



(12)发明专利

(10)授权公告号 CN 104903909 B

(45)授权公告日 2018.07.31

(21)申请号 201480004221.4

(22)申请日 2014.03.14

(65)同一申请的已公布的文献号

申请公布号 CN 104903909 A

(43)申请公布日 2015.09.09

(30)优先权数据

13/841,498 2013.03.15 US

14/213,244 2014.03.14 US

(85)PCT国际申请进入国家阶段日

2015.07.08

(86)PCT国际申请的申请数据

PCT/US2014/029680 2014.03.14

(87)PCT国际申请的公布数据

W02014/145039 EN 2014.09.18

(73)专利权人 甲骨文国际公司

地址 美国加利福尼亚

(72)发明人 J·J·A·伯耶尔

A·K·阿哈梅德 T·彻芬尔德

V·普拉布胡 R·特瓦瑞

(74)专利代理机构 中国国际贸易促进委员会专

利商标事务所 11038

代理人 边海梅

(51)Int.Cl.

G06F 21/60(2006.01)

(56)对比文件

EP 1577736 A3,2006.12.27,

US 8261320 B1,2012.09.04,

US 2002169954 A1,2002.11.14,

US 2008289019 A1,2008.11.20,

CN 1163805 C,2004.08.25,

CN 1320232 A,2001.10.31,

US 6317868 B1,2001.11.13,

审查员 宋鹏飞

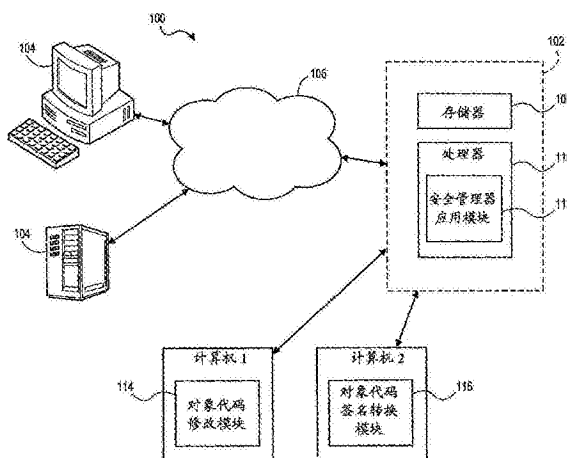
权利要求书3页 说明书19页 附图17页

(54)发明名称

在应用之间计算机内受保护的通信的方法及设备

(57)摘要

公开了用于提供安全服务的系统、方法和机器可读介质。所述方法包括接收应用对象代码的修改,以允许软件应用发送对安全服务的请求;从存储器检索对应于软件应用的修改后的应用对象代码;经由处理器从修改后的应用对象代码接收对安全服务的请求;并且经由处理器提供安全服务。公开了根据所述方法执行操作的系统和机器可读介质。



1. 一种用于从计算设备上的源应用向目的地应用安全地传送数据对象的方法,该方法包括:

在计算设备上提供源应用和目的地应用,源应用和目的地应用每个都具有原始的编译之后的对象代码;

利用与存储器操作上耦合的至少一个处理器,修改源应用的原始的对象代码,以创建用于源应用的第一替换对象代码;

利用与存储器操作上耦合的至少一个处理器,修改目的地应用的原始的对象代码,以创建用于目的地应用的第二替换对象代码;

从源应用向目的地应用传送利用对象数据保护密钥加密的数据对象;

从源应用的第一替换对象代码向计算设备上的安全管理器应用请求与源应用关联的源应用密钥;

使用来自所述安全管理器应用的数据保护根密钥解密所述源应用密钥;

由源应用的第一替换对象代码利用解密的源应用密钥解密对象数据保护密钥;

由源应用的第一替换对象代码利用数据共享密钥或目的地应用密钥加密对象数据保护密钥,目的地应用密钥与目的地应用关联;

与目的地应用共享利用数据共享密钥或目的地应用密钥加密的对象数据保护密钥;

在目的地应用的第二替换对象代码中,解密利用数据共享密钥或目的地应用密钥加密的对象数据保护密钥;以及

在目的地应用的第二替换对象代码中,利用未加密的对象数据保护密钥解密数据对象。

2. 如权利要求1所述的方法,其中共享包括向目的地应用传送利用数据共享密钥或目的地应用密钥加密的对象数据保护密钥。

3. 如权利要求1所述的方法,还包括:

由安全管理器应用确定源应用和目的地应用之间数据对象的传送是否是受限的。

4. 如权利要求1所述的方法,还包括:

由中央安全应用验证源应用或目的地应用的签名。

5. 如权利要求4所述的方法,其中签名是公钥基础设施(PKI)的产物。

6. 如权利要求1所述的方法,还包括:

由安全管理器应用生成源应用密钥、目的地应用密钥和数据共享密钥当中的至少一个。

7. 如权利要求6所述的方法,还包括:

在源应用向安全管理器应用注册时生成源应用密钥;或者

在目的地应用向安全管理器应用注册时生成目的地应用密钥。

8. 如权利要求6所述的方法,还包括:

提示用户密码;及

利用该密码生成源应用密钥或目的地应用密钥。

9. 如权利要求6所述的方法,还包括:

在源应用请求时由安全管理器应用生成数据共享密钥。

10. 如权利要求1所述的方法,还包括:

由目的地应用的第二替换对象代码利用目的地应用密钥加密对象数据保护密钥。

11. 如权利要求1所述的方法,其中计算设备是移动设备。

12. 如权利要求1所述的方法,还包括:

针对所述源应用检索来自远程服务器的策略,所述策略指定所述加密。

13. 如权利要求12所述的方法,其中所述策略指定所述源应用无消息传送、无聊天或者无打印。

14. 如权利要求1所述的方法,其中所述源应用的原始的对象代码选自包括以下的组:
.dylib文件、.so文件和.dll文件。

15. 一种用于从计算设备上的源应用向目的地应用安全地传送数据对象的设备,所述设备包括:

用于在计算设备上提供源应用和目的地应用的装置,源应用和目的地应用每个都具有原始的编译之后的对象代码;

用于利用与存储器操作上耦合的至少一个处理器修改源应用的原始的对象代码以创建用于源应用的第一替换对象代码的装置;

用于利用与存储器操作上耦合的至少一个处理器修改目的地应用的原始的对象代码以创建用于目的地应用的第二替换对象代码的装置;

用于从源应用向目的地应用传送利用对象数据保护密钥加密的数据对象的装置;

用于从源应用的第一替换对象代码向所述计算设备上的安全管理器应用请求与源应用关联的源应用密钥的装置;

用于使用来自所述安全管理器应用的数据保护根密钥解密所述源应用密钥的装置;

用于由源应用的第一替换对象代码利用解密的源应用密钥解密对象数据保护密钥的装置;

用于由源应用的第一替换对象代码利用数据共享密钥或目的地应用密钥加密对象数据保护密钥的装置,目的地应用密钥与目的地应用关联;

用于与目的地应用共享利用数据共享密钥或目的地应用密钥加密的对象数据保护密钥的装置;

用于在目的地应用的第二替换对象代码中,解密利用数据共享密钥或目的地应用密钥加密的对象数据保护密钥的装置;以及

用于在目的地应用的第二替换对象代码中,利用未加密的对象数据保护密钥解密数据对象的装置。

16. 如权利要求15所述的设备,其中共享包括向目的地应用传送利用数据共享密钥或目的地应用密钥加密的对象数据保护密钥。

17. 如权利要求15所述的设备,还包括:

用于由安全管理器应用确定源应用和目的地应用之间数据对象的传送是否受限的装置。

18. 如权利要求15所述的设备,还包括:

用于由中央安全应用验证源应用或目的地应用的签名的装置。

19. 如权利要求18所述的设备,其中签名是公钥基础设施(PKI)的产物。

20. 如权利要求15所述的设备,还包括:

用于由安全管理器应用生成源应用密钥、目的地应用密钥和数据共享密钥当中的至少一个的装置。

21. 如权利要求20所述的设备,还包括:

用于在源应用向安全管理器应用注册时生成源应用密钥的装置;或者

用于在目的地应用向安全管理器应用注册时生成目的地应用密钥的装置。

22. 如权利要求20所述的设备,还包括:

用于提示用户密码的装置;及

用于利用该密码生成源应用密钥或目的地应用密钥的装置。

23. 如权利要求20所述的设备,还包括:

用于在源应用请求时由安全管理器应用生成数据共享密钥的装置。

24. 如权利要求15所述的设备,还包括:

用于由目的地应用的第二替换对象代码利用目的地应用密钥加密对象数据保护密钥的装置。

25. 如权利要求15所述的设备,其中计算设备是移动设备。

26. 如权利要求15所述的设备,还包括:

用于针对所述源应用检索来自远程服务器的策略的装置,所述策略指定所述加密。

27. 如权利要求26所述的设备,其中所述策略指定所述源应用无消息传送、无聊天或者无打印。

28. 如权利要求15所述的设备,其中所述源应用的原始的对象代码选自包括以下的组: .dylib文件、.so文件和.dll文件。

在应用之间计算机内受保护的通信的方法及设备

[0001] 对相关申请的交叉引用

[0002] 本申请要求于2014年3月14日提交的美国专利申请No. 14/213,244的权益并且是其继续申请,而申请14/213,244是于2013年3月15日提交的美国专利申请No. 13/841,498的部分继续申请,这两个申请的全部内容通过引用被结合于此,用于所有目的。

技术领域

[0003] 本公开内容一般而言涉及用于提供安全服务的系统、方法和机器可读介质。更具体而言,本公开内容涉及用于向软件应用提供安全服务的系统、方法和机器可读介质,其中,除其它的之外,安全服务还包括认证、授权、审计、单点登录、安全策略实施、密钥管理和分配、安全通信、安全数据存储以及安全数据共享。

发明内容

[0004] 公开了用于提供安全服务的系统、方法和机器可读介质。根据本公开内容的特征,系统包括存储器和处理器。存储器可用于存储多个应用数据,每个应用数据与软件应用关联并且包括应用对象代码。处理器可以包括安全管理器应用模块。安全管理器应用模块可以对经由软件应用的请求作出响应,该请求是来自对象代码修改模块修改的应用对象代码的对安全服务的请求,修改后的应用对象代码促进对安全服务的请求发送到安全管理器应用模块。

[0005] 在一种实施例中,对象代码修改模块可以被用来通过引入动态或静态库、添加加载命令、符号替换、交叉混合(swizzling)和插入(interposing)当中的至少一个来修改应用对象代码。在另一种实施例中,安全管理器应用模块可以生成选自由认证令牌、认证密钥和安全通信信道组成的组当中的安全工件(artifact),安全管理器应用模块响应于接收到对安全服务的请求而把安全工件发送到软件应用。由对象修改模块接收并修改的应用对象代码可以处于未签署形式。

[0006] 根据本公开内容的特征,应用对象代码可以在应用对象代码被对象代码修改模块修改之前被对象代码签名转换模块从已签署形式转换为未签署形式;并且在应用对象代码被对象代码修改模块修改之后从未签署形式转换为已签署形式。在一种实施例中,对象代码修改模块可以在应用对象代码的修改之前把应用对象代码从已签署形式转换为未签署形式,并且可以在应用对象代码的修改之后把应用对象代码从未签署形式转换为已签署形式。

[0007] 在一种实施例中,应用对象代码的修改可以包括修改被软件应用使用的编程接口、类、对象和函数当中的至少一个。应用对象代码的修改可以包括用于确保与安全策略的兼容性的策略引擎的引入。安全策略可以选自由数据泄漏预防与访问控制策略组成的组。

[0008] 根据本公开内容的特征,安全管理器应用模块可以包括用于确保软件应用与安全策略的兼容性的策略引擎。安全管理器应用模块可以把安全策略发送到软件应用,用于执行。安全策略可以应用到软件应用的一部分、单个软件应用以及多个软件应用当中的至少

一个。在一种实施例中,策略引擎是动态策略引擎,安全策略基于选自由执行上下文、外部事件、明确的策略重定义以及改变组和角色成员资格组成的组当中的至少一个。在另一种实施例中,安全策略是从远程策略服务器检索的。在还有另一种实施例中,第一软件应用从远程策略服务器检索安全策略,并且第二软件应用从第一软件应用检索安全策略。从策略引擎的执行得到的数据可以发送到安全管理器应用模块和/或策略服务器。

[0009] 根据本公开内容的特征,响应于经由软件应用的对安全服务的请求,如果软件应用利用公钥基础设施(PKI)密钥签署,则安全管理器应用模块可以促进安全服务。安全管理器应用模块可以确认软件应用以及关联的计算平台还没有被危及,并且可以验证软件应用的签名。在一种实施例中,多个应用数据包括公共密钥。在另一种实施例中,安全管理器应用模块可以对来自软件应用的注册请求作出响应,以建立应用信任。安全管理器应用模块可以提示用户输入应用注册密码,并且利用应用注册密码生成建立应用信任的密钥,以促进由安全管理器应用模块向软件应用提供的安全服务。

[0010] 在另一种实施例中,安全管理器应用模块可以向软件应用提供密钥,以允许软件应用向安全管理器应用模块发送对安全服务的请求。应用数据可以包括由软件应用或安全管理器应用模块生成的应用数据保护密钥。应用数据保护密钥可以被利用安全管理器应用模块维护的对应的数据保护根密钥加密和解密。在一种实施例中,应用数据保护密钥可以执行加密对象数据保护密钥和解密对象数据保护密钥当中的至少一个,以促进数据对象从第一软件应用到第二软件应用的传送。安全管理器应用模块可以在从第一软件应用向第二软件应用传送数据对象和对象数据保护密钥之前生成用于加密对象数据保护密钥的数据共享密钥。数据共享密钥还可以用于在从第一软件应用向第二软件应用传送数据对象和对象数据保护密钥之后用于解密对象数据保护密钥。根据本公开内容的实施例,安全管理器应用模块和第一软件应用当中的至少一个还可以利用第一软件应用的应用数据保护密钥解密用于数据对象的对象数据保护密钥,并且利用第二软件应用的应用数据保护密钥加密用于数据对象的对象数据保护密钥。

[0011] 根据本公开内容的特征,提供了用于提供安全服务的计算机实现的方法。该方法可以在与具有多个应用数据的存储器通信的处理器上实现,每个应用数据与软件应用关联并且包括应用对象代码。该方法可以包括从存储器检索对应于软件应用的应用对象代码,并且接收应用对象代码的修改,以允许软件应用发送对安全服务的请求,修改包括引入动态或静态库、添加加载命令、符号替换、交叉混合和插入当中的至少一个。该方法还可以包括经由处理器接收对安全服务的请求,并且经由处理器提供安全服务。

[0012] 在一种实施例中,应用对象代码在修改之前从已签署形式转换为未签署形式,并且在修改之后从未签署形式转换为已签署形式。应用对象代码的修改可以包括引入用于确保与安全策略兼容性的策略引擎。安全策略可以应用到软件应用的一部分、单个软件应用以及多个软件应用当中的至少一个。安全策略可以选自由数据泄漏预防策略和访问控制策略组成的组。在一种实施例中,策略引擎是动态策略引擎,安全策略是基于选自由执行上下文、外部事件、明确的策略重定义以及改变组和角色成员资格组成的组当中的至少一个因素的。

[0013] 在一种实施例中,计算机实现的方法包括经由处理器确认软件应用和关联的计算平台还没有被危及,并且经由处理器验证软件应用的 PKI 密钥签名。而且,该计算机实现的

方法可以包括从软件应用接收注册请求,以便在接收对安全服务的请求之前建立应用信任,并且经由处理器提示用户输入应用注册密码。该方法还可以包括经由处理器生成密钥,以便利用应用注册密码建立应用信任,并且经由处理器向软件应用提供密钥,以允许软件应用发送对安全服务的请求。

[0014] 根据本公开内容的特征,计算机实现的方法可以包括由处理器生成应用数据保护密钥、从存储器检索对应的数据保护根密钥,并且经由处理器利用对应的数据保护根密钥加密应用数据保护密钥。在一种实施例中,该计算机实现的方法可以包括经由处理器利用第一软件应用的应用数据保护密钥解密用于数据对象的对象数据保护密钥;经由处理器生成数据共享密钥,用于加密对象数据保护密钥和解密对象数据保护密钥当中的至少一个;经由处理器利用数据共享密钥加密对象数据保护密钥;从第一软件应用向第二软件应用传送数据对象和加密的对象数据保护密钥;经由处理器利用数据共享密钥解密对象数据保护密钥;并且经由处理器利用第二软件应用的应用数据保护密钥加密用于数据对象的对象数据保护密钥。

