新计算短时对称文件加密密钥,并在更新软件合约时忽略对方的公共密钥。所选的各方可以访问先前生成的数据,但可能无法访问任何新生成的传感器数据。此外,可以定期或基于每个文件重新计算短时对称文件加密密钥以增加安全性。在一些实施例中,对与用户地址对应的软件合约的任何修改都必须由非对称私有密钥来签名。

[0084] 在一些实施例中,区块链被用作分布式账本。区块链交易的成本基于选择的软件合约平台。例如,如果选择并实现以太坊平台,则交易时间和成本在很大程度上取决于网络使用情况和最终软件或智能合约的状态。例如,成本可能与发布软件合约、第三方请求访问用户数据、用户更新所接受的第三方的列表、以及用户为新用户数据添加元数据相关联。在一些实施例中,用户更新所接受的第三方的列表和用户为新用户数据添加元数据可以被批处理,使得软件合约的更新频率较低,但对用户来说成本低得多。此外,以太坊还在研究经由软件合约的方式,使得可以代表用户支付交易,这将希望在所述的系统和方法中实现。这可以提供一种方法来帮助参与其中的(onboard)新用户,直到用户通过允许访问他们的数据而赚了一些钱或积分,并且可以为自己支持进一步的交易。此外,EOS是另一种类型的软件合约平台,其使用称为委托权益证明的不同共识机制。以较低的安全性和完整性为代价,所有交易对所有人都是免费的,并且可以完全避免成本,并且可以成为其它智能合约平台的有用替代方案。

[0085] 示例数据平台

[0086] 例如,数据平台112可以包括去标识化(de-identify)和假名化(pseudonymise)的数据数据库114、经加密的数据数据库116、和数据验证系统118。数据平台112还可用于处理和存储数据。例如,数据平台112可以存储用户数据或环境数据,其包括用户设备102收集的关于用户设备102的环境的数据(例如,关于房间或区域的周围信息,包括人脸、房间大小、艺术品,或在私有或公共空间中的人周围的任何东西)。在一些实施例中,数据平台112还可

以存储多个私有密钥和公共密钥、关于哪些数据被各种系统访问或传输的数据传输或交易信息,或任何其它相关信息(例如,何时访问数据,与访问相关联的账户,访问的数据属于谁,访问数据的适当许可是否适当,使用哪个公共密钥或私有密钥来访问数据等)。在一些实施例中,一些数据被临时存储,直到它被发送到代理106以存储在分布式账本108上。在一些实施例中,数据的部分被存储在数据平台112中,而其它部分被存储在分布式账本108中。然而,在一些实施例中,数据可以作为冗余或效率的形式存储在两个系统中。

[0087] 在空间计算设备上生成的用户数据类型可以是高度个人化的,并且在某些情况下是机密的、专有的或敏感的。此类用户数据可用于构建用户环境模型,以实现内容持久性和共享体验。这样做涉及:对象识别器管线,其用于检测和语义标记用户环境中的真实对象;世界重建管线,用于为遮挡和碰撞检测构建密集网格;地图合并管线,保证同一空间内的用户在同一坐标系中操作;以及固定(pin)和恢复与用户创建或共享的虚拟内容的能力。例如,单个用户的会话可能生成数百兆字节的用户数据,以使上述所有操作成为可能。希望该用户数据以安全的方式保存,但也可供用户、空间计算设备的提供商和某些第三方使用,以便创建引人入胜的沉浸式体验。在不使用分布式账本的情况下收集此类数据的示例流程如下:

- [0088] 1. 用户采用空间计算设备捕获原始传感器数据;
- [0089] 2. 用户对空间计算设备上的数据进行加密;
- [0090] 3. 用户将经加密的数据保存到云存储(例如,数据平台),云存储由提供空间计算设备的空间计算公司拥有;
- [0091] 4. 空间计算公司维护在制造过程期间存储在设备上的用户密钥的副本;
- [0092] 5. 空间计算公司解密用户数据,以构建用户环境的模型;以及
- [0093] 6. 空间计算公司解密并与第三方共享用户的数据。

[0094] 在此描述的系统和方法提供了一种解决方案,该解决方案将给予用户个性化控制:谁有权访问用户的用户数据、用户数据的哪些部分可供访问、用户数据的哪些部分可供谁使用、用户可以从提供对其用户数据的访问中受益的平台,以及保证用户的用户数据完整性的机制。例如,用户可以具有授权第三方访问用户的用户数据的选项,而无需空间计算公司能够自己解密数据。在全球消费者数据隐私法律不断变化的领域中,限制空间计算公司访问敏感数据的实现方式在违反或不遵守此类隐私法律的情况下是有利的。

[0095] 示例去标识化和假名化的数据数据库

[0096] 去标识化和假名化的数据数据库114可以包括用户数据或环境数据,其已被处理以移除数据来源的任何引用或指示。例如,访问存储在去标识化和假名化的数据数据库114上的此类信息的实体将不能对与数据相关联的人/用户或多人/多个用户进行逆向工程。应该理解,在一些情况下(例如,小型数据集等),实体可以能够基于某些因素并基于实体自己的专有信息或其它可公开访问的信息,在统计上缩小可能的用户。然而,数据本身不应指示数据属于谁。例如,公司可以为在蒙大拿州比尤特(Butte)使用用户设备102的任何用户从去标识化和假名化的数据数据库114访问去标识化和假名化的数据,这可以为10个人提供结果。然后,公司可以在某个阈值内确定这10人中的一些人可能是谁,或者仅基于结果,或者采用附加的专有或公开可用的数据。然而,数据去标识化和假名化的数据本身不会提供此类指示,并且希望任何逆向工程,特别是仅基于结果的逆向工程,都尽可能地受到限制。

因此,重要的是证明去标识化和假名化的数据的算法被正确地测试和实现,并且在一些实施例中在提供给第三方之前验证去标识化和假名化的数据。

[0097] 在一些实施例中,当数据虚拟化系统111向数据平台112请求数据时,数据平台112可以访问去标识化和假名化数据的数据库114以定位相关的经加密的用户数据以向数据虚拟化系统111发送去标识化和假名化数据。关于交易的数据可以被记录并且关于交易的信息可以被发送到代理106以用于在分布式账本108上的处理和存储。处理可以包括将交易数据与特定用户或用户设备102或分布式账本上的位置相关联。处理还可以包括格式化数据,使得它正确地保存在分布式账本108中而没有任何错误,并用于优化或有效的取得或审查。

[0098] 示例加密数据数据库

[0099] 加密数据数据库116可以存储从用户设备102接收的加密用户数据或环境数据。在一些实施例中,数据平台112可以在存储之前加密数据。在一些实施例中,用户设备102可以在发送到数据平台112用于存储之前加密数据(例如,采用公共或私有加密密钥)。在一些实现方式中,例如,可能希望用户设备102加密用户设备102自己的数据以在发生侵犯的情况下提高整体系统安全性。如果发生侵犯并且数据平台112被破坏,则加密数据对任何侵犯者都应该是无用的,因为加密数据永远不会以未加密的方式到达数据平台112,并且解密所需的密钥可以存储在单独的位置(例如,分布式账本108或用户设备102)。

[0100] 在一些实施例中,当数据虚拟化系统111向数据平台112请求数据时,数据平台112可以访问加密数据数据库116以定位相关的加密用户数据以向数据虚拟化系统111发送加密数据。可以记录关于交易的数据,并且可以将关于交易的信息发送到代理106以在分布式账本108上进行处理并存储。处理可以包括将交易数据与特定用户或用户设备102或分布式账本108上的位置相关联。处理还可以包括格式化数据,使得它正确地保存在分布式账本108中而没有任何错误,并用于优化或有效的取得或审查。

[0101] 示例数据验证系统

[0102] 数据验证系统118可以在各种系统之间传输之前验证各种信息。例如,并且如关于图3更详细描述,数据验证系统118可以接收私有加密密钥和软件或智能合约标准或规则,以及相关加密用户数据被发送到数据虚拟化系统111的确认(例如,包括描述传输时间和类型的信息以及用户数据的描述,或可能相关的任何其它信息)。数据验证系统118然后可以验证加密的用户数据和私有加密密钥匹配(例如,通过解密数据),并且然后向代理106发送验证结果以允许代理向数据虚拟化系统111发送验证的私有加密密钥以解密已经接收的加密用户数据。

[0103] 示例数据虚拟化系统

[0104] 数据虚拟化系统111可以与购买者设备104、数据平台112和代理106通信。数据虚拟化系统111可以从购买者设备104接收请求以访问、请求或取得某些信息或用户数据。例如,数据虚拟化系统111可以从数据平台112请求用户数据,并且如果被允许,接收请求的用户数据(例如,加密的用户数据)。在一些实施例中,关于如何提取数据或提取什么数据的指令(例如,基于软件合约的条款)可以在数据虚拟化系统111向数据平台112发送请求之前被发送到数据虚拟化系统111。此外,例如,数据虚拟化系统111可以接收与一个或多个用户设备或用户的用户数据相关联的私有加密密钥。私有加密密钥可用于解密从数据平台112接收的加密用户数据。此外,在一些实施例中,数据交易信息(例如,关于从一个或多个第三方

服务或数据平台等下载、取得、访问或接收用户相关数据的信息)可以被发送到代理106进行存储。

[0105] 数据虚拟化系统111可以包括用户界面以促进购买者设备104对由数据虚拟化系统111接收和解密的任何用户数据的交互和操作。数据虚拟化系统111还可以提供分析工具,该分析工具被配置为提供统计结果、图表、图形和模型以供购买者设备104与之交互和操纵。数据虚拟化系统111还可以允许下载分析结果。然而,在一些实施例中,并且可能基于由软件合约110规定的用户隐私设置,例如,数据虚拟化系统111可以阻止解密的用户数据的下载或传输,并且将解密的用户数据的使用限制为仅有源(active)购买者设备104会话。会话终止后,数据将被删除,并准备新的私有加密密钥来解密用户数据以增强安全性(例如,使得释放的私有加密密钥不再有用)。例如,该过程将关于图3和图4更详细地描述。

[0106] 示例用户设备

[0107] 在一些实施例中,用户设备102可以与代理106和数据平台通信。例如,用户设备102可以从代理接收公共或私有加密密钥以加密任何收集或生成的用户数据或环境数据。经加密的用户数据可以以特定的时间间隔(例如,在生成数据时实时、每天、每小时、或在连接到网络时,或在任何其它所期望的时间或间隔)发送到数据平台进行存储。在一些实施例中,不会将密钥发送到用户设备102,并且可以将收集或生成的用户数据发送到数据平台112用于加密然后存储。如上文和在此所讨论的,在一些实现方式中,例如,可能希望用户设备102对用户设备102自己的数据进行加密,以在发生侵犯的情况下提高整体系统安全性。如果发生侵犯并且数据平台112被破坏,则加密数据对任何侵犯者都应该是无用的,因为它永远不会以未加密的方式到达数据平台112,并且解密所需的密钥可以被存储在单独的位置(例如、分布式账本108或用户设备102)。

[0108] 与用户设备102相关联的用户还可以提供用户隐私设置或隐私设置。用户可以控制用户自己的用户数据或由其设备生成的环境数据。用户还可以控制哪些用户数据可从其它来源(例如,第三方、其它设备、用户自己或任何其它可用数据)访问。例如,用户可以经由网络浏览器或其它输入法指示与用户的用户数据相关联的用户的隐私设置或隐私规则。隐私设置可以指示关于用户数据的可访问性、共享或出售的限制。例如,隐私设置可以指示但不限于以下:什么类型的购买者可以或不能访问或购买用户数据,对什么类型的数据可访问的限制(例如,环境数据、与用户相关联的第三方数据、用户提供的数据等)、数据何时可访问的限制(例如(例如,一天、一周或一个月的时间)、数据访问频率的限制、访问的目的、访问的类型(例如,连接的类型或机器访问)、访问位置(例如,(例如,如经由IP确定的购买者系统的原产国)、有关外部数据源的许可(例如,是否可以导入社交媒体数据以丰富用户数据)或任何其它相关因素。隐私设置还可以包括黑名单或白名单,为用户提供按名称或类型阻止或允许访问特定个人、实体、公司等的能力。例如,用户可以将所有银行或相关联的公司加入黑名单,以阻止银行和相关联的公司访问所有用户数据。在一些实施例中,用户隐私设置或隐私规则可以由用户随时更新。在用户更新用户的隐私设置之后,所有与用户的用户数据相关的未来交易事件都将由新更新的隐私设置控制。

[0109] 示例购买者设备

[0110] 购买者设备104可以与数据虚拟化系统111通信。购买者设备104可以由购买者操作或与购买者相关联。购买者可以使用购买者设备104来购买、查看、访问、审查、分析可用

用户数据或通过数据虚拟化系统111与可用用户数据进行交互。应当理解,购买者可以购买或访问的任何用户数据至少部分地基于如编程到每个用户相应的软件合约中的每个用户的隐私设置。在一些实施例中,软件合约还可以规定什么类型的购买者应该或不应该访问他们的数据。例如,特定用户可能会禁止所有银行或银行代表访问他们的数据,因为他们可能担心这会影响他们的信用。

[0111] 在一些实施例中,数据虚拟化系统111可以包括用户界面以促进购买者设备104对由数据虚拟化系统111接收和解密的任何用户数据的交互和操纵。数据虚拟化系统111还可以提供分析工具,该分析工具被配置为提供统计结果、图表、图形和模型以供购买者设备104与之交互和操纵。数据虚拟化系统111还可以允许下载分析结果。然而,在一些实施例中,并且可能基于由软件合约110规定的用户隐私设置,例如,数据虚拟化系统111可以阻止解密用户数据的下载或传输并限制使用解密用户数据(例如,使用仅限于有源购买者设备104会话,或者某些分析工具可能被阻止或限制等)。例如,在终止有源购买者设备104会话时,数据将被删除,并且将准备新的私有加密密钥来解密用户数据以增强安全性(例如,使得释放的私有加密密钥不再有用)。例如,该过程将关于图3和图4更详细地描述。

[0112] 用户设备102或购买者设备104可以包括增强、混合或虚拟现实显示设备,诸如例如参考图7A描述的可穿戴显示系统1000,或参考图7B描述的设备702a-702c,或参考图8描述的用户设备824。

[0113] 各种系统之间的示例数据流的描述

[0114] 图2-6示出用于跨各种系统和组件接收和实现与用户数据或环境数据相关联的用户隐私设置的各种方法的流程图。尽管在图2-6中描绘了顺序,但是应当理解,数据可以在各种系统之间以任何顺序、以任何方向或组合来回流动。例如,一个系统的某些能力可以在另一个系统或一组系统上实现。此外,例如,一个系统可以由多个系统组成。

[0115] 用户隐私设置的示例处理

[0116] 图2A示出用于为用户创建或更新隐私设置的示例方法200的流程图。

[0117] 在框202中,用户设备102接收与用户相关联的隐私设置。用户设备102可以加密新的或更新的隐私设置。隐私设置可以包括新设置或对先前接收的设置的更新。