[0015] 根据本公开内容的特征,提供了机器可读介质。机器可读介质可以提供指令,指令在被具有处理器和存储器的机器读取时,使机器根据本公开内容的方法执行操作。

[0016] 一些实施例涉及从中央应用向计算设备上的另一应用提供安全服务。该方法包括提供配置为在计算设备上提供安全服务的第一应用、在计算设备上提供第二应用,第二应用具有原始的编译之后的对象代码,利用与存储器操作上耦合的至少一个处理器修改第二应用的原始的对象代码,以创建替换对象代码,该替换对象代码配置为与第一应用通信、调用第二应用中的替换对象代码并且利用第二应用中的替换对象代码从第一应用请求安全服务。

[0017] 原始的对象代码可以通过选自由引入动态库、引入静态库、引入附加的加载命令、符号替换、指针交叉混合和插入组成的组当中的至少一种技术修改。该方法可以包括由第一应用生成选自由认证令牌、密钥、安全凭证、单点登录令牌、标识符、安全策略、安全命令、安全配置、会话句柄、会话令牌和安全通信信道组成的组当中的安全工件,并且响应于对安全服务的请求而把安全工件从第一应用发送到第二应用。原始的对象代码可以包括未签署代码。该方法还可以包括在修改之前把原始的对象代码从已签署形式转换为未签署形式,并且在修改之后把替换对象代码从未签署形式转换为已签署形式。计算设备可以是移动设备。

[0018] 修改可以包括修改编程接口、类、对象和函数当中的至少一个。第二应用的原始的对象代码的修改可以包括引入用于确保与安全策略的兼容性的策略引擎。安全策略可以选自由数据泄漏预防策略和访问控制策略组成的组。第一应用可以包括用于确保第二应用与安全策略的兼容性的策略引擎,第一应用向第二应用发送安全策略,用于执行。安全策略可以应用到以下当中的至少一个:第二应用的一部分、单个软件应用以及多个软件应用。安全策略可以基于选自由执行上下文、外部事件、明确的策略重定义以及改变组和角色成员资格组成的组当中的至少一个因素。安全策略是从远离计算设备的服务器检索的。

[0019] 该方法还可以包括通过修改第三应用的对象代码把策略引擎从第二应用引入到第三应用中。得自替换对象代码执行的数据可以被发送到第一应用或远程服务器。响应于对安全服务的请求,如果软件应用用公钥基础设施(PKI)密钥签署,则第一应用可以促进安

全服务。该方法还可以包括由第一应用确认第二应用和计算设备还没有被危及,并且验证第一应用的签名。安全服务可以向第二应用和第三应用提供公共密钥。第一应用可以响应于来自第二应用的注册请求而建立应用信任,该第一应用提示用户输入应用注册密码,并且利用应用注册密码生成建立应用信任的密钥,以促进由第一应用向第二应用提供安全服务。第一应用可以向第二应用提供密钥,以允许第二应用发送对安全服务的请求。

[0020] 该方法还可以包括生成应用数据保护密钥,该应用数据保护密钥是由利用第一应用维护的对应数据保护根密钥加密和解密的。应用数据保护密钥可以执行加密对象数据保护密钥和解密对象数据保护密钥当中的至少一个,以促进数据对象从第一软件应用到第二软件应用的传送。该方法还可以包括在从第一软件应用向第二软件应用传送数据对象和对象数据保护密钥之前生成用于加密对象数据保护密钥的数据共享密钥,并且在第一软件应用向第二软件应用传送数据对象和对象数据保护密钥之后生成用于解密对象数据保护密钥的数据共享密钥。安全管理器应用模块和第一软件应用当中的至少一个可以利用第一软件应用的应用数据保护密钥解密用于数据对象的对象数据保护密钥,并且利用第二软件应用的应用数据保护密钥加密用于数据对象的对象数据保护密钥。

[0021] 一些实施例涉及用于动态更新软件应用的安全策略的方法。该方法包括在计算设备上提供具有原始的编译之后的对象代码的应用,利用与存储器操作上耦合的至少一个处理器修改应用的原始的对象代码,以创建替换对象代码,替换对象代码被配置为用于实施安全策略,检索第一安全策略,利用替换对象代码实施安全策略,利用第二安全策略替换第一安全策略,然后利用替换对象代码实施第二安全策略,其中第一和第二安全策略是基于选自由执行上下文、外部事件、明确的策略重定义以及改变组和角色成员资格组成的组当中的至少一个因素的。

[0022] 第一或第二安全策略可以从远离计算设备的服务器检索。第一应用可以从远程服务器检索第一或第二安全策略,并且第二应用从第一应用检索第一或第二安全策略。得自替换对象代码执行的数据可以发送到远程服务器。计算设备可以是移动设备。

[0023] 一些实施例涉及用于在计算设备上的应用之间建立信任的方法。该方法包括在计算设备上提供软件应用,每个应用具有原始的编译之后的对象代码,利用与存储器操作上耦合的至少一个处理器修改每个应用的原始的对象代码,以创建用于每个应用的替换对象代码,替换对象代码被配置为访问应用之间的共享秘密,由此在应用之间建立信任关系。

[0024] 该方法还可以包括在修改之前把每个软件应用的原始的对象代码从已签署形式转换为未签署形式,并且在修改之后把每个软件应用的替换对象代码从未签署形式转换为已签署形式。该方法还可以包括在计算设备上提供安全管理器应用,其中用于每个应用的替换对象代码被修改,以便与安全管理器应用通信,由每个软件应用的替换对象代码从安全管理器应用获得共享秘密。该方法还可以包括在允许第一应用的替换对象代码访问共享秘密之前由安全管理器应用验证软件应用的第一应用的签名。签名可以是公共密钥基础设施(PKI)密钥的产物。

[0025] 该方法还可以包括在安全管理器应用处,从软件应用的第一应用接收注册请求,在第一应用注册时由安全管理器应用提示用户密码,利用密码生成密钥,该密钥是共享秘密,并且把该密钥提供给第一应用。该方法还可以包括由安全管理器应用生成应用数据保护密钥,由安全管理器应用检索对应的数据保护根密钥,并且由安全管理器应用利用对应

的数据保护根密钥加密应用数据保护密钥。

[0026] 一些实施例涉及用于把数据对象从计算设备上的源应用安全地传送到目的地应用的方法。该方法包括在计算设备上提供源应用和目的地应用,源应用和目的地应用当中每一个都具有原始的编译之后的对象代码,利用与存储器操作上耦合的至少一个处理器修改源应用的原始的对象代码,以便为源应用创建第一替换对象代码,利用与存储器操作上耦合的至少一个处理器修改目的地应用的原始的对象代码,以创建用于目的地应用的第二替换对象代码,从源应用向目的地应用传送利用对象数据保护密钥加密的数据对象,由源应用的第一替换代码检索与源应用关联的源应用密钥,利用检索出的源应用密钥由源应用的第一替换代码解密对象数据保护密钥,利用数据共享密钥或目的地应用密钥由源应用的第一替换代码加密对象数据保护密钥,目的地应用密钥与目的地应用关联,与目的地应用共享利用数据共享密钥或目的地应用密钥加密的对象数据保护密钥,在目的地应用的第二替换代码中解密利用数据共享密钥或目的地应用密钥加密的对象数据保护密钥,在目的地应用的第二替换代码中利用未加密的对象数据保护密钥解密对象数据。

[0027] 该方法可以包括向目的地应用传送利用数据共享密钥或目的地应用密钥加密的对象数据保护密钥。检索可以使用计算设备上的安全管理器应用。该方法还可以包括由安全管理器应用确定源应用和目的地应用之间数据对象的传送是否是受限的,并且基于该确定促进检索。该方法还可以包括在促进检索之前由中央安全应用验证源应用或目的地应用的签名。签名可以是公钥基础设施 (PKI) 密钥的产物。检索可以包括利用解密加密的安全应用密钥的请求从安全应用向安全管理器应用发送加密的安全应用密钥,并且利用数据保护根密钥由安全管理器应用解密安全应用密钥,然后从安全管理器应用向源应用传送源应用密钥。检索可以包括从源应用向安全管理器应用发送对源应用密钥的请求,利用数据保护密钥由安全管理器应用解密源应用密钥,然后从安全管理器应用向源应用传送源应用密钥。检索可以包括从源应用向安全管理器应用请求数据保护根密钥,由源应用接收数据保护根密钥,并且由源应用利用数据保护根密钥解密源应用密钥。

[0028] 该方法还可以包括由安全管理器应用生成源应用密钥、目的地应用密钥和数据共享密钥当中的至少一个。该方法还可以包括在向安全管理器应用注册源应用时生成源应用密钥,或者在向安全管理器应用注册目的地应用时生成目的地应用密钥。该方法还可以包括提示用户密码,并且利用该密码生成源应用密钥或目的地应用密钥。该方法还可以包括在源应用请求时由安全管理器应用生成数据共享密钥。该方法还可以包括由目的地应用的第二替换代码利用目的地应用密钥加密对象数据保护密钥。计算设备可以是移动设备。

[0029] 根据本公开内容的特征,提供了机器可读介质。机器可读介质可以提供指令,当指令被具有处理器和存储器的机器读取时,使机器根据本公开内容的方法执行操作。

[0030] 实施例可以包括计算机软件,当计算机软件被计算机执行时,使计算机执行所述方法。

附图说明

[0031] 结合附图参考以下描述,以上提到的本公开内容的特征和对象将变得更加显然,其中相同的标号指示相同的元素,并且其中:

[0032] 图1根据本公开内容的实施例说明了用于提供安全服务的系统的框图。

[0033] 图2根据本公开内容的实施例说明了用于向驻留在相同平台上的其它软件应用提供集中式安全服务的集中式安全管理器应用模块的框图。

[0034] 图3根据本公开内容的实施例说明了对象代码修改的示例性框图。

[0035] 图4是根据本公开内容的实施例说明了安全管理器应用向其它软件应用发送安全工件的示例性框图。

[0036] 图5是根据本公开内容的实施例说明通过修改现有应用对象代码来修改软件应用的行为的方法的示例性框图。

[0037] 图6-图11根据本公开内容的实施例说明了用于通过在对象代码中注入策略引擎来修改软件应用的行为的方法的示例性框图。

[0038] 图12是根据本公开内容的实施例说明了利用安全管理器应用模块在软件应用之间建立信任的方法的示例性框图。

[0039] 图13是根据本公开内容的实施例说明与具有公共密钥的软件应用通信的安全管理器应用模块的示例性框图。

[0040] 图14是根据本公开内容的实施例说明了软件应用的密码注册以便建立与安全管理器应用模块的信任的示例性框图。

[0041] 图15是根据本公开内容的实施例说明了使用应用数据保护密钥来维护软件应用中的安全性的示例性框图。

[0042] 图16是根据本公开内容的实施例说明了用于从源(第一)应用向目的地(第二)应用安全地传送数据对象的方法的示例性框图。

[0043] 图17是根据本公开内容的实施例说明了用于从源(第一)应用向目的地(第二)应用安全地传送数据对象的另一方法的示例性框图。

具体实施方式

[0044] 以下详细描述包括单独地并且组合地利用了各种特征和教导的代表性例子,并且参考附图更详细地描述各种实施例。该详细描述仅仅是要向本领域技术人员教导用于实践本教导优选方面的更多细节,而不是要限定权利要求的范围。因此,以下详细描述中所公开的特征的组合对于实践所述教导不一定是必需的,而是仅仅要描述本教导的特定代表性示例。

[0045] 以下详细描述的一些部分是按照在计算机存储器中执行的算法和操作序列给出的。这些算法描述和表示是由数据处理领域中技术人员所使用的工具,以便最有效地把其工作的实质传达给本领域其他技术人员。算法或操作序列在这里并且一般而言被设想为是导致期望结果的步骤的自相一致序列。步骤是需要物理量的物理操纵的步骤。通常,虽然不是必需,但这些量采取能够被存储、传送、组合、比较和以别的方式被操纵的电或磁信号的形式。

[0046] 但是,应当牢记,所有这些和相似的术语应当与适当的物理量关联并且仅仅是适用于这些量的方便标记。除非以与从以下讨论显然的不同方式具体陈述,否则应当认识到,贯穿本描述,利用诸如“处理”或“计算”或“运算”或“确定”或“显示”等术语的讨论指把计算机系统寄存器和存储器中表示为物理(电子)量的数据操纵和变换为电子设备存储器或寄存器或其它此类信息存储、传输或显示设备中类似地表示为物理量的其它数据的计算机系

统或类似的电子设备的动作或过程。

[0047] 这里给出的方法不固地关联到任何特定的电子设备或其它装置。各种通用系统可以与根据本文教导的程序一起使用,或者它可以证明构造执行所需方法步骤的更专业装置的方便性。用于各种这些系统的所需结构将从以下描述显现。应当认识到,各种编程语言可以被用来实现如本文所述的实施例的教导。

[0048] 本专利文档描述用于向包括移动设备在内的设备上的软件应用提供安全服务的独特系统、方法和机器可读介质。除其它的之外,这些安全服务还可以包括认证、授权、审计、单点登录、安全策略实施、密钥管理和分配、安全通信、安全数据存储和安全数据共享。就这一点而言,在本文讨论各种协议和标准并且这些协议和标准能结合所讨论的实施例使用。虽然本文描述的实施例可以结合任何协议或标准使用,但是以下协议和标准的全部内容通过引用被结合于此: IETF RFC 2631 (Diffie-Hellman); IEEE 1363; IETF RFC 3280 (X.509 Public Key Infrastructure); IETF RFC 4120 (Kerberos V5); IETF RFC 4178 (SPNEGO); IETF RFC 2616 (HTTP 1.1); IETF RFC 4559; IETF RFC 4556 (PKINIT for Kerberos); IETF RFC 6101/2246/5246 (SSL/TLS); SAML V1.0/1.1/2.0; OpenID; OAuth; WS-Federation 和 OATH HOTP/TOTP/OCRA。

[0049] 通过修改计算机应用的对象代码的用于计算机应用的安全服务管理

[0050] 本领域中存在一个问题就是,一旦计算设备被恶意软件感染,在计算机上执行的几乎任何应用就可以通过偷看其持久性存储器或拦截它与其它应用之间的通信而被探听。一些应用被编程为通过加密它们发送的一切、保存到盘等等来最小化这个问题,但是这需要这些特征在它们最初编程的源代码,以及它们与其通信或共享文件的每个其它应用中。一些实施例包括修改安装在计算设备上的应用的原始的编译之后的对象代码,以便添加加密和解密、删除对不安全网络的调用、从安全管理器应用请求加密密钥,等等。例如,以明文保存电子邮件的电子邮件客户端应用的 .dylib 文件可以用通过利用加密保存电子邮件的另一个 .dylib 文件转变 (switch out)。在另一个例子中,业务智能应用的符号表可以被更改,使得它可以调用与其原始不同的对象文件,该不同的对象文件阻止公司防火墙之外的电子邮件消息。在还有另一个例子中,策略引擎可以拷贝到新对象代码中并且对可被更新的策略执行。

[0051] 在一种实施例中,利用安全管理器应用提供了用于移动设备的集中式安全服务体系架构。本公开内容的一个特征包括,通过编译之后的对象代码修改,集中式安全管理器应用和其它应用与由安全管理器应用提供的服务的集成的组合。

[0052] 图1根据本公开内容的实施例说明了用于提供安全服务的系统 100 的框图。系统 100 可以包括可以经网络 106 访问远程设备 104 的计算设备 102。

[0053] 在一种实施例中,计算设备 102 可以包括存储器 108 和处理器 110。存储器 108 可以用于存储多个应用数据,每个应用数据与软件应用关联并且包括应用对象代码。

[0054] 如可以认识到的,存储器 108 可被用来,例如,响应于终端用户动作而存储和/或检索数据。如众所周知的,存储器可以包括可被划分或交叉相关的数据库类别,并且数据库等的任意组合可以从服务器中提供。在一种实施例中,数据库的任何部分都可以经网络 106 远程提供。来自外部数据库的外部数据可以以设备 102 能够理解的任何标准化的形式提供。例如,位于提供商处的外部数据库可以响应于来自服务器的请求而以标准格式有利地提供终

端用户数据,例如,名称、用户标识和计算机标识号,等等,并且终端用户数据块被变换成代码模块可以理解的函数调用格式。

[0055] 如可以认识到的,存储器108可以是诸如机器可读介质的存储设备,机器可读介质可以是以处理器可读的形式提供(即,存储和/或发送)信息的任何机制。例如,机器可读介质可以是只读存储器 (ROM)、随机存取存储器 (RAM)、高速缓存、硬盘驱动器、软盘驱动器、磁盘存储介质、光学存储介质、闪存存储器设备或者能够存储信息的任何其它设备。此外,机器可读介质还可以包括计算机存储介质和通信介质。机器可读介质包括以用于信息存储的任何方法或技术实现的易失性和非易失性、可移除和不可移除介质,诸如计算机可读指令、数据结构、程序模块或其它数据。机器可读介质还包括但不限于RAM、ROM、EPROM、EEPROM、闪存存储器或者其它固态存储器技术、CD-ROM、DVD或者其它光学存储器、磁带盒、磁带、磁盘存储或其它磁性存储设备,或者可以用来存储期望信息并且可被计算机访问的任何其它介质。

[0056] 计算设备102还可以包括一个或多个电和/或物理耦合到处理器 110的功能模块,包括安全管理器应用模块112。如本文所使用的,术语“模块”指体现在硬件和/或固件中的逻辑,或者指以诸如像 C++的编程语言书写的软件指令的集合,有可能具有入口和出口点。软件模块可以被编译和链接成可执行程序,或安装在动态链接库中,或者可以以诸如BASIC的解释性语言书写。应当认识到,软件模块可以从其它模块调用,和/或可以响应于检测到的事件或中断而被调用。软件指令可以嵌入在诸如EPROM的固件中。还将认识到,硬件模块可以由连接的逻辑单元组成,诸如门和触发器,和/或可以由诸如可编程门阵列的可编程单元组成。本文所描述的模块优选地实现为软件模块,但可以在硬件和/或固件中表示。

[0057] 在一种实施例中,每个模块都作为模块化代码对象提供,其中代码对象通常通过一组标准化的函数调用交互。在一种实施例中,代码对象是以诸如C++的合适软件语言书写的,但是代码对象可以以任何低级或高级语言书写。在一种实施例中,代码模块用C++实现并且在运行在Windows平台、iOS平台、Android平台等等上的计算机上编译。本领域技术人员将认识到,任何数量的实现,包括直接对硬件的代码实现,也是可能的。

[0058] 安全管理器应用模块112可以操作上耦合到由对象代码修改模块 114和/或对象代码签名转换模块116修改的应用对象代码。安全管理器应用模块112可以对经由软件应用对安全服务(例如网络106上的安全通信)的请求作出响应。对象代码修改模块114和/或对象代码签名转换模块116可以修改应用对象代码,以促进对安全服务的请求向安全管理器应用模块112的发送。用于每个应用数据的修改后的应用对象代码可以存储在存储器108中。

[0059] 图2根据本公开内容的实施例说明了用于向驻留在相同平台上的其它软件应用118-122提供集中式安全服务117的集中式安全管理器应用模块112的框图。如可以认识到的,其它软件应用118-122可以通过修改现有的应用对象代码124-128,而不是通过修改其它软件应用118-122中的源代码,来链接到集中式安全服务117。在一种实施例中,除其它已知的对象代码修改技术之外,对象代码修改124-128 还可以涉及注入动态或静态库、添加加载命令、符号替换、交叉混合和插入。本领域技术人员将认识到,术语“修改”可以包括添加、替换和/或删除。图3根据本公开内容的实施例说明了对象代码修改的示例性框图。

[0060] 在一种实施例中,诸如认证令牌、密钥、凭证、单点登录令牌、标识符、安全策略、安

全命令、安全配置、会话句柄、会话令牌和安全通信信道的安全工件可以由安全管理器应用模块112生成并且按需分配给其它软件应用118-122。图4是根据本公开内容的实施例说明了安全管理器应用模块112向其它软件应用118-122发送安全工件 130-134的示例性框图。

[0061] 如可以认识到的,安全管理器应用模块112可以是具体地为那个目的建立的特定软件应用(例如,安全容器应用)。在另一种实施例中,安全管理器应用模块112可以是修改后的移动应用,例如,在给定设备上安装或启动的第一应用,其中安全管理器功能是上述对象代码修改的一部分。在一种实施例中,具有专用目的的安全管理器应用模块的系统可能是优选的,以最小化代码和功能跨多个应用的重复,但这不是必需的。

[0062] 本领域技术人员将认识到,存在修改对象代码的几种方法。在一种实施例中,对象代码修改124-128的阶段可以在软件应用118-122 执行时被动态执行。这可以允许对象代码修改124-128和所得到的应用行为修改基于在那个执行的具体上下文时可用的数据来确定。

[0063] 图5是根据本公开内容的实施例说明了通过修改现有应用对象代码来修改软件应用118-122的行为的方法的示例性框图。修改过程可以在两个阶段中执行。对象代码修改过程的第一阶段可以在软件应用 118-122安装在它将在其执行的平台上之前执行,导致中间的修改后的应用对象代码130。对象代码修改过程的第二阶段可以在软件应用 118-122安装在它将在其执行的平台上之后执行,导致最终的修改后的应用对象代码131。

[0064] 在一种实施例中,对象代码修改过程的第二阶段可以由中间的修改后的应用对象代码130对它自己执行。在另一种实施例中,对象代码修改过程的第一和第二阶段可以基于配置和/或策略不同地执行。如可以认识到的,对象代码修改过程的第二阶段可以在每次应用开始执行和/或在执行过程中基于各种因素不同地执行,所述因素包括但不限于执行上下文、外部事件、明确的策略重定义、各种计数器以及拥有移动设备的用户的改变组和角色成员资格。在另一种实施例中,对象代码修改过程的第二阶段可以包括从外部源加载一些新对象代码。

[0065] 根据本公开内容的实施例,对象代码修改124-126可以用来以不破坏(break)现有应用功能的方式修改软件应用118-122的行为。这可以通过在原始的未修改的应用代码被平台或操作系统执行之前让修改后的对象代码被平台或操作系统执行来实现。

[0066] 在一种实施例中,提供了通过修改现有应用对象代码(而不通过修改应用源代码)来分析和修改软件应用118-122的行为的方法。该方法可以包括分析未修改的应用对象代码和任何关联的配置信息,以确定它将如何被预期要在其上运行的平台或操作系统执行,以便提取应用执行简档;以不再被平台或操作系统直接使用这样一种方式来修改未修改的应用对象代码和任何关联的配置信息;利用应用执行简档来再现未修改的应用如何在新对象代码中(可选地具有新的关联的配置信息)被平台或操作系统执行;并且组合新对象代码与未修改的应用对象代码,从而导致修改后的应用对象代码124-128。

[0067] 在一种实施例中,修改后的应用对象代码124-128可以包括注入到软件应用118-122中的动态库。如可以认识到的,参考该动态库的新加载命令可以添加到未修改的应用对象代码中存在的现有加载命令列表。

[0068] 如可以认识到的,到对象代码修改过程的输入可以是未签署形式的未修改的移动应用对象代码,而来自对象代码修改过程的输出可以是未签署或已签署形式的修改后的移

动对象代码。在一种实施例中,把已签署形式的未修改的移动应用对象代码转换成未签署形式的未修改的移动应用对象代码的过程可以在对象代码修改过程之前执行。在另一种实施例中,把未签署形式的修改后的移动应用对象代码转换成已签署形式的修改后的移动应用对象代码的过程可以在对象代码修改过程之后执行。在还有另一种实施例中,把未签署形式的中间的修改后的移动应用对象代码转换成已签署形式的中间的修改后的移动应用对象代码的过程可以在之前描述的两阶段对象代码修改过程的第一阶段之后执行。

[0069] 在一种实施例中,图1中所示的对象代码签名转换模块116可以用来在由对象代码修改模块114对应用对象代码修改之前把应用对象代码从已签署形式转换为未签署形式,并且可以用来在由对象代码修改模块114对应用对象代码修改之后把应用对象代码从未签署形式转换为已签署形式。

[0070] 如可以认识到的,已签署形式的未修改的应用对象代码到未签署形式的未修改的应用对象代码的转换和/或未签署形式的修改后的应用对象代码到已签署形式的修改后的应用对象代码的转换可以作为对象代码修改过程的一部分来执行。修改后的对象代码124-128可以包括对应用本身内部的或者该应用使用的现有编程接口、类、对象和/或函数的行为的修改。编程接口、类、对象和/或函数可以由移动设备平台提供。

[0071] 在一种实施例中,该过程可以导致现有编程接口、类、对象和/或函数被阻塞、除去、用备选实现方式替换,和/或部分或全部被修改。在另一种实施例中,该过程会导致新编程功能在现有编程接口、类、对象和/或函数被使用之前和/或之后被执行。在还有另一种实施例中,虽然现有编程接口、类、对象和/或函数仍然在对象代码中存在,但该过程会导致新编程功能代替现有编程接口、类、对象和/或函数被执行。

[0072] 如可以认识到的,对象代码修改124-128可以被组织成模块,其中每个模块实现对象代码修改124-128的一部分,并且在对象代码修改过程中应用到应用的模块集合可以通过配置和/或策略来控制。在对象代码修改过程中应用到软件应用118-122的模块集合可以在前面描述的两阶段对象代码修改过程的第一阶段和/或第二阶段中确定。在对象代码修改过程中应用到软件应用118-122的模块集合还可以由与应用一起交付的配置文件确定。

[0073] 根据本公开内容的实施例,提供了通过修改现有应用对象代码(而不是通过修改应用源代码)来修改软件应用118-122的存储行为的方法。该方法可以包括通过利用现有的插入或交叉混合技术,用新接口或函数替换未修改的应用直接调用用于存储数据的现有编程接口或函数。新编程接口或函数可以用来在数据被写时加密数据和/或在数据被读时解密数据。新编程接口或函数还可以调用现有编程接口或函数。如可以认识到的,现有编程接口或函数可以由移动设备平台提供。现有编程接口或函数可以是POSIX I/O API的一部分。

[0074] 根据本公开内容的一部分,提供了通过修改现有应用对象代码来修改软件应用118-122的通信行为的方法。该方法可以包括利用修改后的应用对象代码暂停来自软件应用118-122的通信请求。修改后的应用对象代码可以用来检查必要的安全工件是否在该通信请求中存在。在一种实施例中,如果必要的安全工件在通信请求中不存在,则修改后的应用对象代码可以检索必要的安全工件。在检索出必要的安全工件之后,修改后的应用对象代码可以把它们添加到通信请求,并且可以允许通信请求继续。如可以认识到的,通信请求可以是网络通信请求。

[0075] 安全工件可以是认证令牌、密钥、凭证、单点登录令牌、标识符、安全策略、安全命

令、安全配置、会话句柄、会话令牌和安全通信信道。安全工件可以从服务器和/或安全管理器应用模块112检索。

[0076] 通过修改计算机应用安全策略的对象代码来修改计算机应用安全策略

[0077] 现有技术中存在一个问题就是,一旦计算机应用安装在计算机上,其安全过程或规则通常就不能改变。一些实施例包括改变应用的对象代码,使得安全策略可以被更新。应用的对象代码可以添加、删除、替换、编辑或以别的方式被修改。例如,如果确定移动设备在国际间行进,则运行在设备上的电子邮件客户端可以从远程服务器下载新策略,其中该客户端使其自己的关于保存和检索数据的原始.dylib(或者.so或者.dll)文件被添加了用于从远程服务器检索安全策略文本文件的步骤的文件替换。新策略可以引入用于跨海行进的新规则,诸如没有消息传送、聊天或打印。作为另一个例子,新策略可以规定由业务智能应用保存或发送的一切的加密。

[0078] 图6-图11根据本公开内容的实施例说明了用于通过在对象代码中注入策略引擎132来修改软件应用118-122的行为的方法的示例性框图。该方法可以包括把策略引擎132-136注入到软件应用118-122中,策略引擎确保软件应用118-122与包括数据泄漏预防策略、访问控制策略等等的安全策略兼容。

[0079] 如可以认识到的,软件应用132-136可以链接到由安全管理器应用模块112提供的安全服务,如图7-9所示。如图8中所示,由策略引擎132-136实施的策略可以实时改变(是动态的)。这可以基于各种因素,包括但不限于执行上下文、各种计数器、外部事件、明确的策略重定义以及设备用户的改变组和角色成员资格。

[0080] 如图7-图11中所示,安全管理器应用模块112可以可选地包括策略引擎137。策略引擎132-136可以支持发送到软件应用118-122的命令的处理,包括远程锁定、擦除、禁用,等等。擦除命令的处理可以导致软件应用118-122设置回其初始(未使用)状态。各个策略(和命令)可以应用到所有软件应用118-122、软件应用118-122的一部分、单个软件应用118,或者软件应用118的一部分。

[0081] 策略(和命令)可以由每个软件应用118-122从安全管理器应用模块112检索,如图9中所示。作为替代,如图10中所示,策略(和命令)可以由每个软件应用118-122从在设备外部的策略服务器138检索。在一种实施例中,策略(和命令)可以由每个软件应用118-122从安全管理器应用模块112检索,其中安全管理器应用模块112从在设备外部的策略服务器138检索策略(和命令)。如图11中所示,策略(和命令)还可以由每个软件应用118-122(包括安全管理器应用模块112)从之前检索策略(和命令)的另一软件应用118-122检索。如可以认识到的,策略(和命令)由每个软件应用118-122(包括安全管理器应用模块112)的检索可以利用各种方法执行,包括但不限于推送机制、拉取机制、轮询、回调函数、对事件的注册、广播,等等。

[0082] 在一种实施例中,策略的实施或者命令的执行会导致生成执行结果。执行结果可以发送回安全管理器应用模块112和/或策略服务器138。在一种实施例中,执行结果可以是审计事件。执行结果可以是用于收集关于应用使用情况的统计数据的数据。执行结果还可以是用于确定从一个或多个软件应用118-122被使用开始经过多长时间的数据。如可以认识到的,通过其在每个软件应用118-122中实施策略和执行命令的方法可以涉及之前描述的对象代码修改过程。

[0083] 本领域技术人员将认识到,若干安全服务可以在软件应用118-122的对象代码被修改之后由安全管理器应用模块112提供给软件应用118-122。例如,安全服务可以包括认证、授权、审计、单点登录、静态数据的保护、传输中数据的保护、数据泄漏保护策略实施、访问控制策略实施、应用命令执行、密钥管理、密钥分配、程序之间的安全数据共享、软件应用118-122之间的安全通信、供应 (provisioning)、应用生命周期管理、被危及的平台检测、被危及的应用检测,等等。

[0084] 此外,本领域技术人员将认识到,存在若干类型可以使用的认证、单点登录、数据泄漏保护策略、访问控制策略、应用命令和安全工件。认证的类型可以包括密码、PKI证书、挑战/响应、一次性密码、安全令牌、生物识别,等等。单点登录的类型可以包括Kerberos、NTLM、SAML、OpenID、OAuth、WS-Fed、密码HTTP Cookie,等等。可以被实施的数据泄漏保护策略的类型可以包括无离线存储、无备份、对受信任应用的受限开放、对受信任应用的受限拷贝/粘贴、无电子邮件、无消息传送、无聊天、无社交共享、无打印,等等。可以被实施的访问控制策略的类型可以包括认证强度、认证频率、空闲超时、认证会话持续时间、被启用的应用列表、网站和web服务黑名单/白名单、危及检测、闲置时间、时间围栏、地理围栏,等等。可以被执行的应用命令的类型可以包括应用禁用、远程锁定、远程擦除,等等。分配到软件应用118-122的安全工件的类型可以包括用户凭证、认证令牌、单点登录令牌、标识符、数据泄漏保护策略、应用策略、应用命令、应用配置,等等。

[0085] 在计算机上的应用之间建立信任

[0086] 现有技术中存在一个问题就是,安全应用不能认识到它是否可以与同一计算机上的另一应用共享数据,因为该另一应用可能被危及。该另一应用可以是恶意软件,或者它可以是已经被恶意软件危及的合法应用。一些实施例包括通过在设备上安装时让每个应用针对共享秘密,诸如加密密钥或密钥对,向中央安全应用或者彼此注册来在移动设备上的应用之间建立信任。例如,在新应用在设备上安装时,提示用户选择密码,并且密码被用来创建用于应用的密钥。如果另一个受信任的应用想与已安装的应用共享数据,则受信任的应用可以使用用于目标应用的密钥来加密用于其的数据。

[0087] 一些实施例的技术优点包括当时间不是非常宝贵时计算设备上的应用可以在非紧迫的时间彼此建立信任。应用的签名可以在随后进行比较,以确定它们是否匹配在它们最初创建时所存在的签名。

[0088] 如可以认识到的,安全管理器应用模块112可以向受信任的应用提供安全服务和敏感数据的方式用来在设备上的软件应用118-122之间建立信任。图12是根据本公开内容的实施例说明了利用安全管理器应用模块112在软件应用118-122之间建立信任的方法的示例性框图。响应于经由软件应用118-122对安全服务的请求,如果软件应用118-122利用公共PKI密钥签署,则安全管理器应用模块112促进安全服务。当软件应用118-122通过充分利用现有的计算平台能力和/或安全管理器应用模块112被安装时,每个软件应用118-122的签名可以被验证。计算平台可以经由平台签名验证模块142验证每个软件应用118-122的签名,同时安全管理器应用模块112可以经由安全管理器应用签名验证模块140验证每个软件应用118-122的签名,如图12中所示。在一种实施例中,安全管理器应用模块112可以用来确认软件应用118-122和关联的计算平台还没有被危及,并且验证软件应用118-122的签名。