[0118] 在框204中,代理106接收新的或更新的隐私设置,并且如果需要,解密隐私设置。在框206中,代理106基于接收的隐私设置来创建软件合约(例如,智能合约等)。

[0119] 在框208中,代理106创建私有加密密钥。在框210中,代理106加密私有加密密钥。例如,可以采用公共加密密钥来加密私有加密密钥。

[0120] 在框212中,代理106将软件合约和经加密的私有加密密钥存储在分布式账本108中。代理106与分布式账本108通信并且充当各种设备之间的中介。由于某些分布式账本技术的限制,代理可能是用于与分布式账本交互并保存到分布式账本的必需组件。在一些实施例中,可能不需要代理106,并且分布式账本108本身可以能够担任代理106的角色。

[0121] 在框214中,代理106创建公共加密密钥。类似于关于图2-6描述的所有框,虽然框214发生在框206之后,但应当理解,框214可以紧接在框204之后、在框204之前(例如,当用户第一次创建账户或连接到代理106时)、在框208之后,或以足以实现系统和方法的预期目的的任何顺序发生。

[0122] 在框216中,代理106向用户设备102发送公共加密密钥。在框218中,用户设备102

从代理106接收公共加密密钥。

[0123] 在框220中,用户设备例如基于用户设备102的周围环境来收集环境数据,该环境数据是用户数据的至少一部分。

[0124] 在框222中,用户设备102使用公共加密密钥来加密收集的环境数据和任何其他用户数据。在框224中,加密的环境数据采用元数据进行语义标记。在一些实施例中,元数据是未加密的并且不包含个人可标识信息。例如,语义注释或标记可以包括将附加信息附加到加密环境数据,使得审查加密数据的计算机和/或管理员能够确定关于加密数据的信息(例如,它是谁的数据,什么用户设备与数据相关联等)。在一些实施例中,可以限制语义标记的范围以进一步保护用户隐私。

[0125] 在框226中,语义标记和加密的数据通过加密连接以电子方式发送到数据平台112。在一些实施例中,数据平台112可以是数据存储介质(例如,Data Lake、NoSQL数据库等)。在一些实施例中,数据平台112可以是一系列或一组数据存储介质。在一些实施例中,数据平台112可以包括数据验证系统(例如,118)并且对发送到数据平台112和从数据平台112发送的数据执行处理和验证。在框228中,数据平台112接收语义标记和加密的数据。

[0126] 在框230中,数据平台112存储语义标记和加密的数据。在一些实施例中,在框232中,在存储后,语义标记和加密的数据被分配哈希标识(例如,最少32个字节)。在一些实施例中,语义标记和加密的数据可以被分配另一种类型的标识值或参考号。

[0127] 在框234中,数据平台112向代理106发送数据交易的通知(例如,语义标记和加密的数据的接收和处理,或关于数据交易的任何其它相关信息)。数据平台112还发送哈希标识值(或任何其它标识值,如果没有使用哈希)和语义标记信息。在框236中,代理106接收信息和/或数据。

[0128] 在框238中,代理106将哈希标识值和/或交易数据编码到分布式账本108中。例如,哈希标识值和交易数据可以参考或与存储在框212中的软件合约和加密的私有加密密钥的副本一起存储。跟踪哈希标识值、交易数据、软件合约和私有加密密钥之间的关系的好处是例如,用户可以查看用户的隐私设置并基于交易数据验证隐私设置是否按预期工作,或者是否应该对隐私设置进行任何更改。

[0129] 图2B-2C示出用于为用户创建或更新隐私设置的示例方法的泳道流程图。类似于图2A,图2B-2C示出由数据存储介质、用户设备、oracle和数据虚拟化应用执行的各种步骤。

[0130] 基于隐私设置定位、验证和促进用户数据的传输的示例

[0131] 图3示出用于定位、发送和解密用户数据的示例方法的流程图。如图所示,某些附加的或替代的框在图4、6A和6B中描绘。

[0132] 在框302中,代理106接收对用户数据的请求,该用户数据可以与一个或多个用户相关联。关于该请求的更多细节将结合图6B、框622进行描述。

[0133] 在框304中,代理106在分布式账本108或分布式账本中搜索与一个或多个用户相关联的软件合约。关于图2A-2C和本文提供了基于用户隐私设置来创建软件合约的示例描述。

[0134] 在框306中,代理106定位分布式账本108的包括相关软件合约的最新部分。在一些情况下,对于一些用户,可能只存在与每个用户相关联的一个软件合约。在一些情况下,对于其他用户,可能存在与每个用户相关联的两个或更多个软件合约。这是因为,例如,在一

些分布式账本技术中,数据可以存储在区块中。一旦区块被写入分布式账本,该区块就不能被更改或删除。因此,对软件合约的任何更新都必须作为新的软件合约被写入新区块。如果用户向其隐私设置提供多次更新,则将存在保存到分布式账本的多个区块的多个软件合约。将旧版本的隐私设置存储在分布式账本中的益处是允许用户(或其它实体)直接或间接地查看其隐私设置的更改历史,如对应的软件合约中所示。当为特定用户写入新的软件合约时,对代理106而言,包括对软件合约与谁相关联以及在一些情况下的软件合约的创建版本或何时创建软件合约的参考或指示是有益的。在一些示例中,如果特定用户存在多个软件合约,则代理106可以依赖交易信息(例如,将区块数据写入特定区块的日期和时间,或将区块写入分布式账本的日期和时间)来确定哪个软件合约是最新的。

[0135] 在框308中,代理106基于用户的最新软件合约中的每个来确定一个或多个用户中的哪一个允许共享他们的用户数据。例如,一些用户可能不希望与接收的对用户数据请求相关联的特定购买者共享任何信息,并且与这些用户相关联的数据不应被共享或使其可访问。只有请求的用户数据和用户允许共享的用户数据才应该和与请求相关联的购买者共享或可访问。

[0136] 在框310中,代理106向数据虚拟化系统111发出指令以提取被请求并且与被允许共享的用户相关联的用户数据。在框312中,数据虚拟化系统111从框310接收指令。

[0137] 在框314中,数据虚拟化系统111基于从代理106接收的指令从数据平台112请求用户数据。在框316中,数据平台112接收对访问用户数据的请求。

[0138] 在框318中,数据平台112在一个或多个数据库中为允许共享的一个或多个用户定位并取得相关加密用户数据。关于数据平台112如何与用户数据交互的附加细节将结合图2和4-6进行描述。在框320中,数据平台112将相关加密用户数据发送或可用于数据虚拟化系统111。在框321中,数据虚拟化系统从框320接收或访问相关加密用户数据。

[0139] 在框322中,数据平台112向数据验证系统118和代理106发送以下确认:在框320、321中相关加密用户数据被成功地发送到数据虚拟化系统111或被数据虚拟化系统111接收。在框323中,代理接收确认,并且在框324中,数据验证系统118接收确认。

[0140] 在框325中,代理106从与被允许共享的一个或多个用户相关联的软件合约取得或访问私有加密密钥。在框327中,私有加密密钥被发送到数据验证系统118,并且在框331中,代理执行从框402开始的图4中描述的附加步骤。在框329中,数据验证系统118接收私有加密密钥。

[0141] 在框326中,例如,数据验证系统118通过成功地解密与每个密钥相关联的用户数据来验证用户数据和私有加密密钥是否匹配。

[0142] 在框328中,基于用户数据是否被成功解密,数据验证系统118向代理106发送验证结果。在一些实施例中,如果要验证多个用户的用户数据并且只有一部分成功而其余部分不成功(例如,私有加密密钥无法正确解密部分用户的数据),则可以将整个结果发送到代理106进行处理。

[0143] 在框330中,代理106接收验证结果。在一些实施例中,如果一些私有加密密钥被成功验证而另一些未被成功验证,则成功的部分可以被发送到数据虚拟化系统111。在一些实施例中,如果一些私有加密密钥被成功验证并且另一些未被成功验证,则没有任何东西被发送到数据虚拟化系统111,并且代理106采用其它潜在的私有加密密钥来重复框325-328

中的过程,直到验证成功,并且然后一起发送所有相关和验证的私有加密密钥。在购买者希望调节或取消请求的情况下,可能希望将所有私有加密密钥一起发送或使用数据虚拟化系统111提示购买者在呈现任何内容之前并非所有数据都可用。在一些实施例中,如果在框326中由数据验证系统118成功验证了一些私有加密密钥而其它未被成功验证,则可以将成功部分发送到数据虚拟化系统,并且框325、327、329、326和328中的过程可以对不成功部分重复,直到定位正确的私有加密密钥,并且然后将其发送到数据虚拟化系统111。

[0144] 可能希望将验证的任何私有加密密钥发送到数据虚拟化系统111,并且稍后在验证后将任何附加的验证的私有加密密钥发送,使得使用数据虚拟化系统111的购买者不会被延迟并且可以更快地查看数据,在框332中,随着从框330接收或访问附加的新私有加密密钥来丰富数据。在一些实施例中,如果在数据验证系统118尝试一定次数(例如,1,2,3等)后无法验证私有加密密钥,则可以将最终错误输出到代理106,并且然后输出到和与无法被验证的私有加密密钥相关联的特定用户数据相关的数据虚拟化系统111。在框332中,数据虚拟化系统111接收或访问验证的私有加密密钥。

[0145] 在框334中,基于来自框321的相关加密用户数据和从框332接收的匹配和验证的私有加密密钥,数据虚拟化系统111可以使用从数据平台接收的每组加密用户数据的相关的私有加密密钥,采用在框332中从代理106接收或访问的私有加密密钥来解密经加密的用户数据。

[0146] 在框336中,数据虚拟化系统111对解密的用户数据进行去标识化和假名化,使得使用数据虚拟化系统111的购买者不能标识与数据相关联的用户。例如,假名化是一种数据管理和去标识过程,通过该过程,数据记录中的个人身份信息字段被一个或多个个人标识符或假名替换。每个替换字段或替换字段的集合的单个假名使数据记录不易标识,同时仍适用于数据分析和数据处理。在一些实施例中,可以通过添加信息将假名化数据恢复到数据的原始状态,然后允许重新标识个人,而匿名化数据永远不会恢复到数据的原始状态。在一些实施例中,在假名化不如期望的那样有效的情况下(例如,参考框338和预配置的或自动阈值),也可以使用分段或改变用户数据的其它方法。

[0147] 在框338中,数据虚拟化系统111运行测试以验证和重新验证任何用户数据的重新标识是不可能的,或者在预配置或自动阈值内统计上是不可能的(例如,40%、50%、51%、80%、90%、95%、99%不太可能将数据与特定人相关联)。

[0148] 在框340中,一旦数据虚拟化系统111被关闭(例如,在接收到来自购买者的终止指令时),数据虚拟化系统111关闭会话并擦除它已接收到的任何用户数据和私有加密密钥。此外,在框342中,图6A描述了关于购买者如何与数据虚拟化系统111交互以及如何在框602中进一步保护用户数据免于被导出或从数据虚拟化系统111中取出的附加细节。

[0149] 用户数据的新私有加密密钥的生成和应用示例

[0150] 图4示出用于生成新的私有加密密钥并采用新的私有加密密钥来重新加密用户数据的方法400的流程图。某些附加的或替代的步骤在图3中描绘。在图3中的框330中将私有加密密钥发送到数据虚拟化系统111之后,图3中的框331可以包括在框404中开始的过程。

[0151] 在框404中,代理106可以为与在图3中的框330中向数据虚拟化系统111发送或可用的私有加密密钥相关联的任何用户数据生成新的私有加密密钥。希望生成新的私有加密密钥以重新加密与任何分布式私有加密密钥相关联的用户数据。例如,如果购买者要发布

其通过数据虚拟化系统接收到的任何私有加密密钥,则用户数据的安全性和隐私性可能受到损害。尽管在一些实施例中,购买者将不能直接访问数据虚拟化系统111接收或访问的任何私有密钥,但是例如,在购买者未经授权入侵数据虚拟化系统以取得密钥的情况下,生成新的私有加密密钥仍然更加安全。

[0152] 在框406中,代理106将新的私有加密密钥存储在在图3中共享或访问其数据的用户相关联的更新的软件合约中。在一些实施例中,关于进出数据虚拟化系统的数据交易的任何信息也将与更新的软件合约一起被存储。例如,与图3中的框330中的私有加密密钥的传输有关的传输细节将被存储在更新的软件合约中。

[0153] 在框408中,代理106将新的私有加密密钥和旧的私有加密密钥(例如,在图3中的框330中发送的密钥)发送或可用于数据平台112。在框410中,数据平台从代理106接收新的私有加密密钥。

[0154] 在框412中,数据平台112定位与其在框410中接收的私有加密密钥相关联的用户数据。在框414中,数据平台112采用旧的私有加密密钥来解密用户数据,并且然后采用新的私有加密密钥来重新加密用户数据。然后在框416中,将重新加密的用户数据存储在一个或多个数据库中。

[0155] 采用第三方数据来丰富用户数据的示例

[0156] 图5示出用于采用从一个或多个第三方服务中取得或访问的第三方数据来丰富用户数据的方法500的流程图。某些附加的或替代的步骤在图6B中描绘。应当理解,可以取得或访问任何第三方数据以丰富用户数据。例如,第三方数据可以包括财务数据(例如,来自信用局或信用评级服务)、社交媒体数据(例如,Facebook、MySpace、LinkedIn、Instagram、Snapchat等)、个人数据(例如,上传到文件共享站点,诸如dropbox、box、google drive、Apple的iCloud等)、来自视频流服务(例如Netflix、Amazon prime video、Hulu等)的任何观看习惯、来自电子邮件或聊天服务(例如,Gmail、Yahoo Mail、Google Hangouts、Zoom video、WhatsApp、Facebook Messenger、Outlook等)的内容、或用户希望提供访问权限的任何其他第三方服务。

[0157] 在可以在在此所述的来自图6B中的框622的过程之后启动的框504中,代理106可以基于从数据虚拟化系统111接收的对用户数据的请求,在分布式账本108中搜索与特定用户或一组用户相关联的一个或多个软件合约(有关请求的更多信息和细节,请参见图6B)。

[0158] 在框506中,代理106可以定位分布式账本的最新部分,该部分包括一个或多个用户的相关软件合约。如上所述,在一些情况下,对于一些用户,可能仅存在与用户中的每个用户相关联的一个软件合约。在一些情况下,对于其他用户,可能仅存在与用户中的每个用户相关联的两个或更多个软件合约。这是因为,例如,在一些分布式账本技术中,数据可以存储在区块中。一旦区块被写入分布式账本,该区块就不能被更改或删除。因此,对软件合约的任何更新都必须作为新的软件合约被写入新区块。如果用户对其隐私设置提供多次更新,则将存在保存到分布式账本的多个区块的多个软件合约。将旧版本的隐私设置存储在分布式账本中的益处是允许用户(或其他实体)直接或间接地查看其隐私设置的更改历史,如对应的软件合约中所示。当为特定用户写入新的软件合约时,对代理106而言,包括对软件合约与谁相关联以及在一些情况下的软件合约的创建版本或何时创建软件合约的参考或指示是有益的。在一些示例中,如果特定用户存在多个软件合约,则代理106可以依赖交