[0089] 每个软件应用118-122的签名可以在运行时被验证,或者充分利用现有的计算平台能力和/或通过安全管理器应用模块112。可用于利用相同PKI密钥签署的软件应用118-122的共享通信机制可以用于建立与安全管理器应用模块112和剩余的受信任的软件应用118-122 的信任。iOS平台上这种共享通信机制的例子是向密钥链写数据。

[0090] 在一种实施例中,包含在PKI密钥的证书中或者与其关联的标识符可以添加到一组软件应用118-122当中每一个,以便让它们彼此信任。

[0091] 在另一种实施例中,所有应用都是利用嵌入在它们当中的公共密钥建立的。在这种情况下,多个应用数据包括公共密钥。图13是根据本公开内容的实施例说明了与具有公共密钥144的软件应用118- 122通信的安全管理器应用模块112的示例性框图。当软件应用118- 122想被信任时,它可以发起与安全管理器应用模块的通信交换验证模块146的通信交换。这种通信交换可以被加密并且可选地利用公共密钥144签署或MAC。如可以认识到的,多种具体且众所周知的密码机制当中任何一种都可以在这种通信交换中用来验证想被信任的软件应用118-122并且安全管理器应用模块112共享相同的公共密钥。在验证通信交换之前,安全管理器应用模块112可以用来检查计算平台和/或软件应用118-122还没有被危及。

[0092] 图14是根据本公开内容的实施例说明了软件应用118-122的密码注册以便建立与安全管理器应用模块112的信任的示例性框图。在一种实施例中,当软件应用118-122最初被安装时,它是不被信任的。为了接收信任,软件应用118-122可以对安全管理器应用模块112进行注册调用。然后,安全管理器应用模块112可以向用户呈现对话框,从而指示请求被信任的软件应用118-122的名称,并且提供应用注册密码148。在呈现该对话框之前,安全管理器应用模块112可以用来检查计算平台和/或软件应用118-122还没有被危及。

[0093] 在一种实施例中,应用注册密码148可以在由不被信任的软件应用118-122提示的对应对话框中输入,并且然后可以被用来派生出用来与安全管理器应用模块112和剩余的受信任的软件应用118-122建立信任的密钥150。这个派生出的密钥150可以用来发起与安全管理器应用模块112的通信交换验证模块146的通信交换。如上所述,这种通信交换可以加密并且可选地利用密钥150签署或MAC。在一种实施例中,在呈现这个对话框之前,修改后的对象代码可以用来检查计算平台和/或软件应用118-122还没有被危及。

[0094] 如可以认识到的,安全管理器应用模块112可以对来自软件应用 118-122的建立应用信任的注册请求作出响应。安全管理器应用模块 118-122可以提示用户输入应用注册密码148,并且利用应用注册密码148生成建立应用信任的密钥150,以促进由安全管理器应用模块112向软件应用118-122提供安全服务。

[0095] 由于利用一种方法的信任建立,一个或多个诸如密钥的安全工件可以从安全管理器应用模块112分配到新近被信任的软件应用118- 122。然后,这些安全工件可以用来以安全方式请求安全服务或交换数据。因此,安全管理器应用模块112可以向软件应用118-122提供密钥150,以允许软件应用118-122向安全管理器应用模块112发送对安全服务的请求。

[0096] 计算机内应用之间受保护的通信

[0097] 本领域中存在一个问题就是,由应用存储的数据或者应用之间的通信可以被运行在相同设备上的恶意软件探听。一旦恶意软件感染了设备,它通常就能够访问存储器中或盘上未加密的数据,或者应用之间未加密的通信。而且这可以在用户不知道的情况下在后

台暗中进行。

[0098] 一些实施例的技术优点允许设备上注册的应用之间几乎所有保存的数据和通信被加密。用于应用内数据的加密和解密的密钥本身被加密,从而阻止可能的攻击者获得该密钥。在一个应用中作为加密数据被持久化的数据可以在不必解密该数据的情况下传送到另一个应用,从而节约处理时间和功率。相反,加密数据的密钥在应用之间被传送,本身被加密。即使恶意软件碰巧找到了通往设备的途径,在应用之间传送数据也是相对安全的。

[0099] 如可以认识到的,安全管理器应用模块112可以配置和/或编程为以方便以下的途径在设备上的软件应用118-122之间共享数据:数据可以在一组受信任的应用之间自由共享,但是不能导出到不受信任的应用;数据可以从不受信任的应用导入到受信任的应用;存储在受信任的应用内部的数据可以一直都加密;在受信任的应用之间共享的数据可以在受信任的应用之间传输中被加密;大数据对象不需要为了在应用之间共享而重新加密,以避免共享过程中显著的计算;以及在无需用户交互的情况下允许应用之间的数据共享(接受UI对话框,等等)。

[0100] 另外,安全管理器应用模块112可以配置和/或编程为,当期望用户交互以从给定数据对象应当在什么应用中打开(共享到其)的列表进行选择时,经由用户接口显示受信任的软件应用118-122的列表。数据可以包括文档、安全工件、策略、命令、应用之间的请求/响应,等等。数据可以在设备上受信任的软件应用118-122内部、设备上不受信任的软件应用118-122内部或者在设备外部创建。用户交互可以用作极其敏感的商业或机密数据的双重检查。

[0101] 一些实施例使用充当设备的集中式密钥储存库的安全管理器应用。安全管理器应用的优点可以是它专用于在高级别保护密钥,从而允许由无安全意识的开发者所写的其它应用在其它领域中专用。

[0102] 图15是根据本公开内容的实施例说明了使用应用数据保护密钥 152-156来维护与安全管理器应用模块112安全性的示例性框图。如图15中所示,每个软件应用118-122可以包括一个或多个独特的应用数据保护密钥152-156。优点是,如果特定的软件应用118-122被危及,包括其应用数据保护密钥152-156在内,则这可以被用来限制仅仅到那个软件应用118-122的暴露。这还可以减小任何给定密钥被使用的频率,从而允许其安全地长时间使用。用于每个软件应用 118-122的应用数据保护密钥152-156可以在与安全管理器应用模块 112建立信任时生成。它们可以在软件应用118-122本身内部或者在安全管理器应用模块112内部生成。

[0103] 安全地存储用于软件应用118-122的应用数据保护密钥152-156 的一种方法是让密钥以加密的形式在软件应用118-122本身内部持久化、通过由安全管理器应用模块112维护的多个数据保护根密钥158 之一来加密。当软件应用118-122需要使用应用数据保护密钥152- 156时,它可以发起与安全管理器应用模块112的请求/响应交换,以便利用对应的数据保护根密钥158解密应用数据保护密钥152-156。请求可以包含加密的应用数据保护密钥152-156,而响应可以包含解密的应用数据保护密钥152-156。优点可以是,与应用关联的应用数据保护密钥与应用一起维护,并且因此只在必要时才加载。

[0104] 安全地存储用于软件应用118-122的应用数据保护密钥152-156 的另一种方法是让密钥在安全管理器应用模块112中持久化、通过由安全管理器应用模块112维护的多个数

据保护根密钥158之一来加密。当应用需要使用应用数据保护密钥152-156时,它可以发起与安全管理器应用模块112的请求/响应交换,以便利用对应的数据保护根密钥158解密应用数据保护密钥152-156。响应可以包含解密的应用数据保护密钥152-156。优点可以是,敏感应用数据保护密钥存储在一起,并且可以更好地检测对其存储器空间的入侵。

[0105] 如可以认识到的,对以上这两种方法任意一个的修改可以包括让安全管理器应用模块112向软件应用118-122提供用于软件应用118-122的对应的数据保护根密钥158,以解密应用数据保护密钥152-156本身。优点可以是,不必在请求时传送应用数据保护密钥。

[0106] 如可以认识到的,应用数据可以包括由软件应用118-122和安全管理器应用模块112当中的至少一个生成的应用数据保护密钥152-156。应用数据保护密钥152-156可以由利用安全管理器应用模块112维护的对应数据保护根密钥158加密和解密。

[0107] 在一种实施例中,安全管理器应用模块112可以被用来促进加密的数据对象172-182在软件应用118-122之间的传送。数据对象172-178可以利用对那个数据对象172-182或者相关数据对象172-182集合独特的对象数据保护密钥160-170加密。这些对象数据保护密钥160-170还可以利用它们驻留在其中的软件应用118-122的一个或多个应用数据保护密钥152-156加密。这可以使得能够不需要在传送过程中解除加密数据对象172-182或重新加密数据对象172-182的情况下在软件应用118-122之间共享数据对象172-182。一般而言,加密和解密对象数据保护密钥160-170比加密和解密数据对象172-182本身快得多,原因在于,大多数数据对象172-182显著大于它们的对象数据保护密钥160-170。

[0108] 图16是根据本公开内容的实施例说明了用于从源(第一)应用184向目的地(第二)应用186安全地传送数据对象172-182的方法的示例性框图。该方法可以包括利用源(第一)应用184的应用数据保护密钥152解密用于数据对象172的对象数据保护密钥160;并且利用由安全管理器应用模块112生成的数据共享密钥188加密用于数据对象172的对象数据保护密钥160。当建立信任时,数据共享密钥188可以从安全管理器应用模块112传送到源(第一)和目的地(第二)应用184和186。数据共享密钥188也可以在新数据对象172需要被共享,或者响应于由源(第一)和目的地(第二)应用184和186的安全服务请求而被安全管理器应用模块112用于加密和解密时按需传送。

[0109] 该方法还可以包括向目的地(第二)应用186传送数据对象172和用于数据对象172的加密的数据保护密钥160;利用数据共享密钥188解密用于数据对象172的对象数据保护密钥160;并且利用目的地(第二)应用186的应用数据保护密钥154加密用于数据对象172的对象数据保护密钥160。

[0110] 如可以认识到的,安全管理器应用模块112可以在从源(第一)软件应用184向目的地(第二)软件应用186传送数据对象172和对象数据保护密钥169之前生成用于加密对象数据保护密钥169的数据共享密钥188,并且在从源(第一)软件应用184向目的地(第二)软件应用186传送数据对象172和对象数据保护密钥160之后解密对象数据保护密钥160。

[0111] 图17是根据本公开内容的实施例说明了用于从源(第一)应用184向目的地(第二)应用186安全地传送数据对象172-182的另一方法的示例性框图。该方法可以包括利用源(第一)应用184的应用数据保护密钥152解密用于数据对象172的对象数据保护密钥160;并且利用目的地(第二)应用186的应用数据保护密钥154加密用于数据对象172的对象数据保护密钥160。当信任建立时,目的地(第二)应用186的应用数据保护密钥154可以从安全管

理器应用模块 112传送到源(第一)应用184。目的地(第二)应用186的应用数据保护密钥154还可以在新数据对象172需要被共享,或者响应于源(第一)应用184的安全服务请求而被安全管理器应用模块112用于加密和解密时按需传送。该方法还可以包括向目的地(第二)应用 186传送数据对象172和用于数据对象172的加密的对象数据保护密钥160。

[0112] 根据本公开内容的实施例,安全管理器应用模块112可以被用来促进受限平台上的应用之间的安全数据共享。设备平台可以对数据如何在软件应用118-122之间共享强加约束。每个平台可以具有用于在软件应用118-122之间共享数据的各种机制,但是每种机制可以具有使其不适用于被其自己用于安全数据共享的具体限制。每个数据共享机制可以具有最大数据尺寸或者把整个数据对象放在存储器108中,使得它不能用于共享大数据对象。它可以让所有软件应用118-122开放地访问,使得它不能用于以未加密的形式共享敏感数据。它不能支持利用需要的用户交互编程地启动,使得它不能用于数据对象的自动编程共享。它还不能向目的地应用传送控制,使得它不能用于请求/ 响应处理。此外,当应用不在前台时,它可以是不活动的,使得它不能用于从另一应用接收数据。

[0113] 本领域技术人员将认识到,存在几类数据共享机制。例如:

[0114] 类1:向目的地应用传送控制的机制,不需要用户交互,并且只能让源应用和目的地应用访问,但是不能用于共享大数据对象。这类机制的例子是iOS平台上的定制URL方案处理。

[0115] 类2:可以用于共享大数据对象的机制,不需要用户交互,并且只能让有限集合的受信任应用访问,但是不向目的地应用传送控制。这类机制的例子是iOS平台上的密钥链。

[0116] 类3:可以用于共享大数据对象的机制,不需要用户交互,但是不向目的地应用传送控制并且是所有应用可开放访问的。这类机制的例子是iOS平台上的粘贴板(pasteboard)。

[0117] 类4:向目的地应用传送控制的机制,不需要用户交互,可以用于共享大数据对象,并且只能由源应用和目的地应用访问,但是只在应用过渡到后台时短时间活动并且当应用完全处于后台时是不活动的。这类机制的例子是iOS平台上的本地接收套接字。

[0118] 类5:向目的地应用传送控制的机制,可以用于共享大数据对象,并且只能让源应用和目的地应用访问,但是需要用户交互来选择目的地应用。这类机制的例子是iOS平台上用于注册的文件类型的open- in函数。

[0119] 在一种实施例中,提供了在受限平台上从源应用184到目的地应用186安全地共享数据而不需要用户交互的方法。该方法包括向源应用184发送利用类2数据共享机制写数据对象172的指令,并且通过源应用184加密数据对象172。该方法还可以包括向源应用184发送使用类1数据共享机制向目的地应用186传送控制的指令,包括识别利用类2数据共享机制所写的数据对象172的足够信息。类1数据共享机制可以可选地包括加密利用类2数据共享机制所写的数据对象 172的对象数据保护密钥160。此外,该方法可以包括向目的地应用186发送利用类2数据共享机制读取数据对象172并解密数据对象 172的指令。

[0120] 提供了可以被用来在发出请求的应用与作出响应的应用之间执行安全的请求/响应交互而不需要用户交互的另一种方法。发出请求的应用可以利用类2数据共享机制写请求,其中请求的至少一些部分由源应用加密。发出请求的应用可以利用类1数据共享机制向作出响应的应用传送控制,包括识别利用类2数据共享机制所写并且发出请求的应用对其

响应的请求的足够信息。类1数据共享机制可以可选地包括加密利用类2数据共享机制所写的请求的密钥。作出响应的应用可以利用类2数据共享机制读取请求并且解密该请求的加密部分。作出响应的应用还可以处理请求并且利用类2数据共享机制写响应,其中响应的至少一些部分由作出响应的应用加密。此外,作出响应的应用可以使用类1数据共享机制向发出请求的应用传送控制,包括识别利用类2数据共享机制所写的响应的足够信息。类1数据共享机制可以可选地包括加密利用类2数据共享机制所写的响应的密钥。发出请求的应用可以利用类2数据共享机制读取响应并且解密该响应的加密部分。

[0121] 在另一种实施例中,只要请求和响应不是太长,请求和可选的密钥的位置就可以在之前的方法中反转,以导致以下方法。发出请求的应用可以利用类2数据共享机制写密钥。然后,发出请求的应用可以利用类1数据共享机制向作出响应的应用传送控制、发送其至少一些部分被密钥加密的请求,包括识别利用类2数据共享机制所写并且发出请求的应用对其响应的密钥的足够信息。然后,作出响应的应用可以利用类2数据共享机制读取密钥并且解密该请求的加密部分。接下来,作出响应的应用可以处理请求并且可选地利用类2数据共享机制写新密钥。作出响应的应用可以利用类1数据共享机制向发出请求的应用传送回控制、发送其至少一部分由密钥加密的响应(或者与请求相同的密钥或者新响应密钥),包括识别利用类2数据共享机制所写的密钥的足够信息。最后,发出请求的应用可以利用类2数据共享机制读取密钥并且解密响应的加密部分。

[0122] 本领域技术人员将根据以上描述认识到用于在受限平台上应用之间的安全数据共享的其它备选方法,例如,请求的不同部分、响应的不同部分以及密钥的不同部分可以以多种途径在类1数据共享机制与类2数据共享机制之间分割。作为替代,类3数据共享机制可以在上述方法中代替类2数据共享机制使用,例如,如果利用类3数据共享机制所写的任何数据都是利用如前所述的应用数据保护密钥来加密的。另一种备选方案包括可在上述方法中代替类2数据共享机制使用的类4数据共享机制(当每个软件应用118-122进入后台时,在其中临时可用),例如,如果每个数据传送可以在过渡到后台的应用变得不活动之前短时间内执行。

[0123] 在一种实施例中,提供了可以用来从受信任的源应用184向受信任的目的地应用186安全地共享数据而不需要用户交互来选择目的地应用186但是阻止数据输出(export)给不受信任的应用的方法。在这个示例性方法中,源应用184可以利用类5数据共享机制写数据对象172。数据对象172可以由源应用186加密,并且可以写为独特的数据或文件类型,使得当从支持给定数据或文件类型的的应用列表选择时,只显示受信任的应用列表。然后,目的地应用186可以利用类5数据共享机制读取数据对象172并且解密数据对象172。如可以认识到的,之前描述的用于从源应用184向目的地应用186安全地传送数据的任何方法都可以用来加密和解密数据对象172。

[0124] 根据本公开内容的实施例,优选地是利用如前所述的应用数据保护密钥传送加密的数据对象,以便最小化对可能利用众所周知的技术潜在地被危及的平台级保护的依赖。为了安全性,利用在应用外部持久化数据的数据共享机制所写的任何暂时(transient)数据可以在其被读取之后被删除。

[0125] 技术优点与应用一样多。例如,在实施例中,用户在其智能电话上可以在业务智能应用中准备机密数据的图表并且从业务智能应用发起新的电子邮件。业务智能应用打开智

能电话的电子邮件客户端,用于让用户“撰写”电子邮件。在数据对象中,图表在商业智能应用中以加密形式持久化,由对象数据保护密钥加密。对象数据保护密钥在商业智能应用中持久化,本身用商业智能应用自己的密钥加密。商业智能应用从智能电话上的中央安全管理器应用请求其密钥,并且中央安全管理器以未加密形式把其提供给商业智能应用。商业智能应用还从安全管理器应用请求数据共享密钥,并且商业智能应用提供数据共享密钥。然后,商业智能应用利用其自己的密钥解密对象数据保护密钥,然后利用数据共享密钥加密对象数据保护密钥。利用数据共享密钥加密的对象数据保护密钥连同(已经加密的)图表传送到电子邮件客户端。在电子邮件客户端中,对象数据保护密钥利用数据共享密钥解除加密,其中数据共享密钥是从安全管理器应用请求的。图表利用对象数据保护密钥解除加密,然后插入用户可以撰写的新电子邮件。

[0126] 如可以认识到的,上述任何方法都可以与在标题为“Methods and Apparatuses for Secure Communication”的未决美国专利申请序列No.13/405,357和标题为“Methods and Apparatuses for Interaction with Web Applications and Web Application Data”的美国专利申请序列No.13/215,178中公开的一个或多个方法和系统集成、组合和/或使用,这两个申请的全部内容都通过引用被结合于此。

[0127] 根据本公开内容的实施例,还提供了提供指令的机器可读介质,当指令被具有处理器110和存储器108的机器读取时,使机器根据上述任何方法执行操作。

[0128] 虽然已经根据目前被认为最实际和优选的实施例对系统、方法和机器可读介质进行了描述,但是应当理解,本公开内容不需要局限于所公开的实施例。它是要覆盖包括在权利要求精神和范围内的各种修改和类似布置,权利要求的范围应当符合最广泛的解释,从而涵盖所有此类修改和类似的结构。本公开内容包括任何和全部以下权利要求的实施例。

[0129] 还应当理解,在不背离本发明本质的情况下,可以进行各种变化。这种变化也隐含地包括在描述中。它们仍然属于本发明的范围。应当理解,本公开内容要产生覆盖本发明各个方面的一个或多个专利,独立地或者作为一个整体系统、机器可读介质并且以方法和装置两种模式。

[0130] 另外,本发明和权利要求的各个要素当中每一个也可以以各种方式实现。本公开内容应当理解为涵盖任何装置实施例、方法、机器可读介质或过程实施例的实施例的每个此类变化,或者甚至仅仅是这些的任何要素的变体。

[0131] 特别地,应当理解,由于本公开内容涉及本发明的要素,因此用于每个要素的措辞可以通过方法术语的等效装置术语来表示-即使只有功能或结果是相同的。这种等效的、更广义的或者甚至更一般的术语应当被认为涵盖在每个要素或动作的描述中。这种术语可以在期望的时候被替换,以便使本发明有权的隐含广义的覆盖明确。

[0132] 应当理解,所有动作都可以表示为采取那个动作的手段或者表示为造成那个动作的要素。类似地,每个公开的物理要素都应当理解为涵盖那个物理要素促进的动作的公开内容。

[0133] 本专利申请中提到的任何专利、公开物或其它参考都通过引用被结合于此。此外,关于每个所使用的术语,应当理解,除非其在本申请中的使用与这种解释不一致,否则常见的词典定义应当被理解为对每个术语结合,并且所有定义、备选术语和同义词,诸如包含在本领域技术人员认识到的至少一个标准技术词典中所包含的,都通过引用被结合于此。

[0134] 另外,所有权利要求术语都应当在其最广阔的形式解释,从而赋予本申请人法律许可的最广泛覆盖范围。虽然已经参考附图和具体的例子描述了实施例,但是本领域技术人员将很容易认识到,在不背离本发明精神和范围的情况下,本文所述过程和装置的许多修改和改写都是可能的。因此,应当清楚地理解,本描述仅仅是作为例子进行的并且不是作为对以下阐述的实施例的范围的限制。