易信息(例如,将区块数据写入特定区块的日期和时间,或将区块写入分布式账本的日期和时间)来确定哪个软件合约是最新的。

[0159] 在框508中,代理106基于存储在分布式账本中并由软件合约表示的用户隐私设置来确定一个或多个用户允许共享收集的数据和来自一个或多个第三方服务的数据。

[0160] 在框510中,代理106向数据虚拟化系统111发出指令以提取被请求的并且与允许从一个或多个第三方服务共享的用户相关联的用户数据。指令还可以包括关于软件合约的细节以及应该和不应该与访问数据虚拟化系统111的购买者共享什么类型的数据,以及谁发起了对数据的请求。在框512中,数据虚拟化系统111接收或访问来自框510的指令。

[0161] 在框514中,数据虚拟化系统111取得或访问从一个或多个第三方服务之一允许的第三方数据。例如,可以通过使用API调用或任何其它可用手段来执行取得。

[0162] 在框516中,数据虚拟化系统111采用元数据对第三方数据进行剖析和标记。在一些实施例中,元数据可以描述第三方数据的来源、与第三方数据相关联的用户、取得数据的时间日期、或任何其它相关信息。

[0163] 在框518中,可以清理和格式化第三方数据。例如,在一些实施例中,可以编辑数据以移除基于用户隐私设置或软件合约不允许共享的任何信息。在一些实施例中,可以取得额外的或不相关的信息(例如,通过API),并且数据必须被格式化以符合数据虚拟化系统111的要求或购买者或系统的显示偏好。

[0164] 在框520中,数据虚拟化系统111可以采用第三方数据丰富和上下文化任何先前存储的用户数据。例如,数据丰富可能意味着将来自外部权威来源的第三方数据与现有的第一方客户数据的数据库合并。此外,例如,上下文化可以是基于实体的上下文信息来标识与实体(例如,人或城市)相关的数据的过程。例如,上下文或上下文的信息可以是关于任何实体的任何信息,其可用于有效减少特定应用范围内决策所需的推理量(经由过滤、聚合和推理)。上下文化然后是基于实体的上下文信息来标识与实体相关的数据的过程。上下文化可以将不相关的数据排除在考虑之外,并有可能从多个方面(包括大规模数据密集型应用中的数量、速度和多样性)减少数据。上下文化的益处可以包括基于应用/服务/用户的兴趣来减少数据量的潜力。此外,上下文化的另一个益处是它可以通过排除不相关的数据来提高数据处理、查询和/或交付的可扩展性和效率。

[0165] 在框522中,数据虚拟化系统111可以向代理106发送在框514中取得的新第三方数据的通知和交易细节。在框524中,代理106可以接收新第三方数据的通知和交易细节。

[0166] 在框526中,代理106可以将数据交易信息(例如,数据提取、剖析和处理、加密等)编码到分布式账本108中。另外,在框526中,代理106可以取得与为其取得第三方数据的用户(或多个用户)相关联的公共加密密钥,并且在框528中,向数据虚拟化系统111发送公共加密密钥。在框530中,数据虚拟化系统接收公共加密密钥。

[0167] 在框532中,数据虚拟化系统111对在框514中从第三方服务取得或访问的第三方数据进行加密,并且在一些实施例中,采用任何先前存储的用户数据对第三方数据进行加密。框532中的加密将在框516、518和520中由数据虚拟化系统111对第三方数据执行处理之后发生。

[0168] 在框534中,数据虚拟化系统111将经加密的用户数据发送到或可用于数据平台112。在框538中,数据平台112接收或访问经加密的用户数据,并且在框540中,将经加密的

用户数据存储在一个或多个数据库中。

[0169] 在框536中,一旦数据虚拟化系统111被关闭(例如,在接收到来自购买者的终止指令时),数据虚拟化系统111关闭会话并擦除任何用户数据(包括任何第三方数据)以及数据虚拟化系统111已经接收到的任何私有加密密钥。此外,图6A和图6B描述了关于购买者如何与数据虚拟化系统111交互以及如何如何在框602中进一步保护用户数据免于被导出或从数据虚拟化系统111取出的附加细节。

[0170] 进一步验证、处理和监控用户数据

[0171] 图6A示出用于验证、处理和监控用户数据的方法600的流程图。某些附加的或替代的步骤在图3中描绘。

[0172] 在可以在图3的框342中的过程之后启动的框604中,例如,数据虚拟化系统111对用户数据执行聚合、预分析和/或上下文化。例如,聚合可以包括聚合函数(aggregate function)或聚集函数(aggregation function),其是一种函数,其中可以将多行数据的值组合在一起以形成单个汇总值。一些常见的聚合函数可以包括:平均值(即算术平均值)、计数、最大值、中值、最小值、众数、范围、总和、nanmean(忽略NaN值的平均值,也称为“nil”或“null”)或stddev。例如,预分析可以配置为描述购买者将如何分析用户数据,这将在访问任何数据之前进行配置。然后,在框606中,数据虚拟化系统111采用如上文和在此所述的元数据来编码用户数据。

[0173] 在框608中,数据虚拟化系统111采用机器学习或人工智能(AI)来监控用户数据,以防止未经授权地导出用户数据。在一些实施例中,希望防止某些用户数据从数据虚拟化系统111未经授权地导出以潜在地增加用户数据的安全性和隐私性。例如,如果购买者要从系统中取出用户数据,则购买者可以出售或发布数据。

[0174] 在一些实施例中,机器学习可用于监控用户数据和购买者与数据虚拟化系统111的交互,以防止未经授权地导出用户数据。例如,数据虚拟化系统111(或其它实施例中的一个或多个其它系统)可以实现机器学习算法或AI来监控用户数据和对用户数据的操纵以确保没有用户数据或用户数据的部分被导出或复制出数据虚拟化系统111。

[0175] 数据虚拟化系统111也可以使用多种不同类型的算法。例如,在此的某些实施例可以使用逻辑回归模型。然而,其它模型也是可能的,诸如线性回归模型、离散选择模型、或广义线性模型。机器学习算法可以被配置为基于由数据虚拟化系统111接收到的新输入随时间推移自适应地开发和更新模型。例如,在数据虚拟化系统111接收或取得新用户信息时,可以周期性地重新生成模型,以帮助在更新用户数据时保持模型中的预测更准确。在此更详细地描述了数据虚拟化系统111。

[0176] 可用于生成和更新参数函数或预测模型的机器学习算法的一些非限制性示例可包括监督和非监督的机器学习算法,包括回归算法(诸如例如,普通最小二乘法回归)、基于实例的算法(诸如例如,学习向量量化)、决策树算法(诸如例如,分类和回归树)、贝叶斯算法(诸如例如,朴素贝叶斯)、聚类算法(诸如例如,k-means聚类)、关联规则学习算法(诸如例如,Apriori算法)、人工神经网络算法(诸如例如,感知机(Perceptron))、深度学习算法(诸如例如,深度波尔茨曼机(Deep Boltzmann Machine))、降维算法(诸如例如,主成分分析)、集成算法(诸如例如,堆栈泛化(Stacked Generalization))、或其它机器学习算法。

[0177] 这些机器学习算法可以包括任何类型的机器学习算法,包括分层聚类算法和聚类

分析算法,诸如k-means算法。在一些情况下,机器学习算法的执行可包括使用人工神经网络。通过使用机器学习技术,可以分析大量(诸如太字节或千万亿字节)的玩家交互数据以标识用户偏好。这些用户偏好可以使用历史数据来离线确定。此外,与不使用在此公开的技术的其它匹配系统相比,所确定的偏好随后可以实时用于选择匹配计划(如下面更详细描述),这可以提供增加的用户享受和因此参与度。

[0178] 在框610中,购买者可以分析用户数据和数据虚拟化系统111的虚拟环境内的任何其它统计数据。购买者只能提取结果分析和授权数据。例如,一些用户可能会授权导出他们相应的用户数据,而其他用户可能不会授权任何导出或一些导出功能(例如,用户的用户数据中仅一部分是可导出的,而另一部分可能是不可导出的)。

[0179] 在框612中,一旦数据虚拟化系统111被关闭(例如,在接收到来自购买者的终止指令时),数据虚拟化系统111关闭会话并且擦除数据虚拟化系统111已经接收到的任何用户数据和任何私有加密密钥。

[0180] 去标识化和假名化的用户数据的请求

[0181] 图6B示出用于处理对去标识化和假名化用户数据的请求的方法650的示例的流程图。某些附加的或替代的步骤在图3和图5中描述。

[0182] 在框614中,数据虚拟化系统111从购买者接收访问或购买用户数据的请求。该请求可以包括对用户数据的请求,该请求需要检查相关联的软件合约以及任何已经处理和存储的去标识化和假名化的用户数据。例如,在一些实施例中,系统(例如,数据平台112、代理106等)可以对用户数据进行去标识化或假名化,并将处理的数据存储在数据平台112中。在一些实施例中,可以检查和验证去标识化和假名化的用户数据,以确保用户数据被充分去标识化和假名化。在一些实施例中,用户必须在他们的隐私设置中指示他们是否允许他们的数据被去标识化和假名化,和/或提供给购买者。在一些实施例中,用户可能不需要做出指示,而是他们的一些或全部数据可以被去标识化和假名化并且提供给购买者。在一些实施例中,去标识化和假名化的用户数据仅包括关于用户整体的通用统计信息。某些过滤选项可以经由数据虚拟化系统111获得,以细化去标识化和假名化的用户数据的查看。

[0183] 在框616中,数据虚拟化系统111处理该请求以确定所请求的用户数据的哪些部分是可用的并且被授权与购买者共享(例如,去标识化和假名化的用户数据)以及所请求的用户数据的哪些部分需要用户经由软件合约表示和强制执行的隐私设置的附加批准。

[0184] 在框618中,对于所请求的用户数据中需要用户附加批准的部分,数据虚拟化系统111向代理106发送对用户数据的请求或使一批请求可用。在框620中,代理106接收对用户数据的请求。

[0185] 在框622中,代理106基于在框614中接收到的请求在分布式账本108或分布式账本中搜索与一个或多个用户相关联的一个或多个软件合约。关于图2A-2C提供了基于用户隐私设置创建软件合约的示例描述。附加步骤关于图3和图5进行讨论。例如,存在从图3中的框302和在图5中的框502开始的框622中继续的步骤。

[0186] 在框624中,对于所请求的用户数据中不需要用户的附加批准并且可用并且被授权与购买者共享的部分,数据虚拟化系统111向数据平台112发送对去标识化和假名化的用户数据的请求。在框626中,数据平台112接收对去标识化和假名化的用户数据的请求。

[0187] 在框628中,数据平台112定位任何去标识化和假名化的用户数据并将其发送到数

据虚拟化系统111。在框630中,数据平台112接收任何去标识化和假名化的用户数据。

[0188] 在框632中,一旦数据虚拟化系统111被关闭(例如,在接收到来自购买者的终止指令时),数据虚拟化系统111关闭会话并擦除任何用户数据,包括任何去标识化和假名化的用户数据,以及数据虚拟化系统111已经接收到的任何私有加密密钥。

[0189] 示例空间计算设备

[0190] 空间计算设备或诸如头戴式显示器(HMD)的可穿戴显示系统可以被配置为与诸如手持式用户输入设备的伴侣设备一起工作。空间计算设备可以包括面向外图像捕获设备,诸如相机,其可以对空间计算设备的用户的环境进行成像。图像捕获设备可用于捕获和获得显示在伴侣设备上的信息或数据(例如,密钥或秘密),以便在空间计算设备和伴侣设备之间建立共享信息或数据(例如,共享密钥、共享秘密、或签名密钥)。共享数据进而可以被空间计算设备或伴侣设备用于加密/解密用于/来自安全数据传输或数据平台的数据。

[0191] 图7A示出可用于向显示系统佩戴者或观看者1004呈现虚拟现实(VR)、增强现实(AR)或混合现实(MR)体验的空间计算设备或可穿戴显示系统1000的示例。可穿戴显示系统1000可被编程为执行在此描述的任何应用或实施例。显示系统1000包括显示器1008以及支持显示器1008的功能的各种机械和电子模块和系统。显示器1008可以被耦合到框架1012,该框架1012可由显示系统用户、佩戴者或观看者1004佩戴,并且被配置为将显示器1008定位在佩戴者1004的眼睛的前面。显示器1008可以是光场显示器。在一些实施例中,扬声器1016被耦合到框架1012并且被定位在用户耳道附近。在一些实施例中,另一个扬声器(未示出)被定位于用户的另一个耳道附近,以提供立体声/可塑形的声音控制。显示器1008诸如通过有线或无线连接可操作地耦合1020到本地数据处理模块1024,该本地数据处理模块1024可以安装在各种配置中,诸如固定地附接到框架1012、固定地附接到用户佩戴的头盔或帽子,嵌入耳机中,或以其它方式可移除地附接到用户1004(例如,在背包式配置中,在皮带耦合式配置中)。

[0192] 框架1012可以具有附接或安装到框架1012的一个或多个相机以获得佩戴者的眼睛的图像。在一个实施例中,相机可以安装到佩戴者的眼睛的前面的框架1012,使得可以直接对眼睛进行成像。在其它实施例中,相机可以沿着框架1012的杆被安装(例如,靠近佩戴者的耳朵)。在此类实施例中,显示器1008可以采用将来自佩戴者的眼睛的光反射回相机的材料进行涂覆。光可以是红外光,因为虹膜特征在红外图像中很突出。

[0193] 本地处理和数据模块1024可以包括硬件处理器,以及诸如非易失性存储器(例如,闪存)的非瞬态数字存储器,它们都可以用于辅助数据的处理、缓存和存储。数据可以包括如下数据:(a) 其从传感器(其例如可操作地耦合到框架1012或以其它方式附接到用户1004)捕获,诸如图像捕获设备(诸如相机)、麦克风、惯性测量单元、加速度计、指南针、GPS单元、无线电设备、或陀螺仪;或(b) 使用远程处理模块1028或远程数据存储库1032获取或处理,可能用于在此类处理或取得之后传送到显示器1008。本地处理和数据模块1024可以通过通信链路1036或1040(诸如经由有线或无线通信链路)可操作地耦合到远程处理模块1028和远程数据存储库1032,使得这些远程模块1028、1032可用作到本地处理和数据模块1024的资源。图像捕获设备可用于捕获眼睛图像处理过程中使用的眼睛图像。此外,远程处理模块1028和远程数据存储库1032可以可操作地彼此耦合。