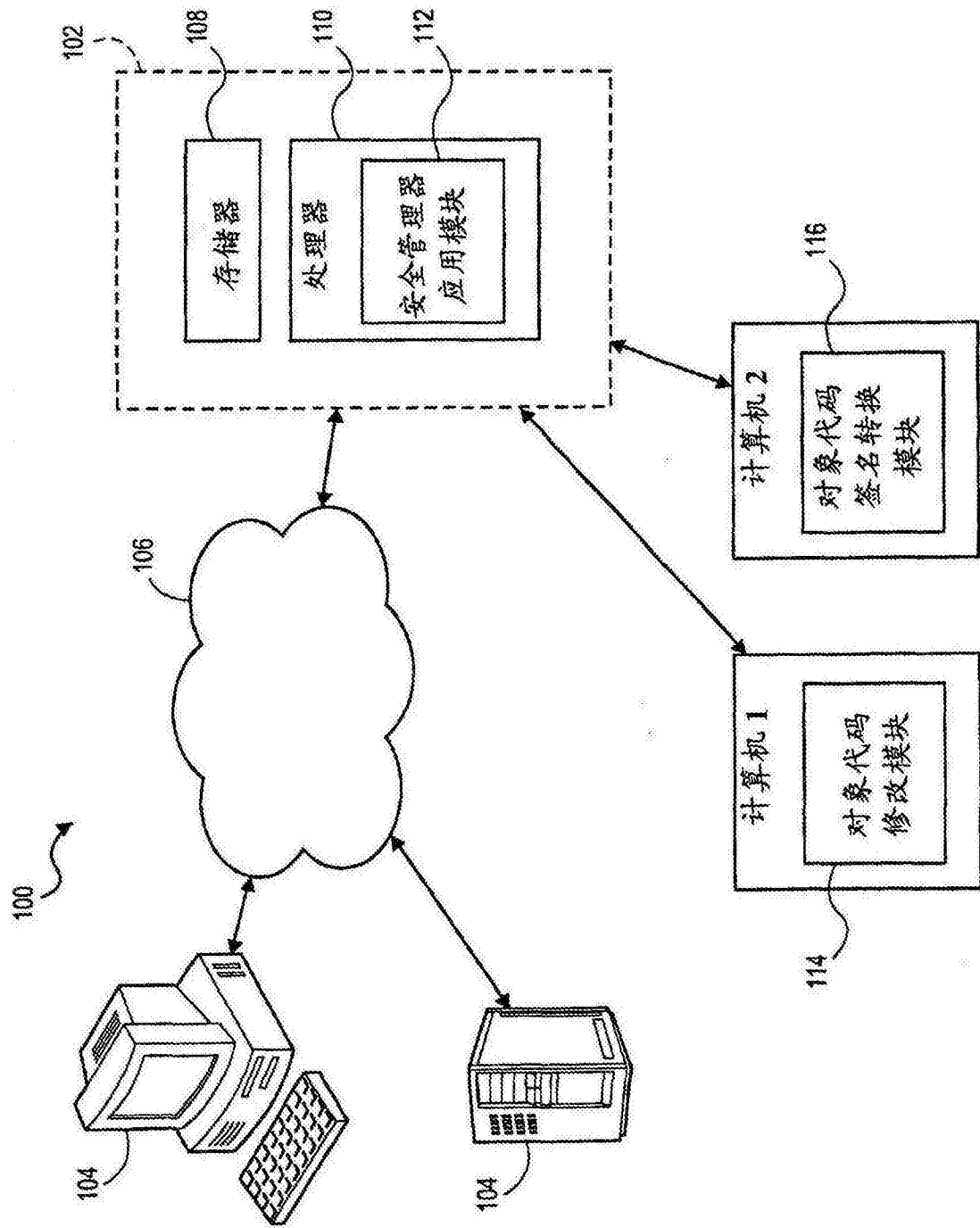


图1

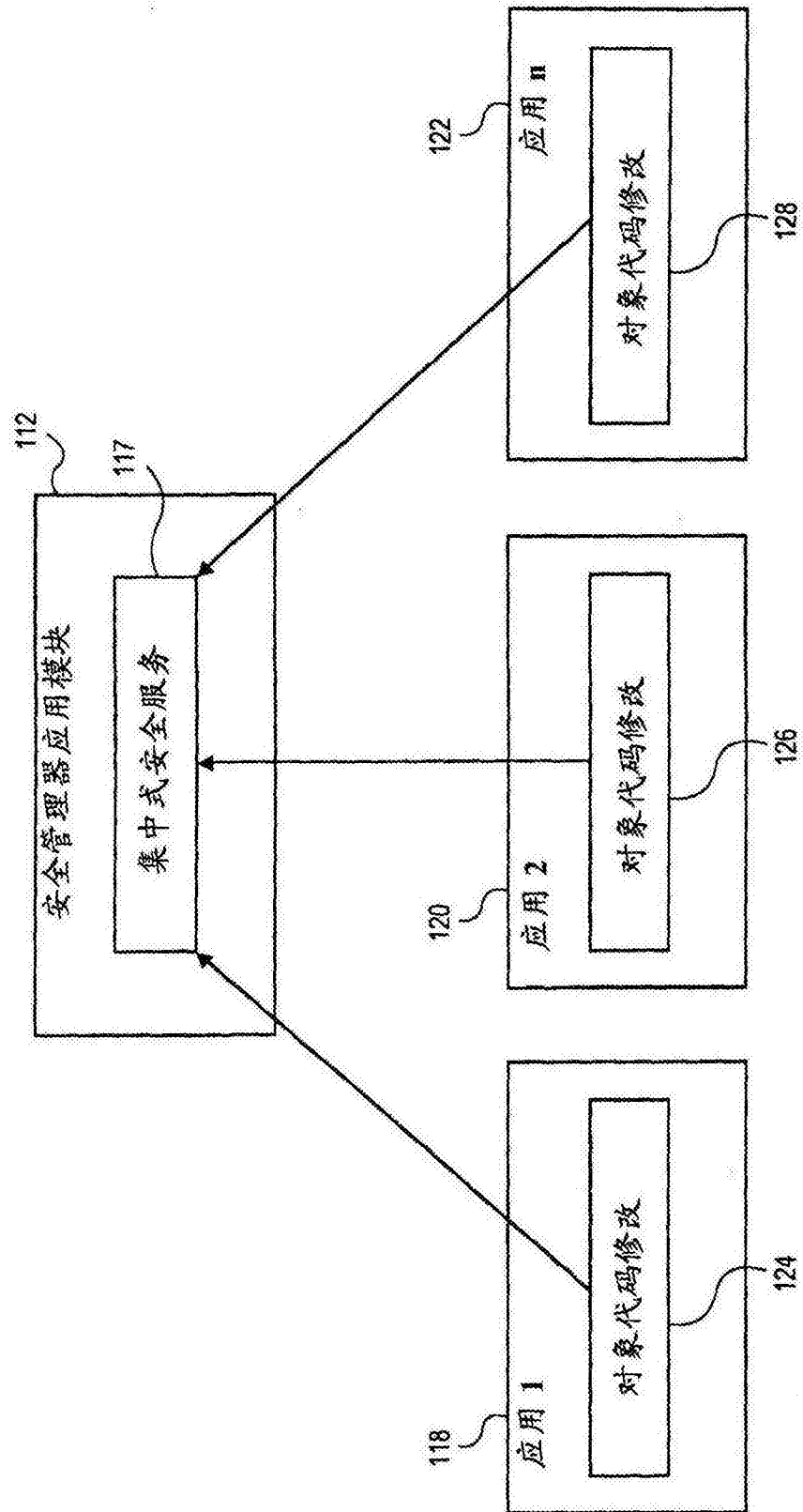


图2

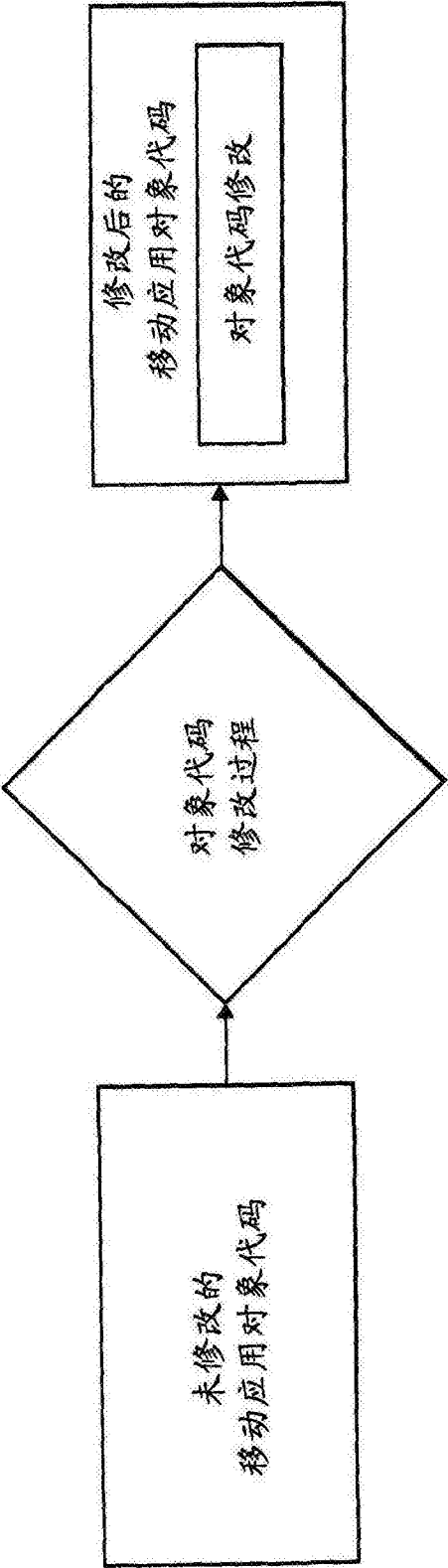


图3

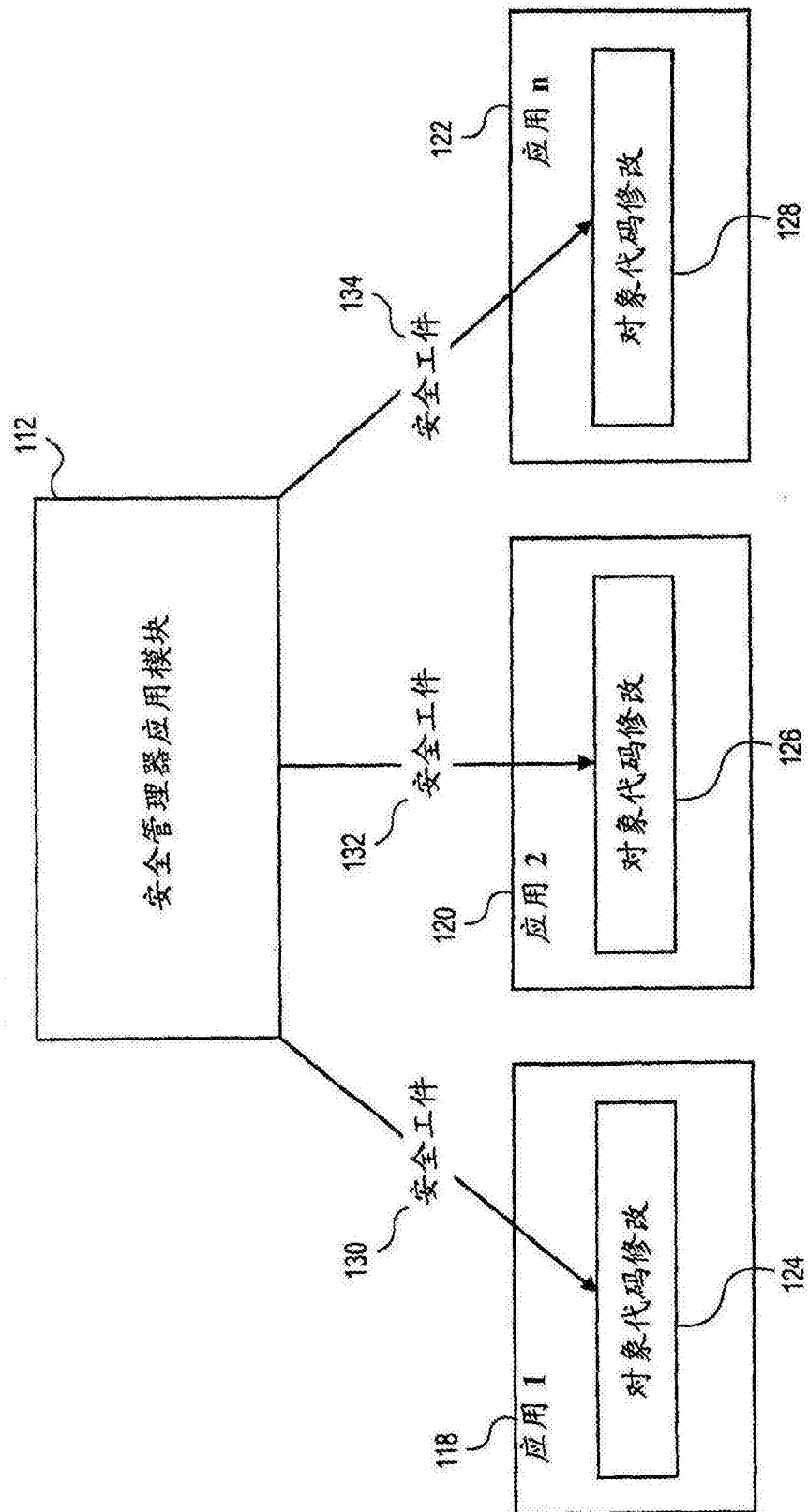


图4

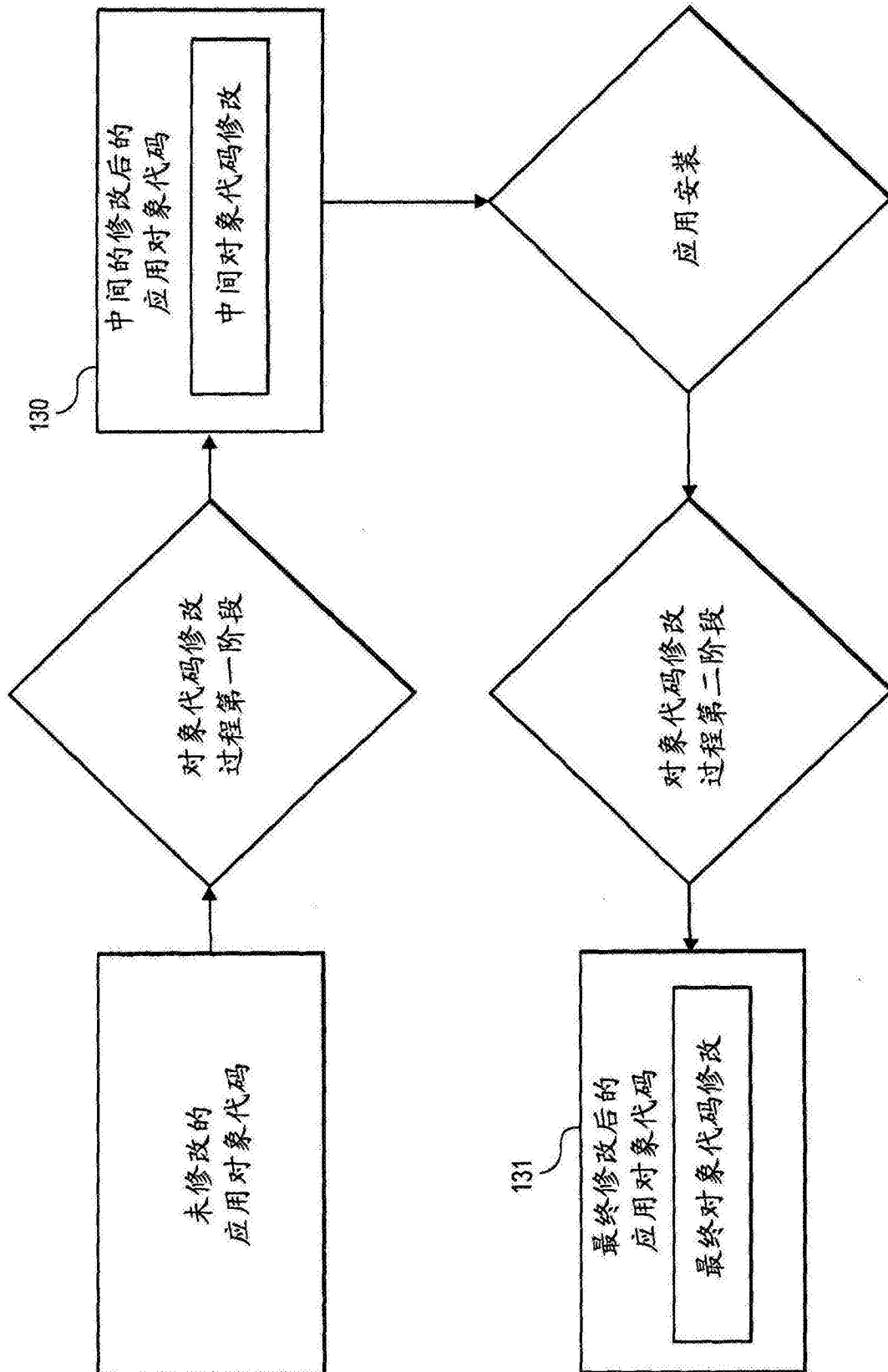


图5

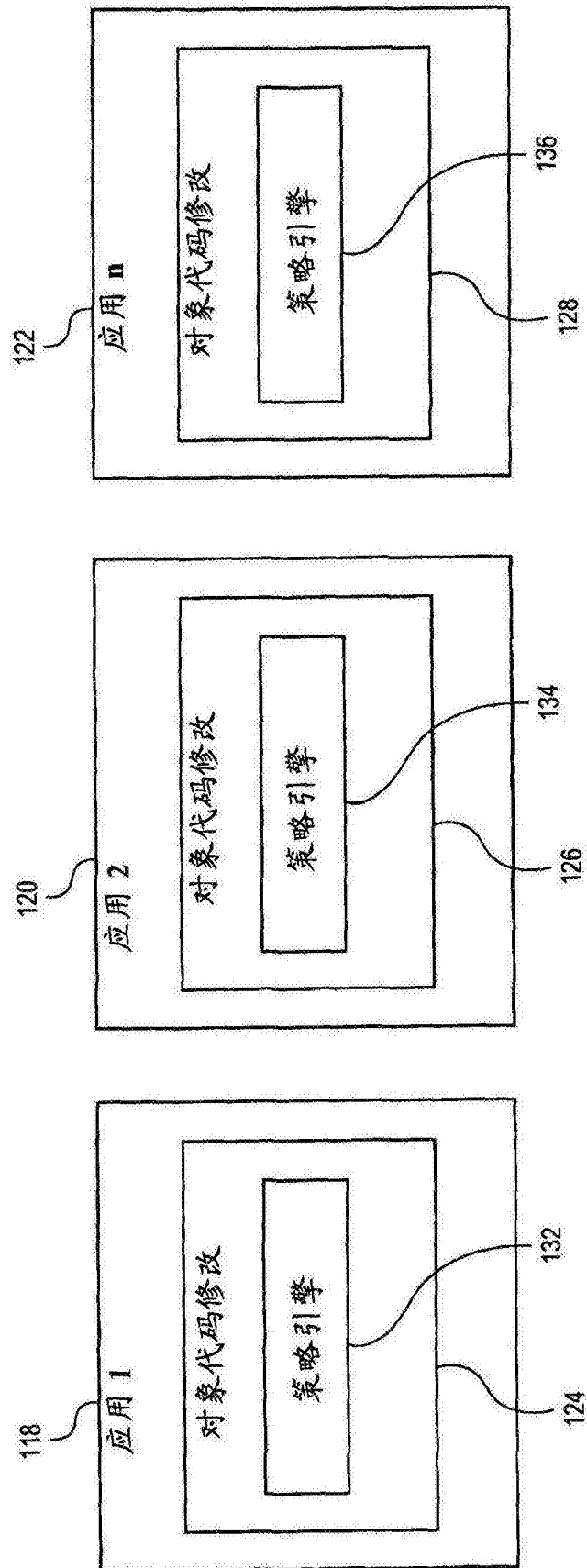