[0194] 在一些实施例中,远程处理模块1028可以包括一个或多个处理器,该处理器被配

置为分析和处理数据或图像信息,诸如由图像捕获设备捕获的视频信息。视频数据可以本地存储在本地处理和数据模块1024中或在远程数据存储库1032中。在一些实施例中,远程数据存储库1032可以包括数字数据存储设施,其可以通过互联网或“云”资源配置中的其它联网配置获得。在一些实施例中,所有数据都被存储并且所有计算都在本地处理和数据模块1024中执行,从而允许从远程模块完全自主地使用。

[0195] 在一些实现方式中,本地处理和数据模块1024或远程处理模块1028被编程为执行如在此所述的系统和方法的实施例。图像捕获设备可以捕获特定应用的视频(例如,用于眼睛跟踪应用的佩戴者的眼睛的视频或用于手势标识应用的佩戴者的手部或手指的视频)。视频可由处理模块1024、1028之一或二者分析。在一些情况下,将虹膜代码生成中的至少一些卸载到远程处理模块(例如,在“云”中)可以提高计算的效率或速度。在此公开的系统和方法的参数可以被存储在数据模块1024或1028中。

[0196] 分析的结果可以被处理模块1024、1028中的一个或二者用于附加操作或处理。例如,在各种应用中,可穿戴显示系统1000可以使用生物度量标识、眼睛跟踪、识别、或手势、对象、姿势等的分类。例如,可穿戴显示系统1000可以分析捕获到的佩戴者1004的手部的视频并识别佩戴者的手部的手势(例如,拾取真实或虚拟对象、表示同意或反对(例如,“上竖大拇指”或“下竖大拇指”等),以及可穿戴显示系统。

[0197] 人类视觉系统是复杂的并且提供真实的深度感知是具有挑战性的。不受理论的限制,据信对象的观看者可能由于聚散和调节的组合而将对象感知为三维的。两只眼睛相对于彼此的聚散运动(例如,瞳孔朝向或远离彼此的滚动运动以聚散眼睛的视线以注视对象)与眼睛的晶状体的聚焦(或“调节”)密切相关。在正常情况下,改变眼睛的晶状体的焦点,或调节眼睛,将焦点从一个对象转移到另一个不同距离的对象,在称为“调节-聚散反射”的关系下,会自动导致相同距离的聚散的匹配变化。同样,在正常情况下,聚散的变化将触发调节的匹配变化。在调节和聚散之间提供更好匹配的显示系统可以形成更逼真或更舒适的三维图像模拟。

[0198] 另一个示例用户数据交易系统

[0199] 图7B示意性地示出用户数据交易系统的一个实施例。用户数据交易系统可以类似于图1中描述的用户数据交易系统100。用于基于通过使用代理(例如,图1的代理106)以及本公开的其它系统和组件而存储和实现的隐私设置来安全地交换用户数据的系统和方法可由一个或多个用户设备702a-702c(例如,来自图1的用户设备102或购买者设备104或图7A的可穿戴显示系统1000)、一个或多个代理706(例如,来自图1的代理106)、一个或多个数据平台712(例如,来自图1的数据平台112)、和数据虚拟化系统711(例如,来自图1的数据虚拟化系统111)实现。在图7B中所示的非限制性示例实施例中,用户701a可以操作用户设备702a和702b(例如,用户设备102可以包括此类设备)来创建和修改他们的用户隐私设置。在图7B中所示的非限制性示例实施例中,购买者701b可以操作用户设备702c来查看、交互、用附加数据来丰富,以及分析与用户701a或其他用户相关联的用户数据。

[0200] 用户设备702a-720c可以包括例如蜂窝电话、平板计算机、电子阅读器、智能手表、头戴式增强、虚拟或混合现实显示系统、可穿戴显示系统、图7A的可穿戴显示系统1000等。用户设备702a-c可以使用通信链路120a、120b(例如蜂窝通信链路或互联网连接)与网络718上的其它设备通信。网络718可以是可通过有线或无线通信链路(例如实现电气和电子

工程师协会 (IEEE) 802.11 标准) 可访问的局域网 (LAN)、广域网 (WAN)、或互联网。

[0201] 代理706可以使用通信链路126与网络718上的其它设备 (例如用户设备702a和702b) 通信。数据平台712可以与网络718上的其它设备 (例如代理706) 通信。数据虚拟化系统711可以与网络718上的其它设备 (例如代理706或用户设备702c) 通信。通信链路120a、120b、126、724、726或728可以是有线或无线通信、蜂窝通信、**蓝牙®**、局域网 (LAN)、广域网 (WLAN)、射频 (RF)、红外线 (IR)、或任何其它通信方法或系统。

[0202] 用户设备702a和702b可以将加密的用户数据发送到数据平台712。用户设备702a和702b还可以被用户701a用来经由代理706来配置或修改用户701a的隐私设置,这可以包括分布式账本 (例如,图1的分布式账本108)。购买者702b可以使用用户设备702c (例如,图1的购买者设备104) 以与数据虚拟化系统711通信以与存储在数据平台上的加密用户数据交互。

[0203] 附加的实现细节和实施例

[0204] 本公开的各种实施例可以是任何可能的技术细节集成级别的系统、方法或计算机程序产品。计算机程序产品可以包括计算机可读存储介质 (或多个介质), 其上具有计算机可读程序指令, 用于使处理器执行本公开的各方面。

[0205] 例如, 在此描述的功能可以在软件指令由一个或多个硬件处理器或任何其它合适的计算设备执行或响应于由一个或多个硬件处理器或任何其它合适的计算设备执行的软件指令时执行。软件指令或其它可执行代码可以从计算机可读存储介质 (或多个介质) 中读取。

[0206] 计算机可读存储介质可以是有形设备, 其可以保留和存储数据或指令以供指令执行设备使用。计算机可读存储介质可以是例如但不限于电子存储设备 (包括任何易失性或非易失性电子存储设备)、磁存储设备、光存储设备、电磁存储设备、半导体存储设备, 或前述的任何合适的组合。计算机可读存储介质的更具体示例的非详尽列表包括以下: 便携式计算机软盘、硬盘、固态驱动器、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或闪存)、静态随机存取存储器 (SRAM)、便携式光盘只读存储器 (CD-ROM)、数字多功能磁盘 (DVD)、记忆棒、软盘、机械编码设备 (诸如穿孔卡片或凹槽中记录有指令的凸起结构), 以及前述的任何合适组合。如在此使用的计算机可读存储介质不应被解释为瞬态信号本身, 诸如无线电波或其它自由传播的电磁波、通过波导或其它传输介质传播的电磁波 (例如, 光脉冲通过光缆) 或通过电线传输的电信号。

[0207] 在此描述的计算机可读程序指令可以从计算机可读存储介质下载到相应的计算/处理设备或经由网络 (例如互联网、局域网、广域网、或无线网络) 下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光传输光纤、无线传输、路由器、防火墙、交换机、网关计算机、或边缘服务器。每个计算/处理设备中的网络适配卡或网络接口从网络接收计算机可读程序指令并转发计算机可读程序指令以存储在相应的计算/处理设备内的计算机可读存储介质中。

[0208] 用于执行本公开的操作的计算机可读程序指令 (例如在此也称为“代码”、“指令”、“模块”、“应用”、“软件应用”等) 可以是汇编指令、指令集架构 (ISA) 指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、集成电路的配置数据, 或者以一种或多种编程语言的任何组合编写的源代码或目标代码, 包括面向对象的编程语言, 诸如Smalltalk、C++

等,以及过程编程语言,诸如“C”编程语言或类似的编程语言。计算机可读程序指令可从其它指令或从自身调用,或可响应于检测到的事件或中断而被调用。被配置为在计算设备上执行的计算机可读程序指令可以在计算机可读存储介质上提供,或作为然后可以存储在计算机可读存储介质上的数字下载(并且可以最初以需要在执行之前安装、解压或解密的压缩或可安装格式存储)。此类计算机可读程序指令可以部分或全部存储在执行计算设备的存储器设备(例如,计算机可读存储介质)上,以供计算设备执行。计算机可读程序指令可以完全在用户计算机(例如,执行计算设备)上,部分地在用户计算机上,作为独立软件包,部分地在用户的计算机上并且部分地在远程计算机上,或者完全在远程计算机或服务器上执行。在后一场景中,远程计算机可以通过任何类型的网络连接到用户的计算机,包括局域网(LAN)或广域网(WAN),或者可以连接到外部计算机(例如,使用互联网服务提供商通过互联网)。在一些实施例中,包括例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA)的电子电路可以通过利用计算机可读程序指令的状态信息来执行计算机可读程序指令来个性化电子电路,以便执行本公开的方面。

[0209] 在此参考根据本公开的实施例的方法、装置(系统)和计算机程序产品的流程图或框图来描述本公开的方面。应当理解,流程图或框图的每个框,以及流程图或框图中的框的组合,可以由计算机可读程序指令来实现。

[0210] 这些计算机可读程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理器以产生机器,使得经由计算机的处理器或其它可编程数据处理装置执行的指令创建用于实现在流程图或框图的一个框或多个框中指定的功能/动作的部件。这些计算机可读程序指令也可以存储在计算机可读存储介质中,该计算机可读存储介质可以引导计算机、可编程数据处理装置或其它设备以特定方式运行,使得其中存储有指令的计算机可读存储介质包括制品,该制品包括实现在一个或多个流程图或框图的一个框或多个框中指定的功能/动作的各方面的指令。

[0211] 计算机可读程序指令也可以加载到计算机、其它可编程数据处理装置或其它设备上,以使得在计算机、其它可编程装置或其它设备上执行一系列可操作步骤以产生计算机实现的过程,使得在计算机、其它可编程装置或其它设备上执行的指令实现流程图或框图的一个框或多个框中指定的功能/动作。例如,指令最初可以携带在远程计算机的磁盘或固态驱动器上。远程计算机可以将指令或模块加载到远程计算机的动态存储器中,并使用调制解调器通过电话、电缆或光线路发送指令。服务器计算系统本地的调制解调器可以在电话/电缆/光线上接收数据并使用包括适当电路的转换器设备将数据放置在总线上。总线可以将数据携带到存储器,处理器可以从该存储器取得和执行指令。由存储器接收的指令可以可选地在由计算机处理器执行之前或之后存储在存储设备(例如,固态驱动器)上。

[0212] 图中的流程图和框图示出根据本公开的各种实施例的系统、方法和计算机程序产品的可能实现方式的架构、功能和操作。在该方面,流程图或框图中的每个框可表示模块、分段或指令的一部分,其包括用于实现指定逻辑功能的一个或多个可执行指令。在一些替代实现方式中,框中标注的功能可以不按照图中标注的顺序发生。例如,取决于所涉及的功能,连续示出的两个框实际上可以基本上同时执行,或者该框有时可以以相反的顺序执行。此外,在一些实现方式中可以省略某些框。在此描述的方法和过程也不限于任何特定的顺序,并且与其相关的框或状态可以以其它合适的顺序执行。

[0213] 因此,虽然可以在附图中以特定顺序描述操作,但是应当认识到,此类操作不需要以所示的特定顺序或按顺序执行,或者执行所有所示的操作,以实现期望的结果。此外,附图可以以流程图的形式示意性地描绘另一个示例过程。然而,未描绘的其它操作可以并入示意性说明的示例方法和过程中。例如,一个或多个附加操作可以在任何所示操作之前、之后、同时或之间执行。此外,在其它实现方式中,操作可以重新排列或重新排序。在某些情况下,多任务和并行处理可能是有利的。此外,上述实现方式中各种系统组件的分离不应理解为在所有实现方式中都需要此类分离,应当理解,所述的程序组件和系统通常可以一起集成在单个软件产品中或打包成多个软件产品。此外,其它实现方式在所附权利要求的范围内。在某些情况下,权利要求中所述的动作可以以不同的顺序执行,并且仍能达到期望的结果。

[0214] 还将注意,框图或流程图图示的每个框,以及框图或流程图图示中的框的组合,可以通过基于专用硬件的系统来实现,该系统执行指定的功能或动作或执行专用硬件和计算机指令的组合。例如,前述部分中描述的任何过程、方法、算法、元素、框、应用或其它功能(或功能的部分)可以体现在电子硬件中,诸如专用处理器(例如,专用集成电路(ASIC))、可编程处理器(例如,现场可编程门阵列(FPGA))、专用电路等(其中任何一个也可以将定制硬连线逻辑、逻辑电路、ASIC、FPGA等与完成这些技术的软件指令的定制编程/执行相结合),或经由电子硬件完全或部分地自动化。

[0215] 任何上述处理器或包含任何上述处理器的设备在此可被称为例如“计算机”、“计算机设备”、“计算设备”、“硬件计算设备”、“硬件处理器”、“处理单元”等。上述实施例的计算设备一般可以(但不一定)由操作系统软件控制或协调,诸如Mac OS、iOS、Android、Chrome OS、Windows OS(例如,Windows XP、Windows Vista、Windows 7、Windows 8、Windows 10、Windows Server等)、Windows CE、Unix、Linux、SunOS、Solaris、Blackberry OS、VxWorks或其它合适的操作系统。在其它实施例中,计算设备可以由专有操作系统控制。传统操作系统控制和调度计算机进程以供执行、执行存储器管理、提供文件系统、联网、I/O服务,并提供用户界面功能,诸如图形用户界面(“GUI”),等等。

[0216] 例如,图8是示出可以在其上实现各种实施例的计算机系统800的框图。此类计算机系统800可以包括如在此所述的代理、分布式账本、用户设备、数据平台或数据虚拟化系统的部分。计算机系统800可用于实现参考图7B描述的系统。计算机系统800包括总线802或用于传送信息的其它通信机制,以及与总线802耦合以处理信息的硬件处理器或多个处理器804。硬件处理器804例如可以是一个或多个通用微处理器。

[0217] 计算机系统800还包括主存储器806,诸如随机存取存储器(RAM)、高速缓存或其它动态存储设备,其耦合到总线802用于存储要由处理器804执行的信息和指令。主存储器806还可用于在执行将由处理器804执行的指令期间存储临时变量或其它中间信息。此类指令当存储在处理器804可访问的存储介质中时,将计算机系统800呈现为定制为执行指令中指定的操作的专用机器。

[0218] 计算机系统800进一步包括只读存储器(ROM) 808或耦合到总线802的其它静态存储设备,用于存储用于处理器804的静态信息和指令。存储设备810,诸如磁盘、光盘或USB拇指驱动器(闪存驱动器)等被提供并耦合到总线802用于存储信息和指令。

[0219] 计算机系统800可以经由总线802耦合到显示器812,诸如阴极射线管(CRT)或LCD

显示器(或触摸屏),用于向计算机用户显示信息。计算机系统800可以经由总线802或网络链路820耦合到用户设备824,该用户设备824可以包括增强、混合或虚拟现实显示设备,诸如例如用户设备102、104、702a-702c、1000。此外,计算机系统800本身还可以包括增强的、混合的或虚拟现实显示设备,诸如例如用户设备102、104、702a-702c、1000。包括字母数字键和其它键的输入设备814耦合到总线802用于将信息和命令选择传送到处理器804。另一种类型的用户输入设备是光标控制816,诸如鼠标、轨迹球或光标方向键,用于将方向信息和命令选择传送到处理器804并用于控制光标在显示器812上的运动。该输入设备通常在两个轴中具有两个自由度,第一轴(例如,x)和第二轴(例如,y),这允许设备指定平面中的位置。在一些实施例中,在没有光标的情况下可以经由接收触摸屏上的触摸来实现与光标控制相同的方向信息和命令选择。

[0220] 计算系统800可以包括用户界面模块以实现可以作为由计算设备执行的计算机可执行程序指令存储在大容量存储设备中的GUI。如下所述,计算机系统800可以进一步使用定制的硬连线逻辑、一个或多个ASIC或FPGA、固件或程序逻辑来实现在此所述的技术,该逻辑与计算机系统相结合导致或编程计算机系统800为特殊用途机器。根据一个实施例,在此的技术由计算机系统800响应于处理器804执行包含在主存储器806中的一个或多个计算机可读程序指令的一个或多个序列而执行。此类指令可以从另一个存储介质(诸如存储设备810)读入主存储器806。执行包含在主存储器806中的指令序列导致处理器804执行在此描述的处理步骤。在替代实施例中,可以使用硬连线电路代替软件指令或与软件指令结合使用。

[0221] 各种形式的计算机可读存储介质可以涉及将一个或多个计算机可读程序指令的一个或多个序列传送到处理器804以供执行。例如,指令最初可以承载在远程计算机的磁盘或固态驱动器上。远程计算机可以将指令加载到远程计算机的动态存储器中,并使用调制解调器通过电话线发送指令。计算机系统800本地的调制解调器可以在电话线上接收数据并使用红外线发射器将数据转换成红外线信号。红外线检测器可以接收红外线信号中携带的数据,并且适当的电路可以将数据放在总线802上。总线802将数据传送到主存储器806,处理器804从该主存储器806取得并执行指令。由主存储器806接收的指令可以可选地在处理器804执行之前或之后存储在存储设备810上。

[0222] 计算机系统800还包括耦合到总线802的通信接口818。通信接口818提供到连接到本地网络822的网络链路820的双向数据通信耦合。例如,通信接口818可以是综合服务数字网络(ISDN)卡、电缆调制解调器、卫星调制解调器或调制解调器,用于提供与对应类型的电话线的数据通信连接。作为另一个示例,通信接口818可以是局域网(LAN)卡,以提供到兼容LAN(或WAN组件以与WAN通信)的数据通信连接。也可以实现无线链路。在任何此类实现方式中,通信接口818发送和接收携带表示各种类型信息的数字数据流的电、电磁或光信号。

[0223] 网络链路820通常通过一个或多个网络向其它数据设备提供数据通信。例如,网络链路820可以通过局域网822向用户设备824或由互联网服务提供商(ISP)826操作的数据设备提供连接。ISP 826进而通过现在通常称为“互联网”828的全球分组数据通信网络提供数据通信服务。本地网络822和互联网828二者都使用携带数字数据流的电、电磁或光信号。通过各种网络的信号和网络链路820上的信号和通过通信接口818的信号(它们携带数字数据进出计算机系统800)是传输介质的示例形式。

[0224] 计算机系统800可以通过网络、网络链路820和通信接口818发送消息和接收数据,包括程序代码。在互联网示例中,服务器830可能通过互联网828、ISP 826、本地网络822和通信接口818发送应用程序的请求代码。例如,服务器830可以包括用户数据交易系统100、数据可视化系统111、代理106、数据平台112、或用户数据隐私系统103中的一些或全部。

[0225] 接收的代码可以在接收到时由处理器804执行,或者存储在存储设备810或其它非易失性存储中以供以后执行。

[0226] 附加注意事项

[0227] 如上所述,在各种实施例中,用户可以通过基于网络的查看器(诸如网络浏览器)或其它合适的软件程序访问某些功能。在此类实现方式中,用户界面可以由服务器计算系统生成并发送到用户的网络浏览器(例如,在用户的计算系统上运行)。可替代地,用于生成用户界面所需的数据(例如,用户界面数据)可以由服务器计算系统提供给浏览器,其中可以生成用户界面(例如,用户界面数据可以由访问浏览器服务的浏览器执行,并且可以配置为基于用户界面数据呈现用户界面)。然后用户可以通过网络浏览器与用户界面交互。某些实现方式的用户界面可以通过一个或多个专用软件应用访问。在某些实施例中,本公开的一个或多个计算设备或系统可以包括移动计算设备,并且用户界面可以通过此类移动计算设备(例如,智能手机或平板计算机)访问。

[0228] 在一些实施例中,数据可以在适当的情况下以图形表示形式呈现,诸如可视表示形式,诸如图表和图形,以允许用户舒适地查看大量数据并利用人类特别强的与视觉刺激相关的模式识别能力。在一些实施例中,系统可以呈现总量,诸如总数、计数和平均值。该系统还可以利用该信息进行内插或外推,例如预测未来的发展。

[0229] 此外,在此描述的交互式 and 动态用户界面通过用户界面与底层系统和组件之间的有效交互的创新来实现。例如,在此公开了接收用户输入、将这些输入翻译和传递到各种系统组件、响应于输入传递的复杂过程的自动和动态执行、系统的各种组件和过程之间的自动交互、以及用户界面的自动和动态更新的改进方法。经由在此描述的交互式用户界面的数据交互和呈现可以相应地提供认知和人体工程学效率和优于先前系统的优势。

[0230] 本公开的各种实施例提供对各种技术和技术领域的改进。例如,如上所述,现有的数据存储和处理技术(包括,例如,在存储器数据库中)在各种方面受到限制(例如,手动数据查看速度慢、成本高且不太详细;数据量太大;等等),并且本公开的各种实施例提供了优于此类技术的显著改进。此外,本公开的各种实施例与计算机技术密切相关。特别地,各种实施例依赖于经由图形用户界面检测用户输入、基于那些用户输入计算对显示的电子数据的更新、相关电子数据的自动处理、以及经由交互式图形用户界面对显示的图像的更新的呈现。此类特征和其它特征(例如,大量电子数据的处理和分析)与计算机技术密切相关并由计算机技术支持,并且除了计算机技术之外不会存在。例如,在没有实现它们的计算机技术的情况下,以下参考各种实施例描述的与显示数据的交互不能由人类单独合理地执行。此外,通过计算机技术实现本公开的各种实施例能够实现在此描述的许多优点,包括与各种类型的电子数据的更有效的交互和呈现。

[0231] 在各种实施例中,公开了系统或计算机系统,其包括具有嵌入其中的程序指令的计算机可读存储介质,以及被配置为执行程序指令以使一个或多个处理器执行包括上述或下述实施例的一个或多个方面(包括所附权利要求的一个或多个方面)的操作的一个或多

个处理器。

[0232] 在各种实施例中,公开了包括计算机可读存储介质的计算机程序产品,其中计算机可读存储介质具有嵌入其中的程序指令,该程序指令可由一个或多个处理器执行以使一个或多个处理器执行包括上述和/或下述实施例的一个或多个方面(包括所附权利要求的一个或多个方面)的操作。

[0233] 可以对上述实施例进行许多变化和修改,其中的元素将被理解为其它可接受的示例。所有这些修改和变化都旨在包括在本公开的范围。前面的描述详述了某些实施例。然而,将理解的是,无论上述在文本中显得多么详细,系统和方法都可以以多种方式实践。还如上所述,应当注意,在描述系统和方法的某些特征或方面时使用特定术语不应被视为暗示该术语在此被重新定义以限于包括与该术语相关联的系统和方法的特征或方面的任何特定特性。

[0234] 除非另有特别说明,或在所使用的上下文中以其它方式理解,否则条件语言(诸如“能够”、“可”、“可能”或“可以”等)通常旨在传达某些实施例包括,而其它实施例不包括某些特征、元素和/或步骤。因此,此类条件语言通常不旨在暗示特征、元素和/或步骤对于一个或多个实施例以任何方式是必需的,或者一个或多个实施例必然包括用于在具有或不具有用户输入或提示的情况下决定这些特征、元素和/或步骤是否被包括在任何特定实施例中或将在任何特定实施例中执行。

[0235] 如在此使用的术语“组件”、“代理”、“模块”、“设备”、“机构”、“单元”、“元件”、“构件”、“装置”、“机器”、“处理器”或“系统”不应解释为调用手段加功能声明语言。例如,用此类术语描述的元素应被解释为能够执行与该术语相关联的任何要求保护的操作,而无需使用或应用特殊或特定编程。

[0236] 当与术语“实时”结合使用时,术语“基本上”形成本领域普通技术人员将容易理解的短语。例如,很容易理解,此类语言将包括没有或几乎没有延迟或等待可辨别的速度,或者此类延迟足够短从而不会干扰、刺激或以其它方式使用户烦恼的速度。

[0237] 除非另外具体说明,诸如短语“X、Y和Z中的至少一个”或“X、Y或Z中的至少一个”等连词应与所使用的上下文一起理解通常表示项目、术语等可以是X、Y或Z,或它们的组合。例如,术语“或”以其包含的意义(而非排他的意义)使用,使得例如当用于连接元素列表时,术语“或”意味着列表中的一个、一些或全部元素。因此,此类连词一般不旨在暗示某些实施例需要X中的至少一个、Y中的至少一个和Z中的至少一个各自存在。

[0238] 如在此所使用并在所附权利要求中的术语“一个”应被赋予包含性而非排他性的解释。例如,除非特别说明,术语“一个”不应理解为表示“恰好一个”或“一个且只有一个”;相反,术语“一个”表示“一个或多个”或“至少一个”,无论是在权利要求中还是在说明书的其它地方使用,也无论在权利要求或说明书的其它地方使用诸如“至少一个”、“一个或多个”或“多个”等量词。

[0239] 在此使用的条件性语言,诸如“能够”、“可”、“可能”、“可以”、“例如”等,除非另有明确说明,或在所使用的上下文中以其它方式理解,通常旨在传达某些实施例包括,而其它实施例不包括某些特征、元件和/或步骤。因此,此类条件性语言通常不旨在暗示特征、元素和/或步骤以任何方式对于一个或多个实施例来说是必需的,或者一个或多个实施例必须包括用于在有或没有作者输入或提示的情况下决定是否这些特征、元素和/或步骤被包括

或将在任何特定实施例中执行。术语“包含”、“包括”、“具有”等是同义词,并且以开放式的方式包容性地使用,并且不排除其它元素、特征、动作、操作等。例如,包括一个或多个处理器的通用计算机不应被解释为排除其它计算机组件,并且可能包括诸如存储器、输入/输出设备和/或网络接口等的组件。

[0240] 虽然以上详细描述已经示出、描述和指出了应用于各种实施例的新颖特征,但是可以理解,在不脱离本公开的精神的情况下,可以对所示出的设备或过程的形式和细节进行各种省略、替换和改变。可以认识到,在此描述的本发明的某些实施例可以在不提供在此阐述的所有特征和益处的形式中体现,因为一些特征可以与其它特征分开使用或实践。在此公开的某些发明的范围由所附权利要求而不是由前述说明指示。落入权利要求的等效含义和范围内的所有变化都应包含在其范围内。

[0241] 在此描述和/或在附图中描绘的过程、方法和算法中的每一个可以体现在由一个或多个物理计算系统、硬件计算机处理器、特定应用电路,和/或被配置为执行特定和特别的计算机指令的电子硬件执行的代码模块中,并由其完全或部分自动化。例如,计算系统可以包括用特定计算机指令或专用计算机、专用电路等编程的通用计算机(例如,服务器)。代码模块可以编译并链接到可执行程序中,安装在动态链接库中,或者可以用解释的编程语言编写。在一些实现方式中,特定操作和方法可以由特定于给定功能的电路来执行。

[0242] 此外,本公开的功能的某些实现方式在数学上、计算上或技术上足够复杂,以至于可能需要特定应用的硬件或一个或多个物理计算设备(利用适当的专用可执行指令)来执行该功能,例如,由于所涉及计算的数量或复杂性,或为了提供基本上实时的结果。例如,视频可能包括许多帧,每帧具有数百万像素,并且需要专门编程的计算机硬件来处理视频数据,以便以商业上合理的时间量提供所需的图像处理任务或应用。

[0243] 代码模块或任何类型的数据可以存储在任何类型的非暂态计算机可读介质上,诸如物理计算机存储器,包括硬盘驱动器、固态存储器、随机存取存储器(RAM)、只读存储器(ROM)、光盘、易失性或非易失性存储器、它们的组合等。方法和模块(或数据)也可以作为各种计算机可读传输介质上发送生成的数据信号(例如,作为载波或其它模拟或数字传播信号的一部分),包括基于无线和有线/基于电缆的介质,并且可以采用多种形式(例如,作为单个或多路复用模拟信号的一部分,或作为多个离散数字数据包或帧)。所公开的过程或过程步骤的结果可以持久地或以其它方式存储在任何类型的非暂态有形计算机存储器中,或者可以经由计算机可读传输介质进行通信。

[0244] 在此描述和/或在附图中描绘的流程图中的任何过程、框、状态、步骤或功能应被理解为潜在地表示代码模块、段或代码部分,其包括一个或多个可执行指令用于实现过程中的特定功能(例如,逻辑或算术)或步骤。各种过程、框、状态、步骤或功能可以从在此提供的说明性示例组合、重新排列、添加、删除、修改或以其它方式改变。在一些实施例中,附加的或不同的计算系统或代码模块可以执行在此描述的一些或所有功能。在此所述的方法和过程也不限于任何特定顺序,并且与其相关的框、步骤或状态可以以适当的其它顺序执行,例如串行、并行或以一些其它方式。任务或事件可以被添加到所公开的示例实施例中或从所公开的示例实施例中移除。此外,在此描述的实现方式中各种系统组件的分离是出于说明性目的,不应理解为在所有实现方式中都需要这种分离。应当理解,所述的程序组件、方法和系统通常可以一起集成在单个计算机产品中或封装到多个计算机产品中。许多实现方

式变化是可能的。

[0245] 过程、方法和系统可以在网络(或分布式)计算环境中实现。网络环境包括企业范围的计算机网络、内部网、局域网(LAN)、广域网(WAN)、个域网(PAN)、云计算网络、众包计算网络、互联网和万维网。网络可以是有线或无线网络或任何其它类型的通信网络。

[0246] 本公开的系统和方法各自具有若干创新方面,其中没有一个单独负责或要求在此公开的期望属性。在此所述的各种特征和过程可以彼此独立地使用,或者可以以各种方式组合使用。所有可能的组合和子组合旨在落入本公开的范围。对本公开中描述的实现方式的各种修改对于本领域的技术人员来说是显而易见的,并且在不脱离本公开的精神或范围的情况下,本文定义的一般原理可以应用于其它实现方式。因此,权利要求不旨在限于在此所示的实现方式,而是要被赋予与本公开、在此公开的原理和新颖特征一致的最宽范围。