图6

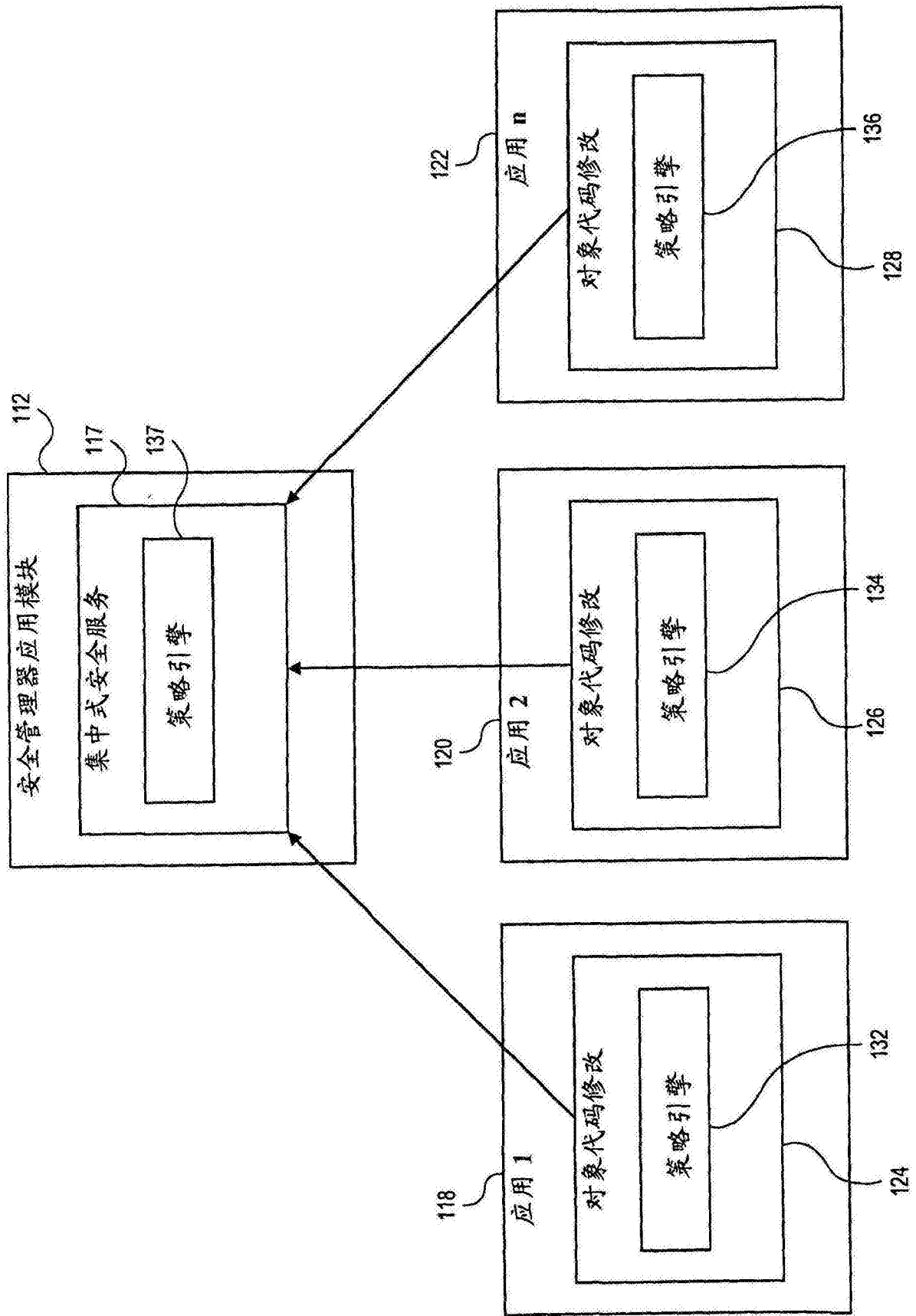


图7

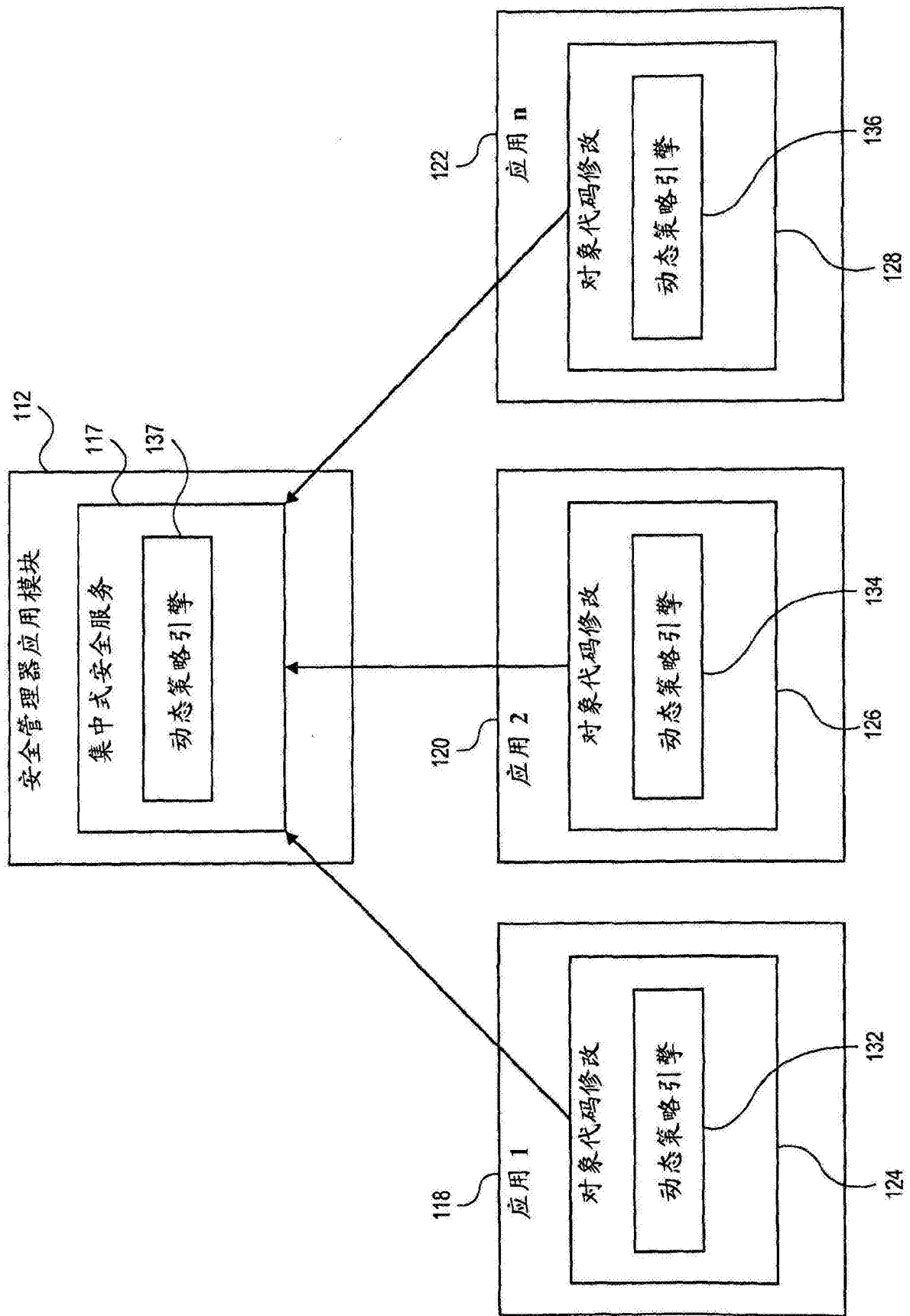


图8

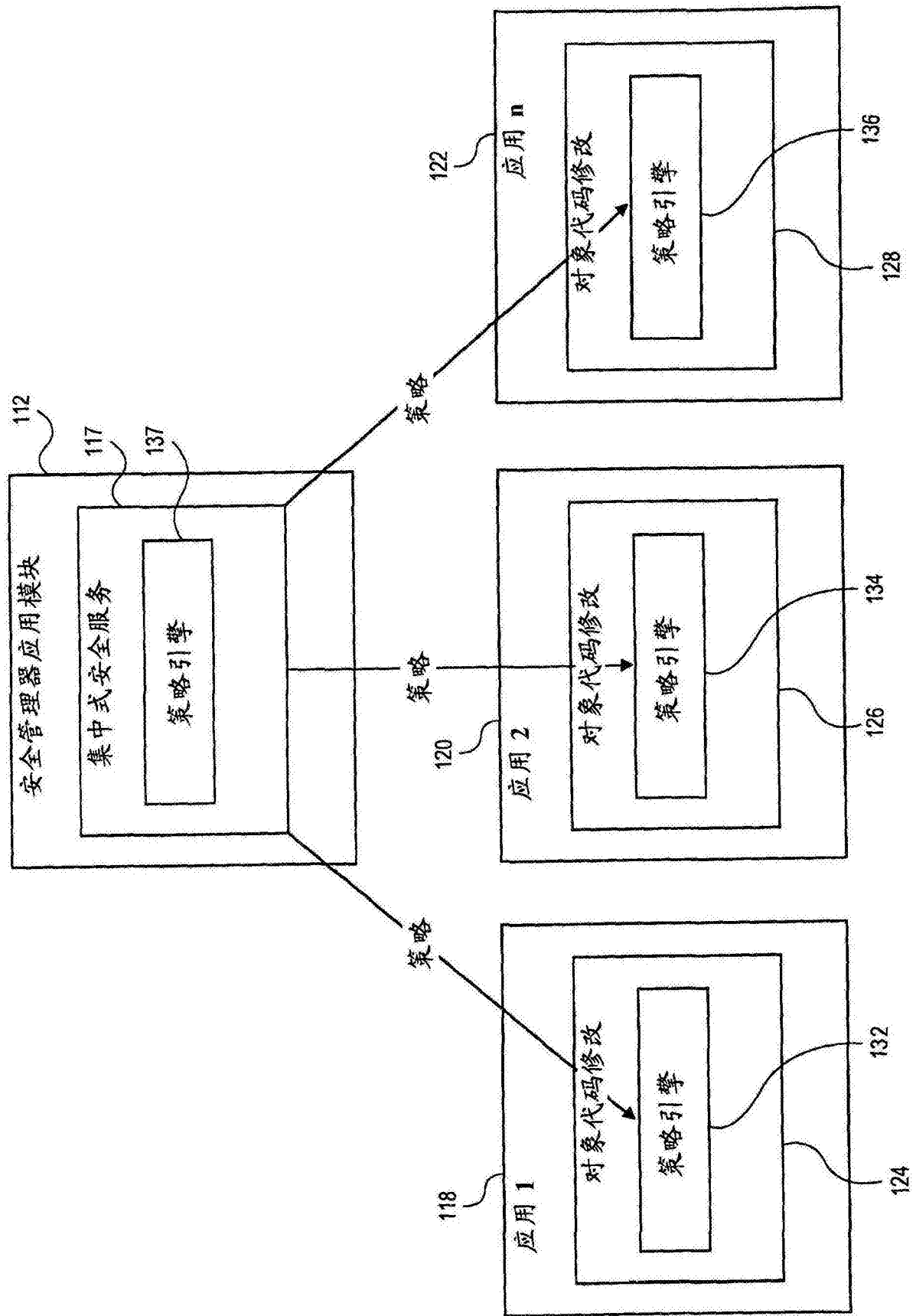


图9

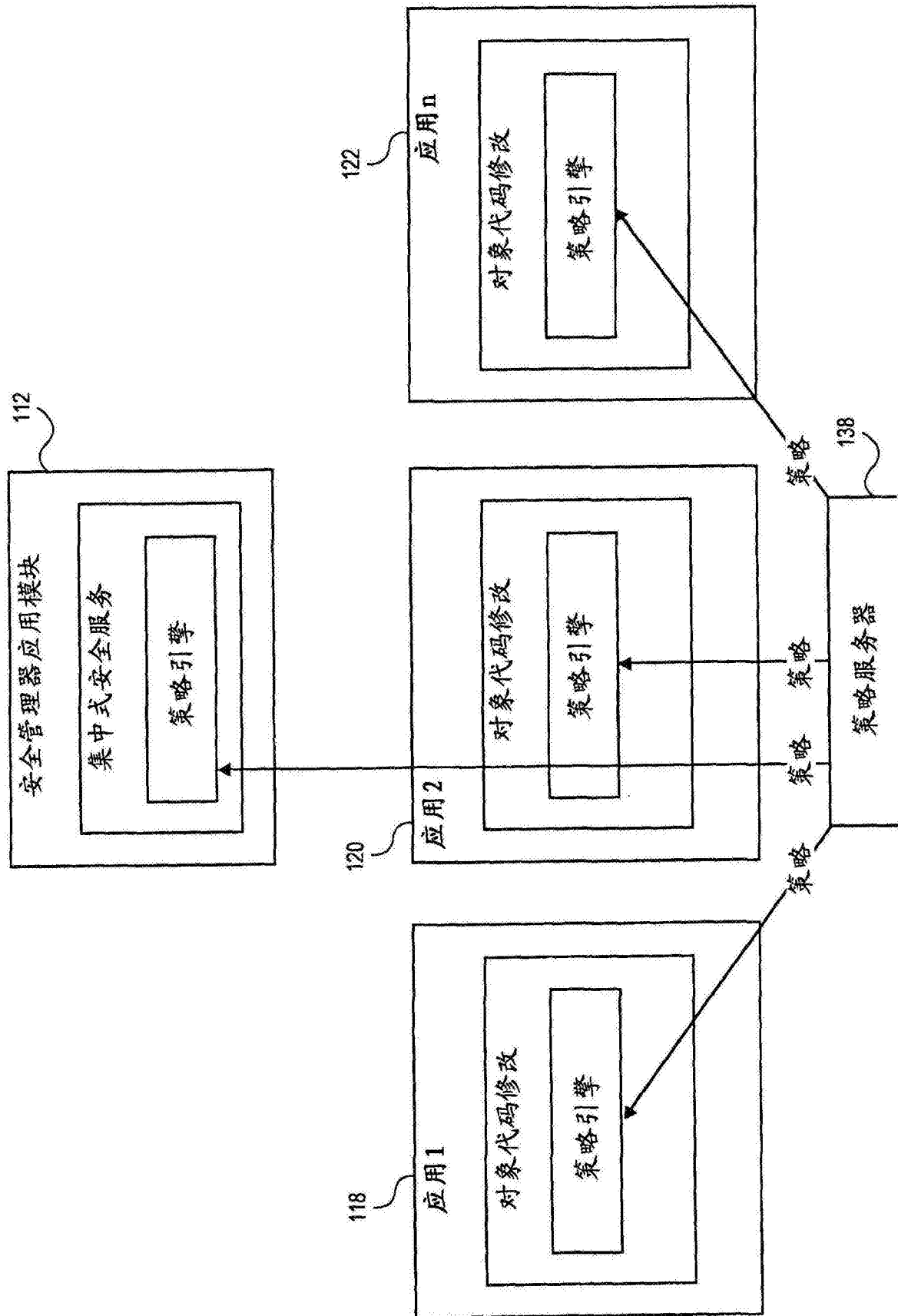


图10

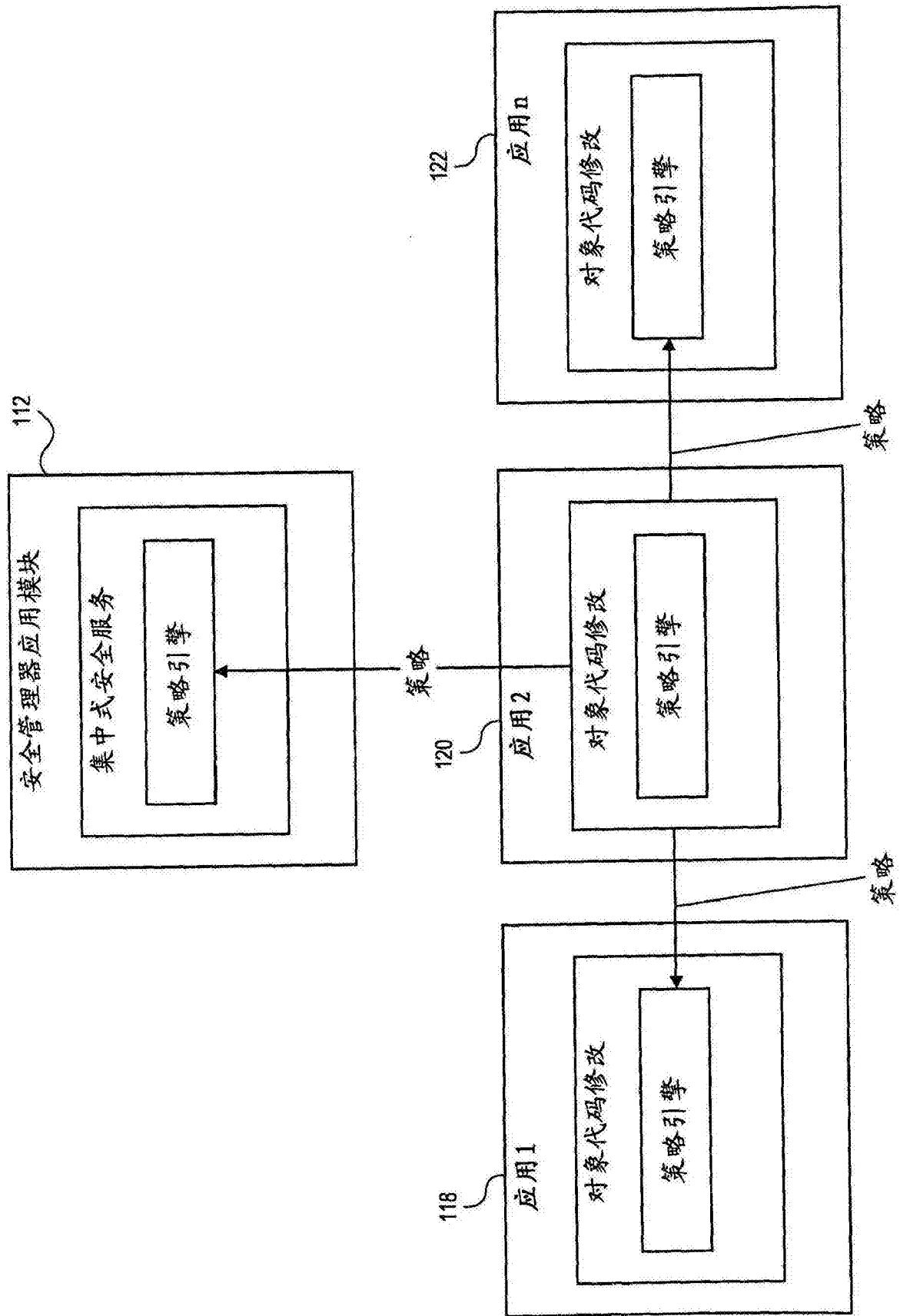


图11