[0247] 本说明书中在单独实现方式的上下文中描述的某些特征也可以在单个实现方式中组合实现。相反,在单个实现方式的上下文中描述的各种特征也可以在多个实现方式中单独或以任何合适的子组合来实现。此外,尽管特征可能在某些组合中被描述为在某些组合中起作用,并且甚至最初如此要求保护,但在某些情况下,来自要求保护的组合的一个或多个特征可以从组合中删除,并且要求保护的组合可以涉及子组合或子组合的变体。没有单个特征或特征组对于每个和所有实施例都是必需的或必不可少的。

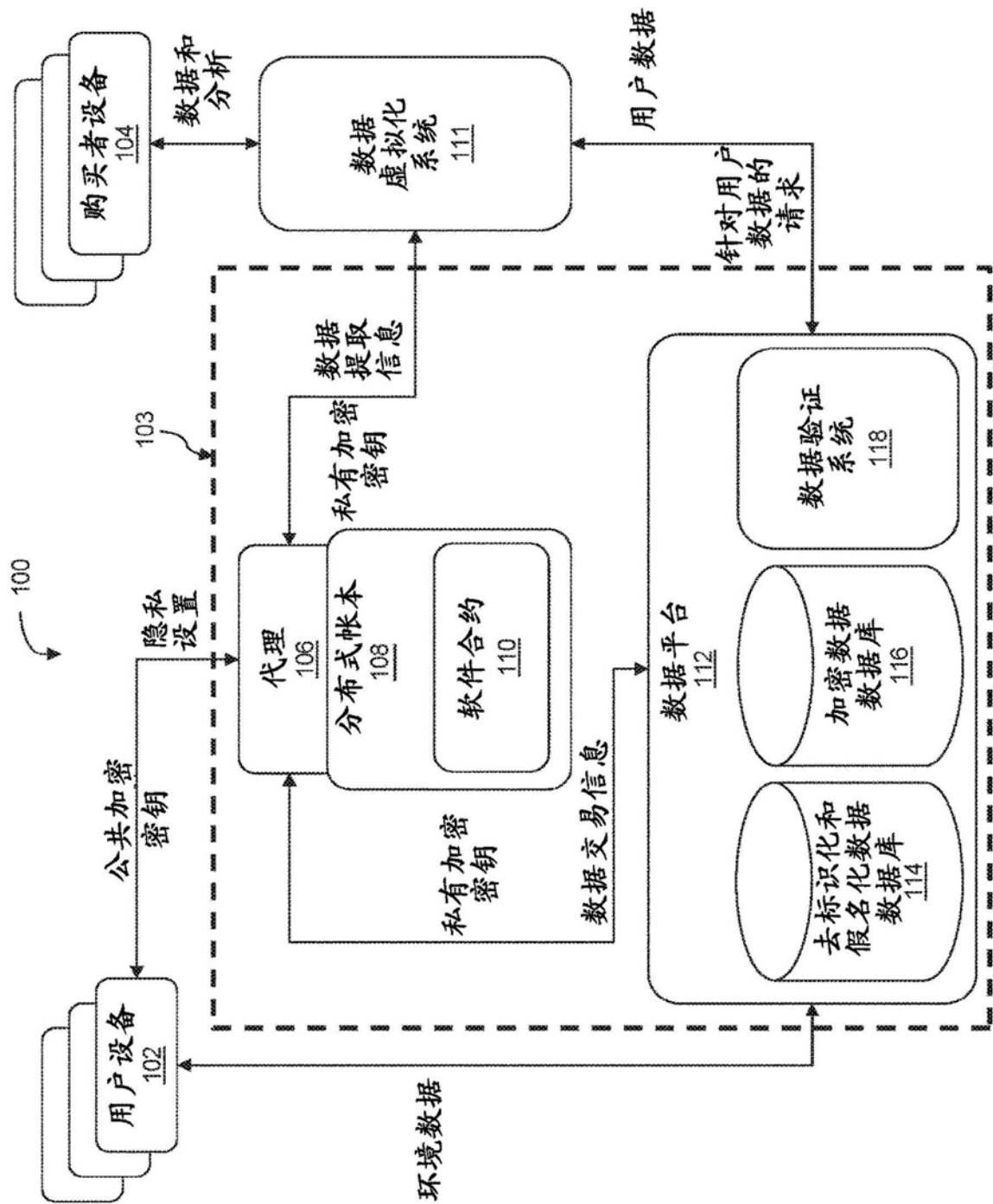


图1

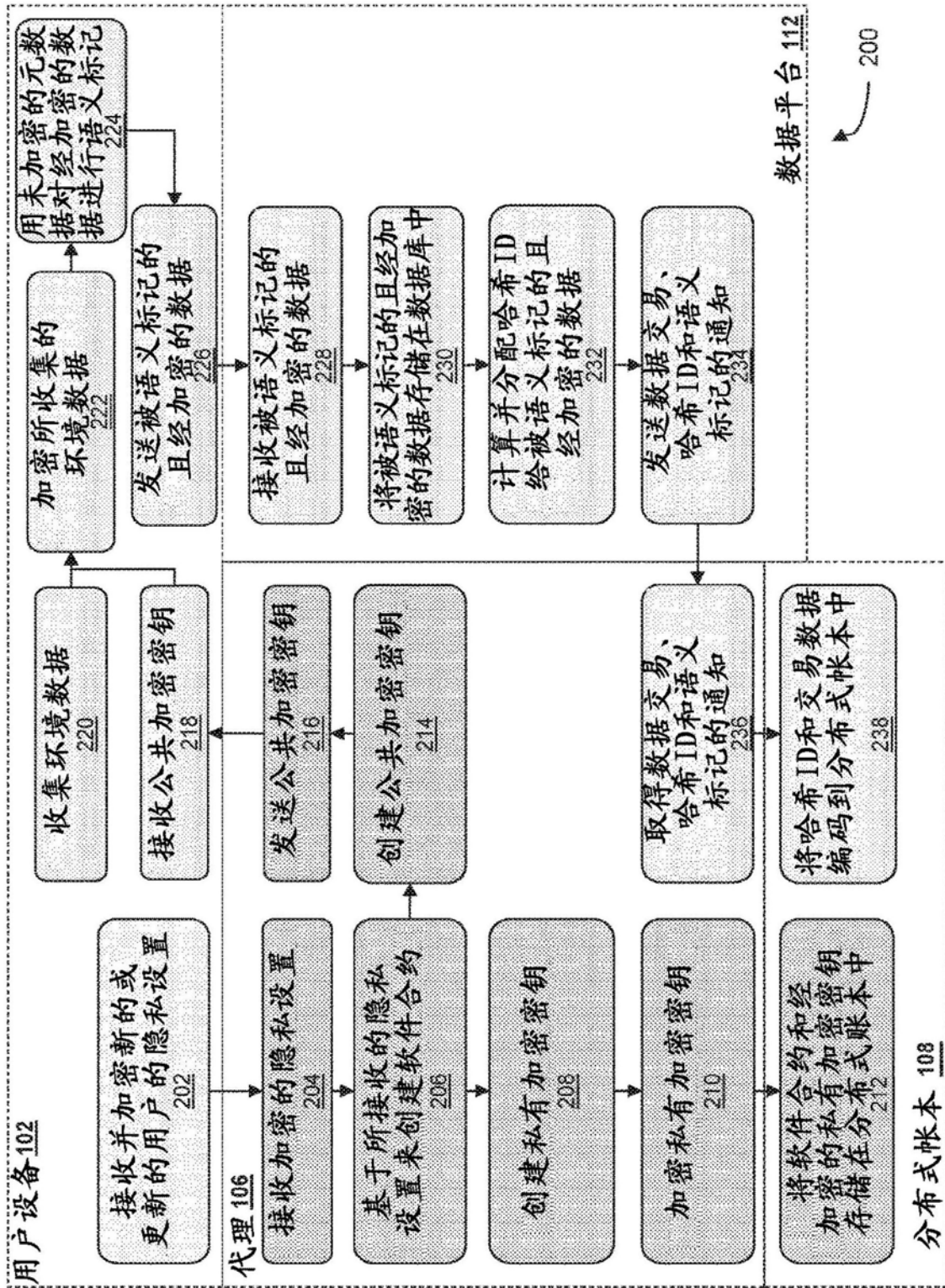


图2A

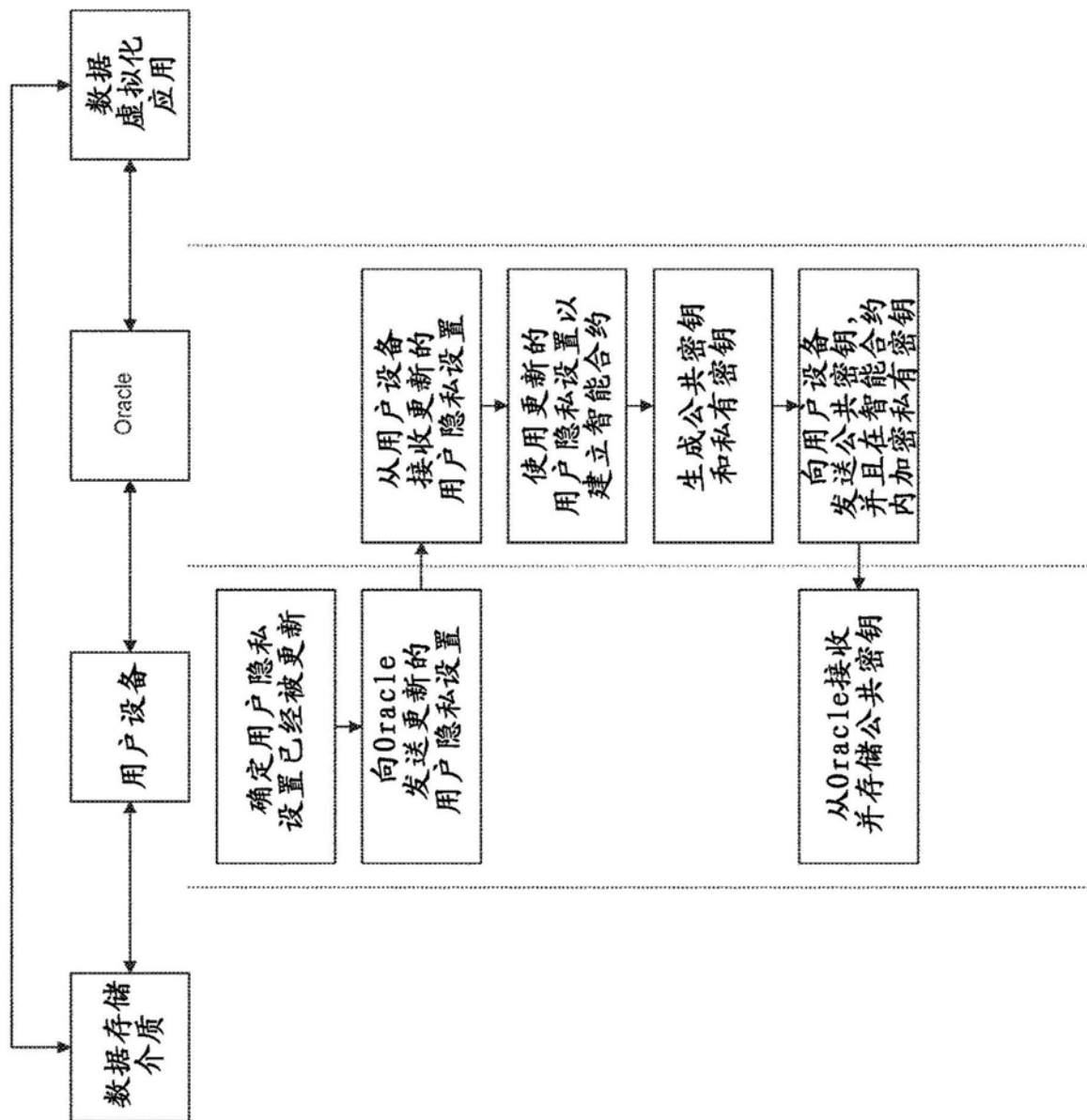


图2B

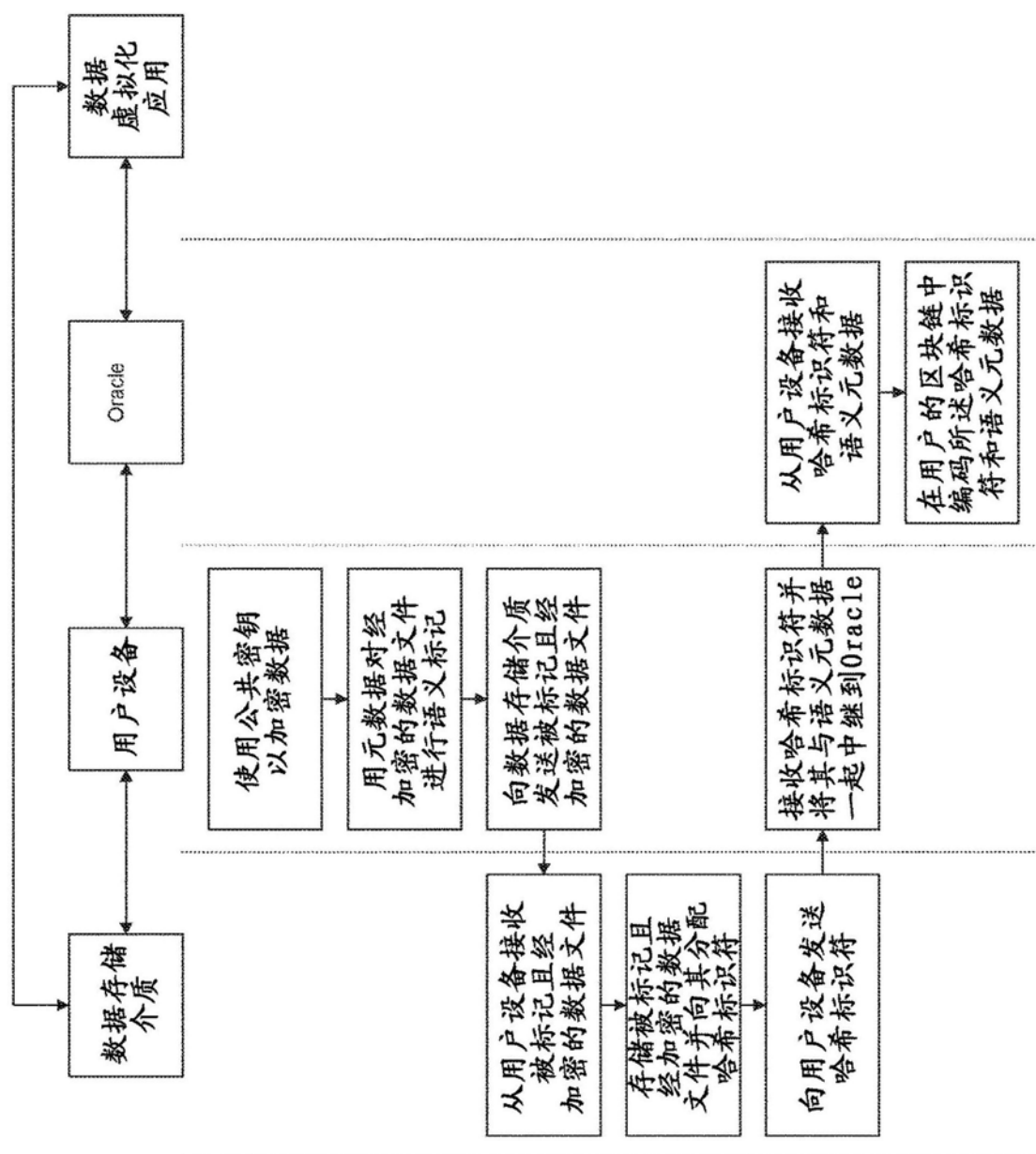


图2C

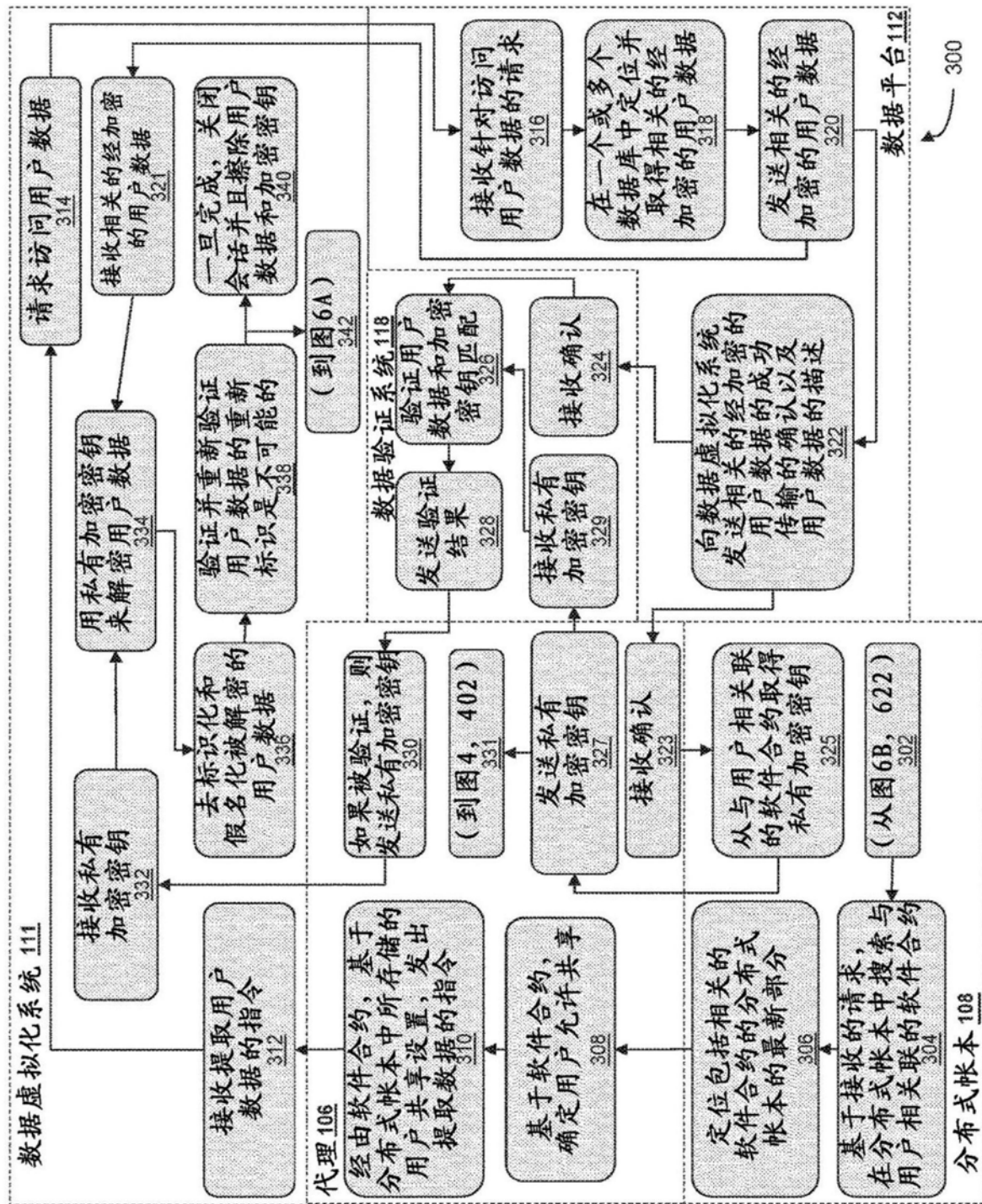


图3

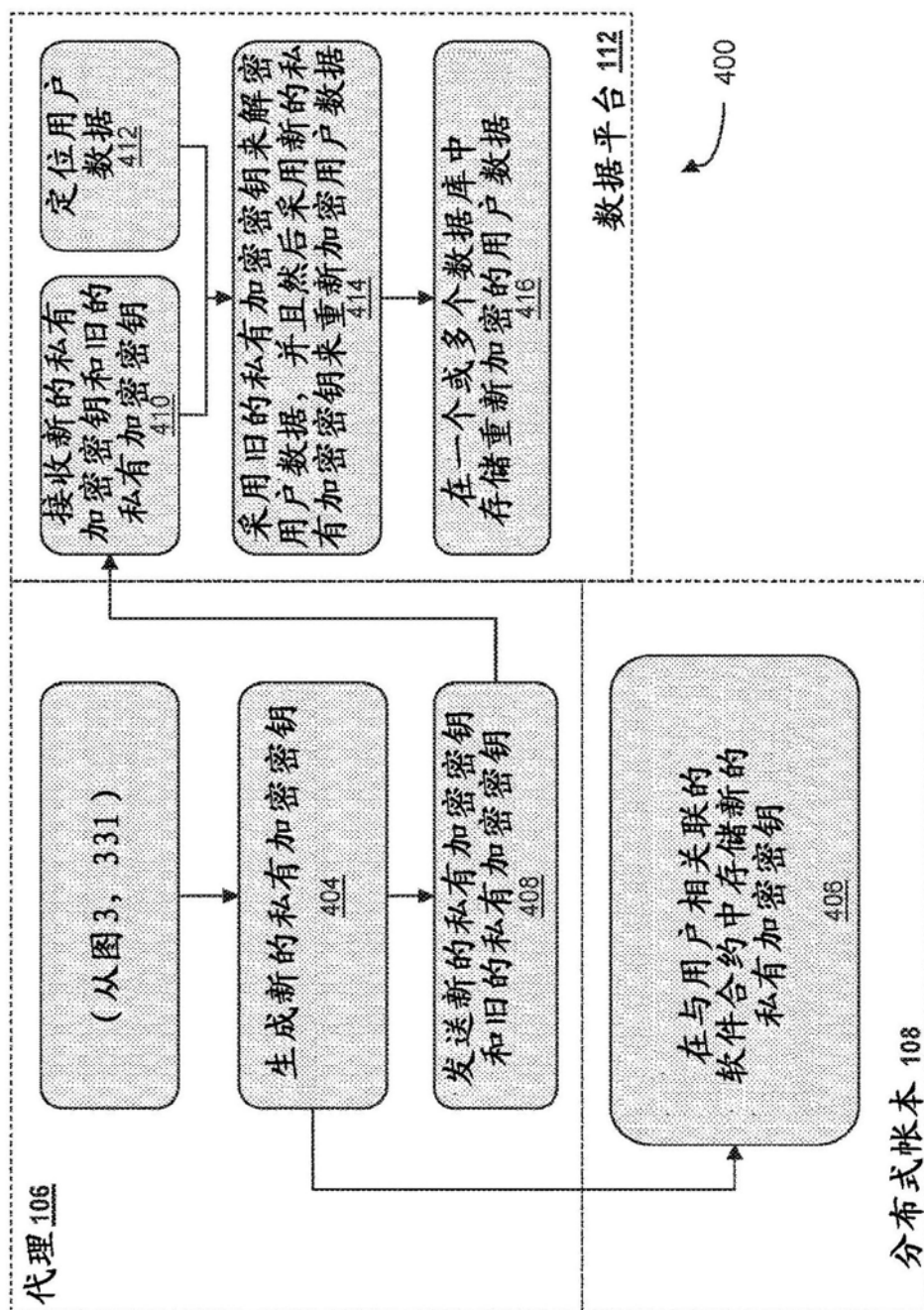


图4