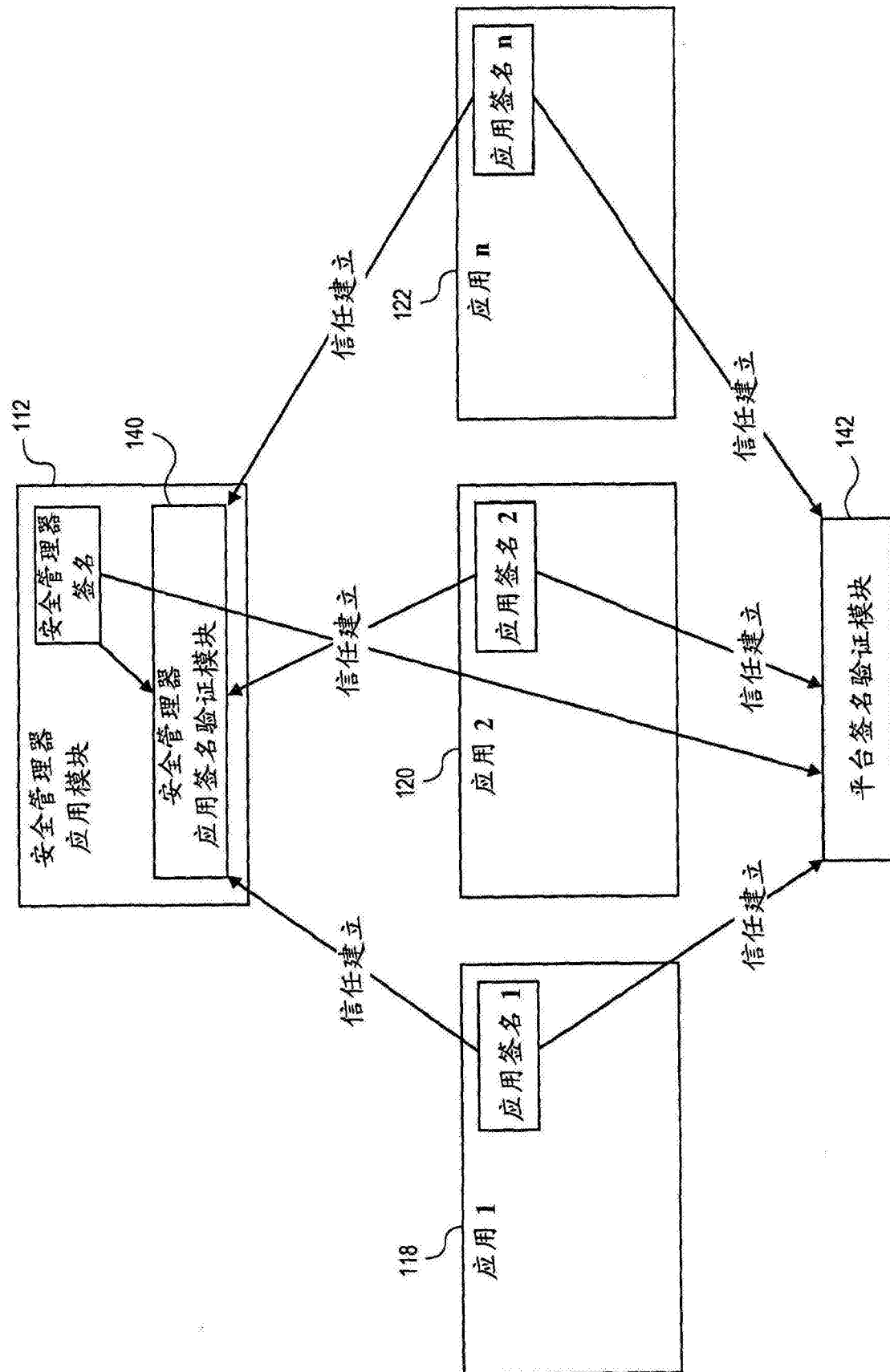


图12

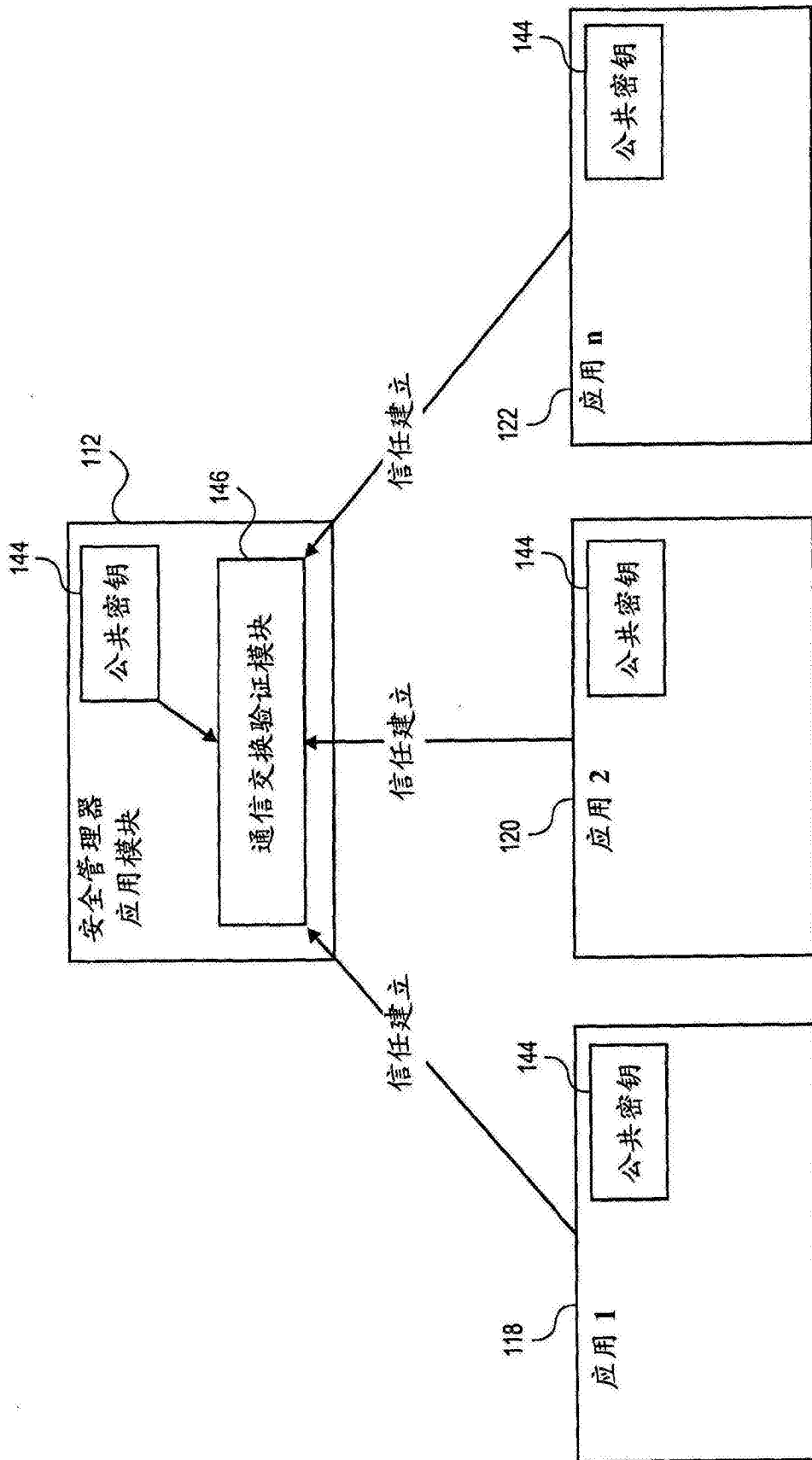


图13

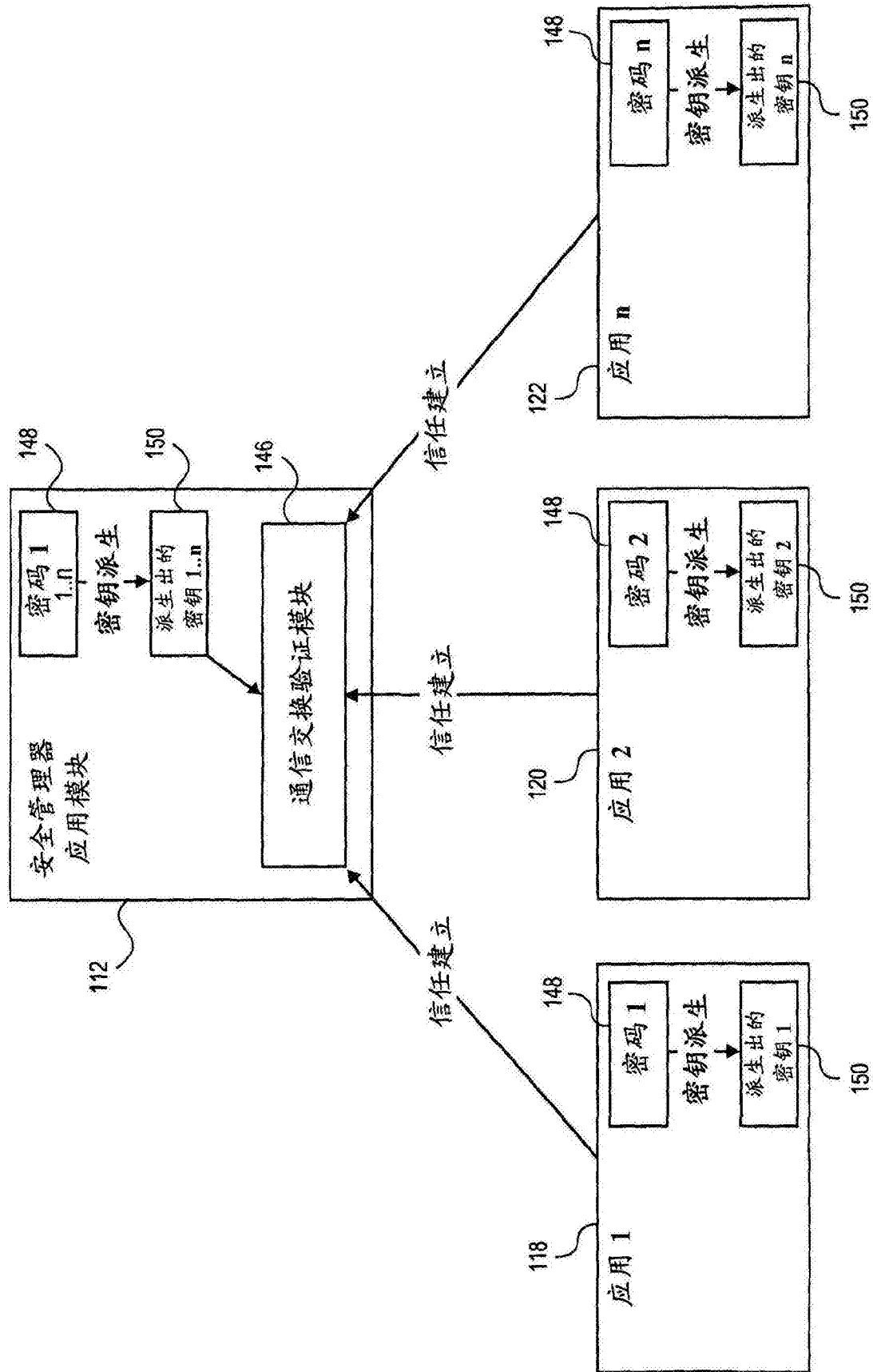


图14

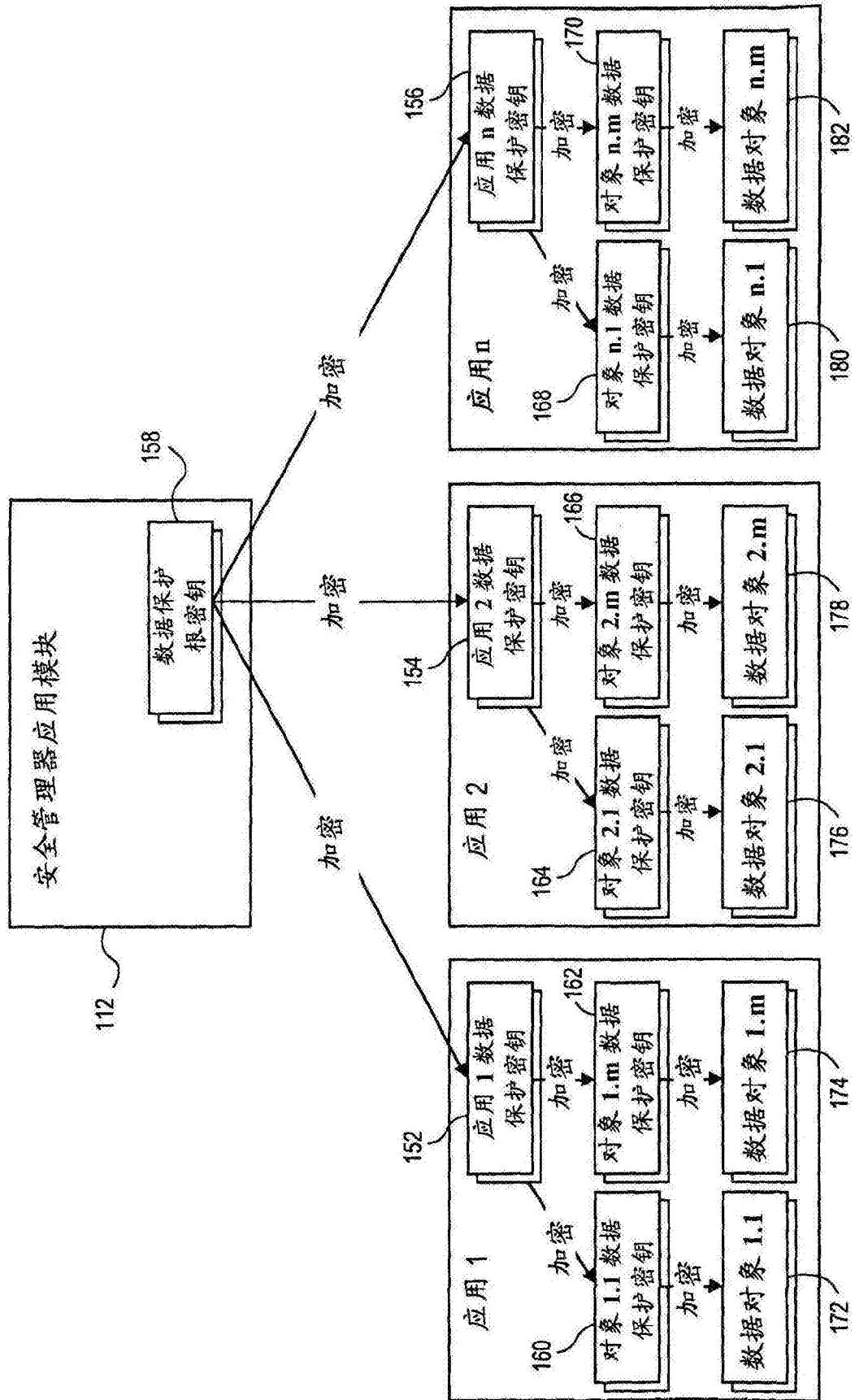


图15

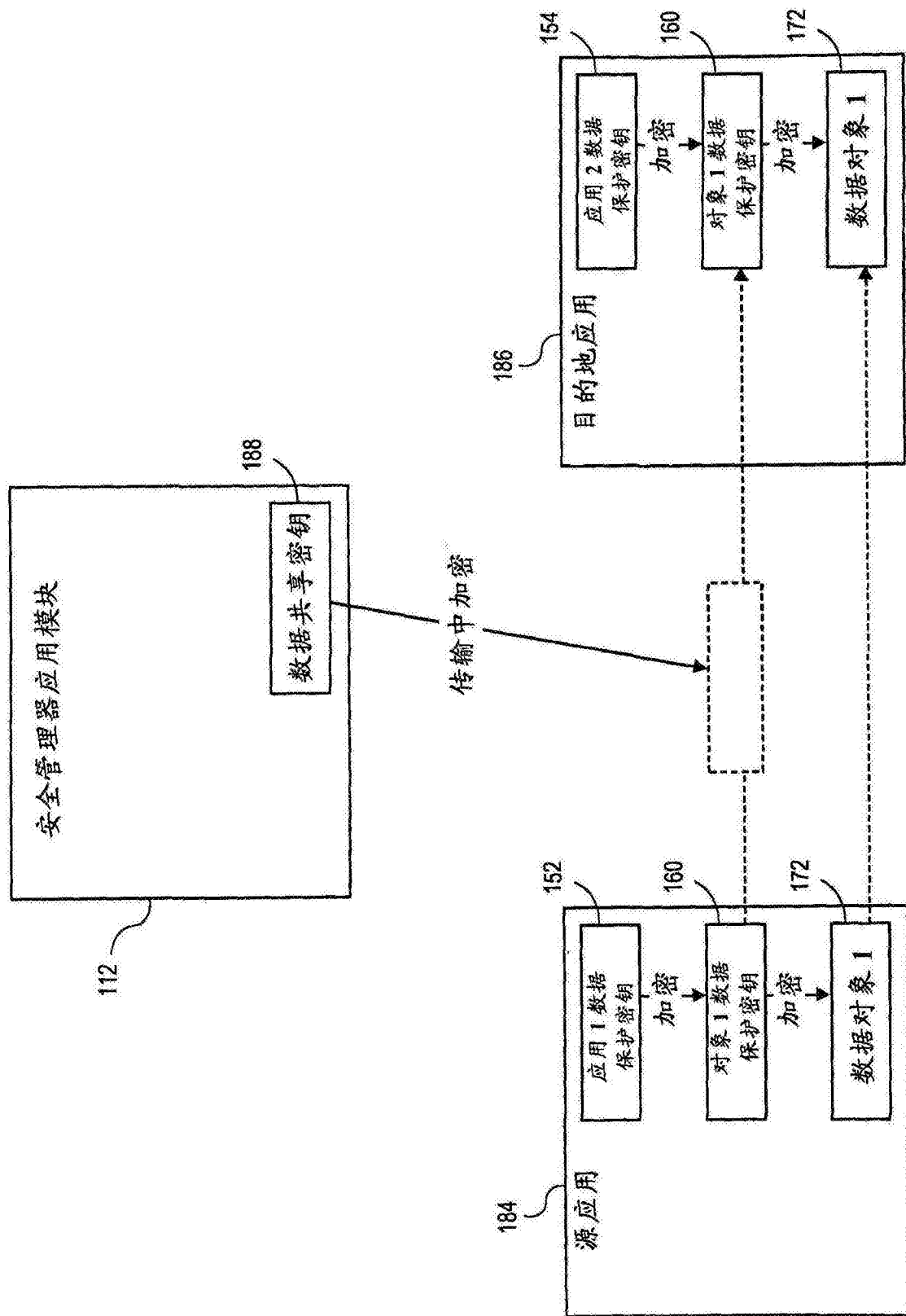


图16

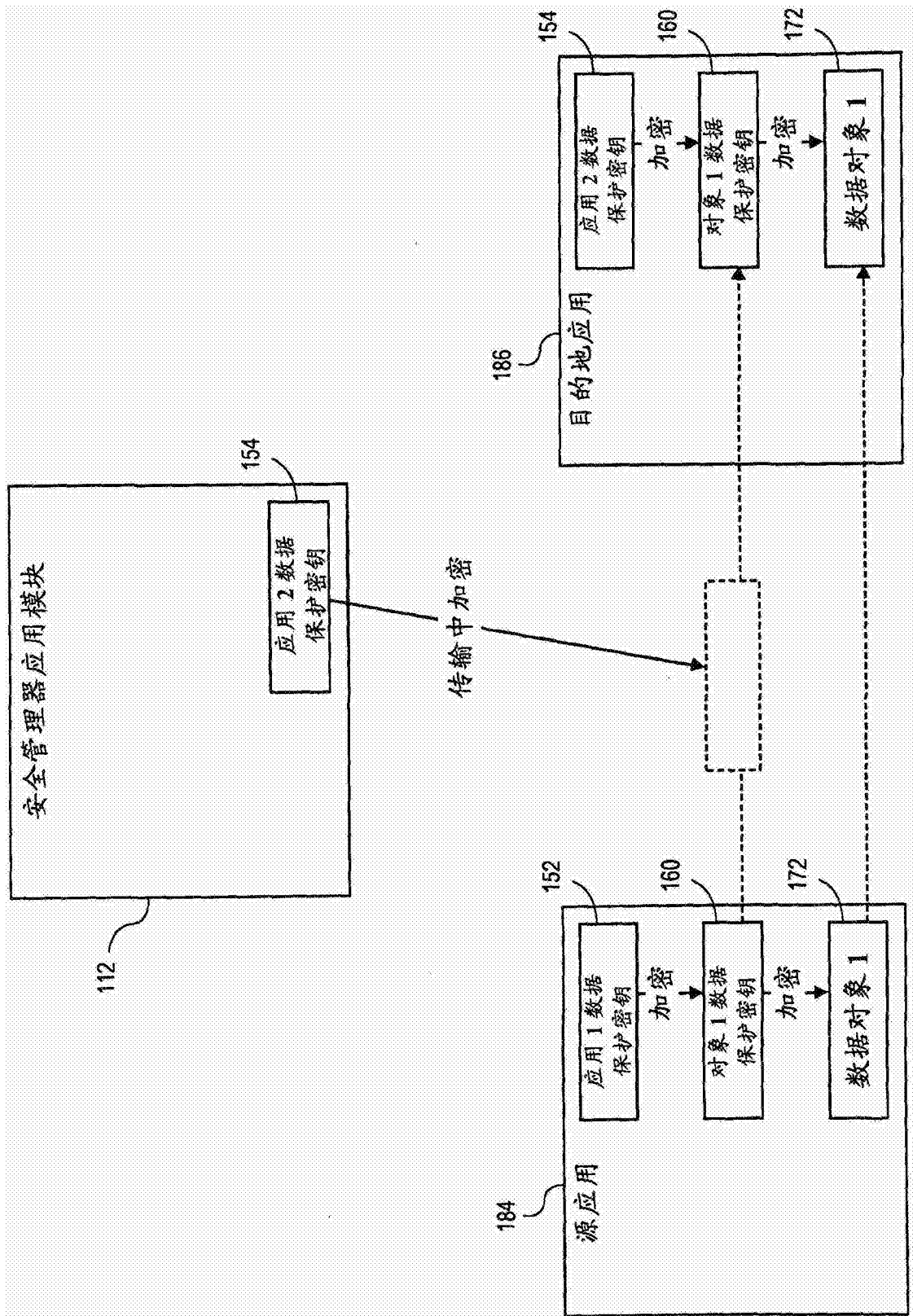


图17