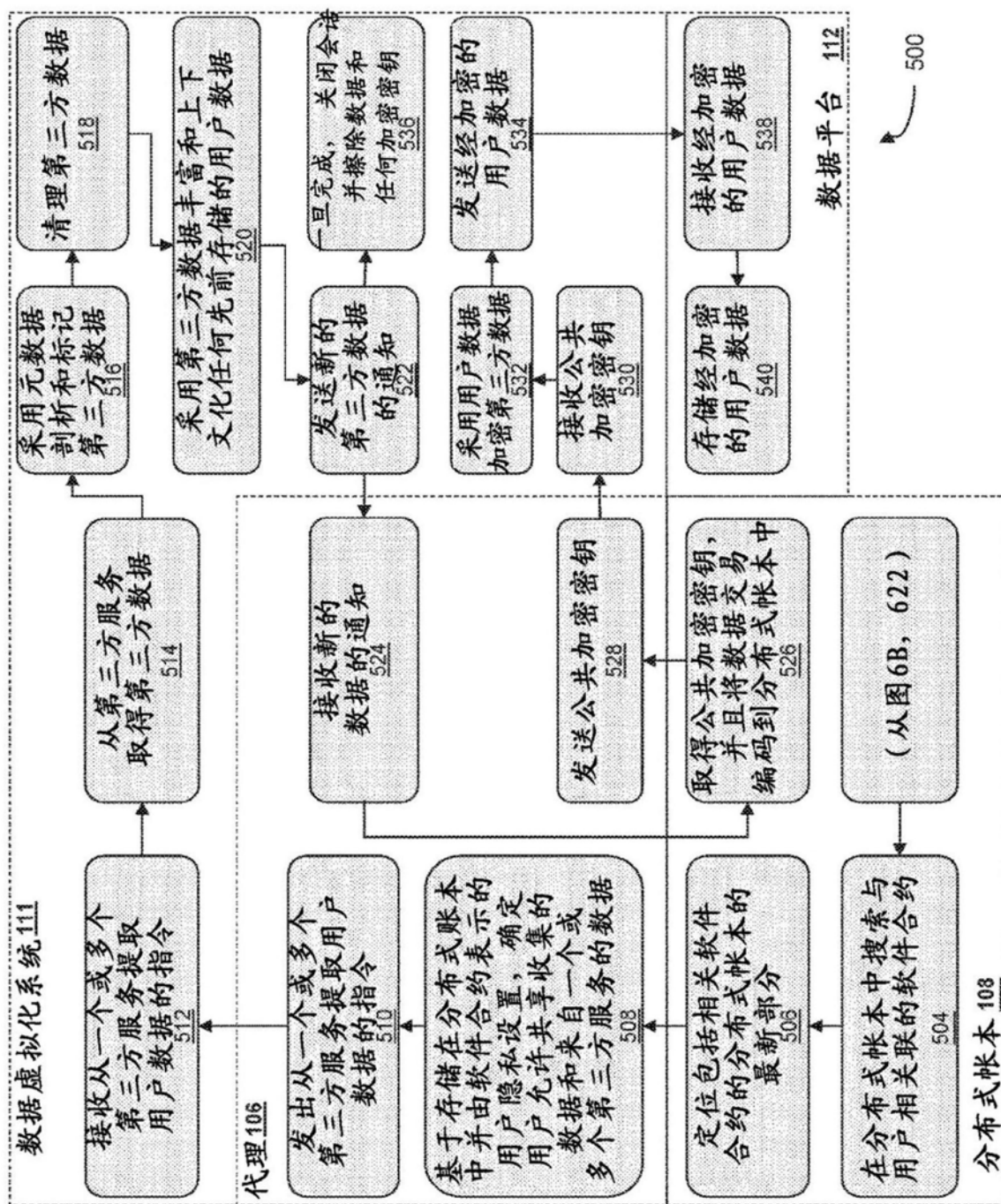


图5

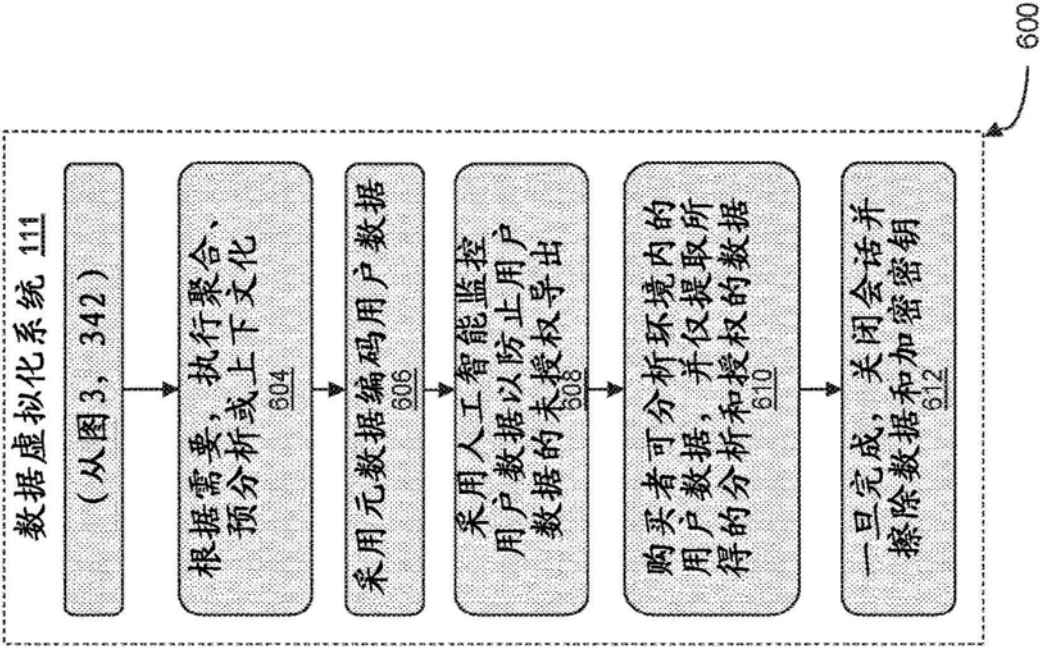


图6A

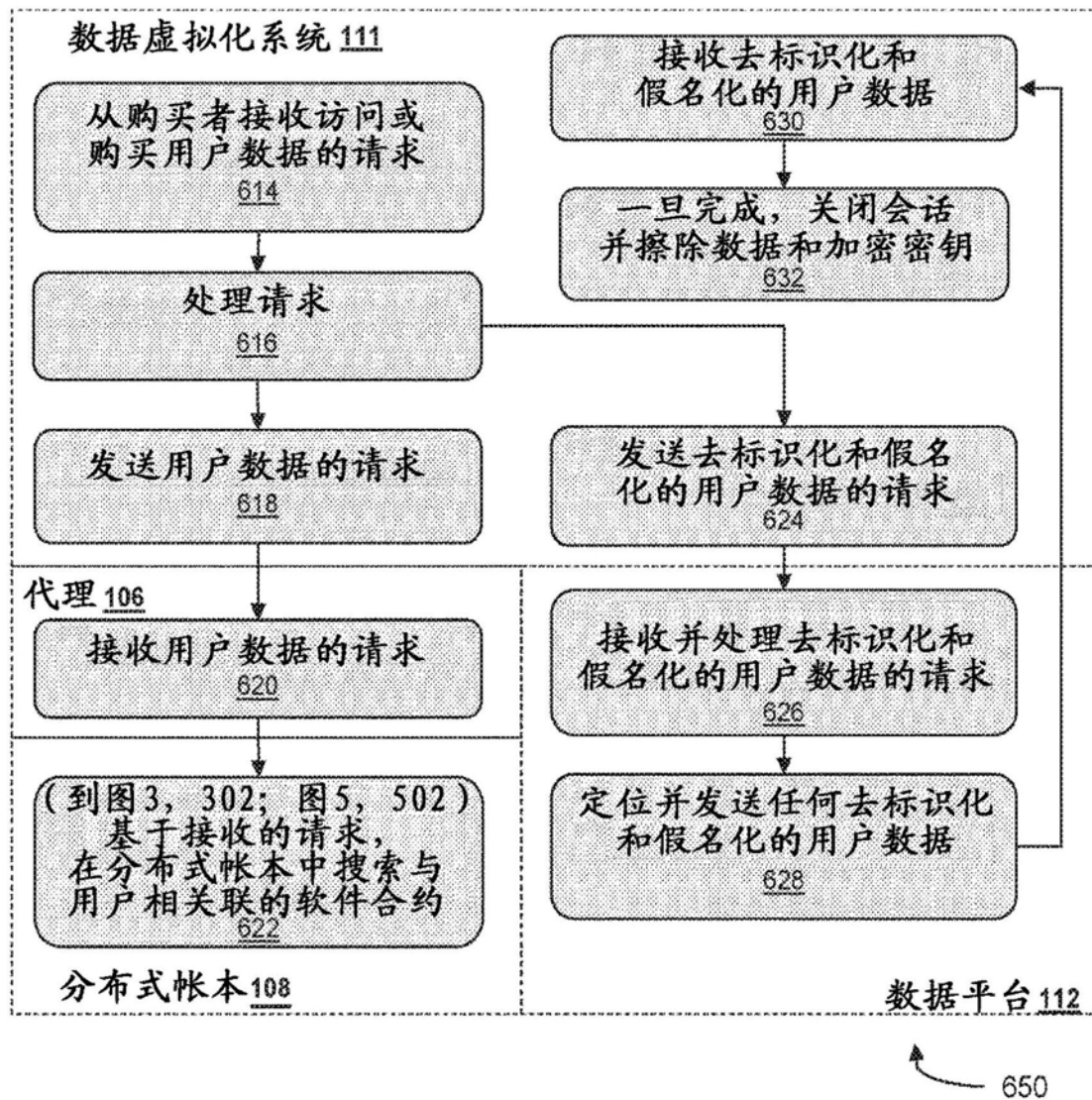


图6B

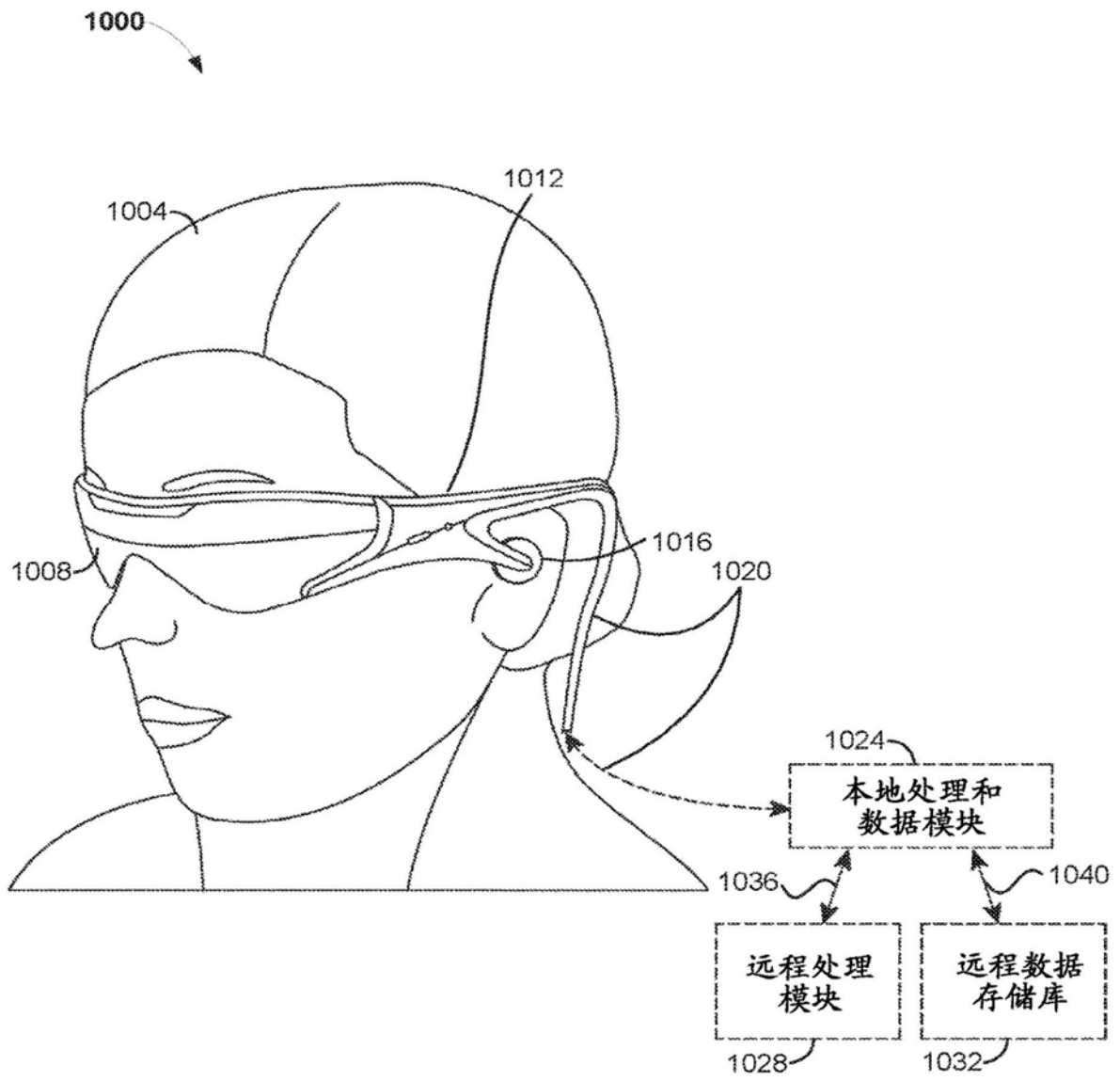


图7A

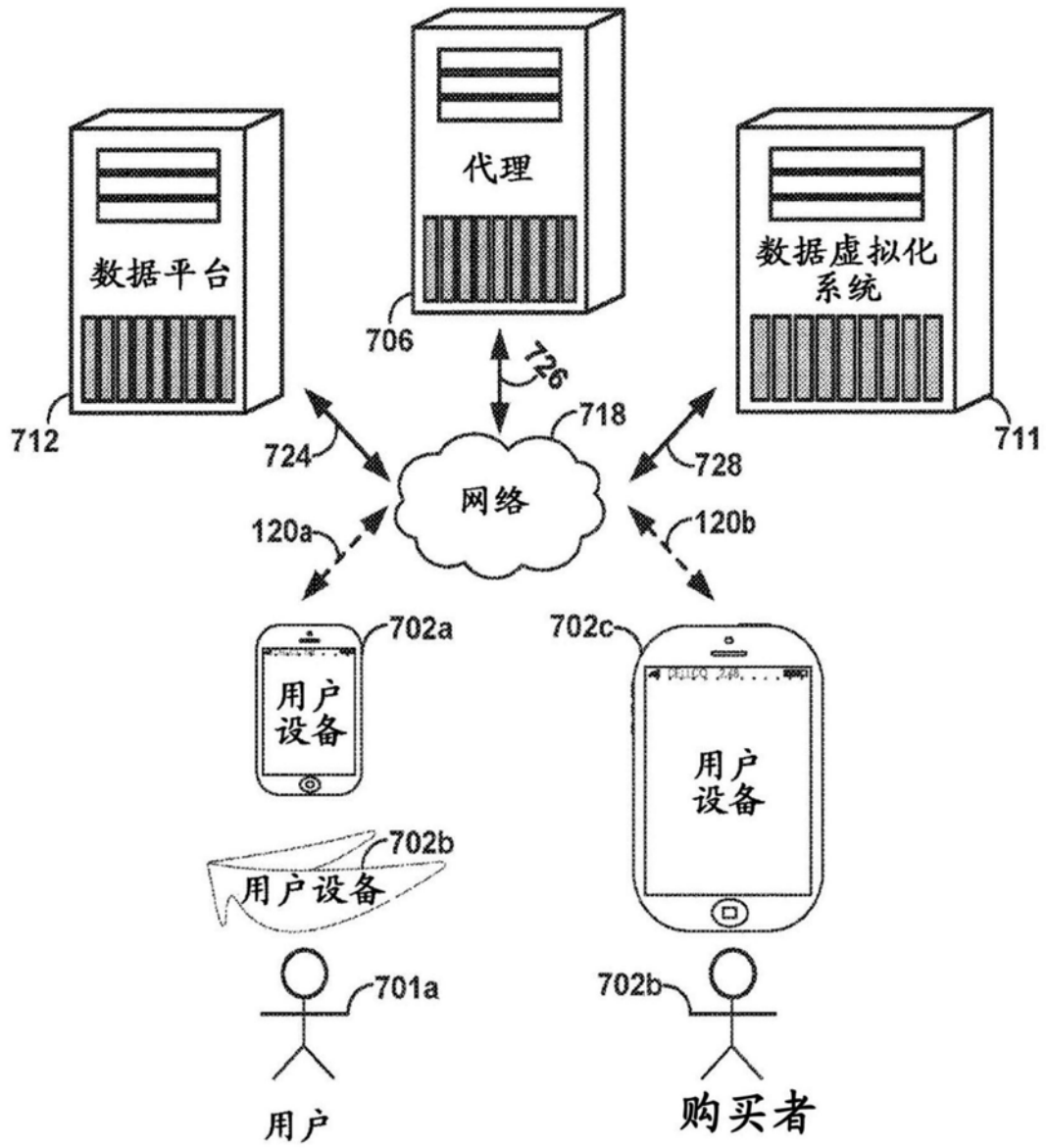


图7B

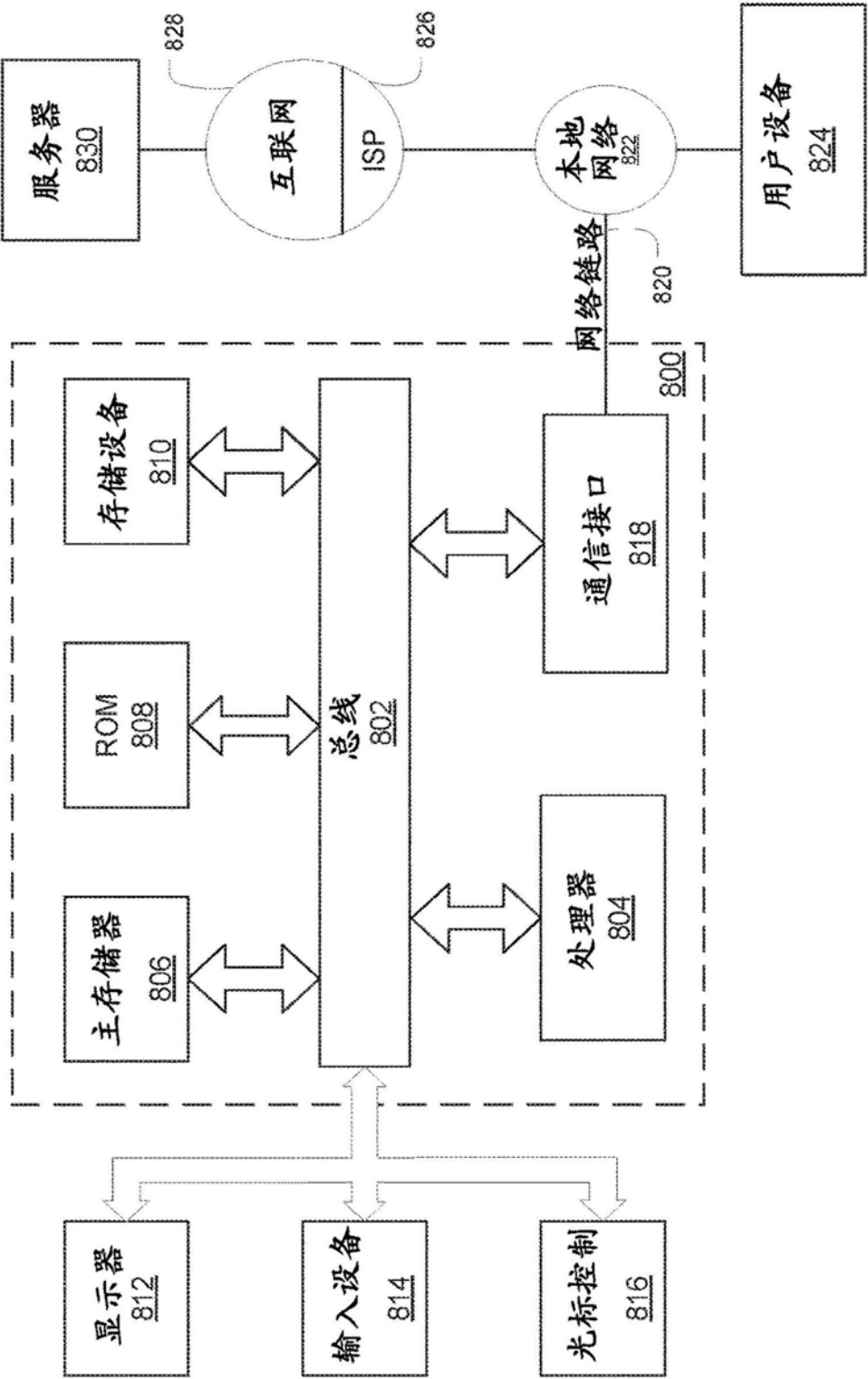


图8