

(12) 发明专利申请

(10) 申请公布号 CN 101953111 A

(43) 申请公布日 2011.01.19

(21) 申请号 200880126865.5

(51) Int. Cl.

(22) 申请日 2008.12.22

H04L 9/08 (2006.01)

G06F 21/20 (2006.01)

(30) 优先权数据

2007907016 2007.12.21 AU

61/021,271 2008.01.15 US

(85) PCT申请进入国家阶段日

2010.08.16

(86) PCT申请的申请数据

PCT/AU2008/001898 2008.12.22

(87) PCT申请的公布数据

WO2009/079708 EN 2009.07.02

(71) 申请人 科库数据控股有限公司

地址 澳大利亚维多利亚墨尔本

(72) 发明人 L·E·纳斯鲍姆 S·汤普森

(74) 专利代理机构 北京北翔知识产权代理有限公司 11285

代理人 杨勇 郑建晖

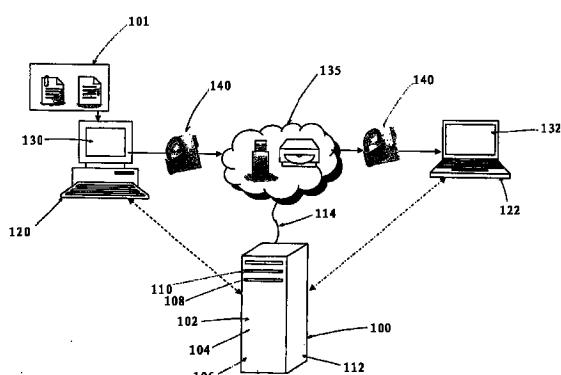
权利要求书 2 页 说明书 8 页 附图 7 页

(54) 发明名称

用于保密数据的系统和方法

(57) 摘要

本发明提供一种用于保密由第一用户分发到至少一个接收用户的数据的方法，包括以下步骤：响应来自第一用户的请求用密钥来加密数据；并把密钥的位置记录到数据库中，其中一旦数据库接收来自所述至少一个接收用户的要求授权的请求，则在所述至少一个接收用户授权后向其提供密钥。



1. 一种用于保密由第一用户分发到至少一个接收用户的 data 的方法, 包括以下步骤 :
 - 响应来自第一用户的请求用密钥来加密数据 ; 并 ,
 - 把密钥的位置记录到数据库中, 其中一旦数据库接收来自所述至少一个接收用户的要求授权的请求, 则在所述至少一个接收用户授权后向其提供密钥。
2. 根据权利要求 1 所述的方法, 包括进一步的步骤 : 数据库接收规则, 所述规则被安排以限制所述至少一个接收用户与 data 的交互。
3. 根据权利要求 1 或 2 所述的方法, 其中, 授权的步骤包括以下进一步的步骤 :
 - 将所述至少一个接收用户的标识配置文件与预定标准比较, 其中, 如果所述预定标准匹配所述标识配置文件, 则所述至少一个接收用户被授权。
4. 根据权利要求 3 所述的方法, 其中, 标识配置文件包括至少一个描述了所述至少一个接收用户的特征的标准。
5. 根据前面权利要求中任一个所述的方法, 其中, 第一用户与客户端应用程序交互, 客户端应用程序向中央源要求密钥。
6. 根据权利要求 5 所述的方法, 其中, 所述至少一个用户与至少一个接收端应用程序交互, 所述至少一个接收端应用程序被安排为向中央源要求授权以解密 data。
7. 根据前面权利要求中任一个所述的方法, 其中, 密钥由中央源和客户端应用程序两者之一产生。
8. 根据前面权利要求中任一个所述的方法, 其中, 中央源包括网闸服务器组件, 其被安排以保护服务器免受未授权用户影响。
9. 根据任意权利要求 8 所述的方法, 其中, 中央源进一步包括日志服务器组件, 其被安排以记录所述接收用户对 data 采取的任何行为。
10. 根据前面权利要求中任一个所述的方法, 其中, data 作为加密的数据串, 被包含在文件包中。
11. 根据权利要求 10 所述的方法, 其中, 所述文件包是安全文档, 其被安排为由接收端应用程序处理。
12. 根据权利要求 10 或 11 所述的方法, 其中, 为 data 对象提供安全信封, 安全信封被安排用来封入 data, 以使得当 data 在信封中时, 所述至少一个接收用户与 data 的交互被第一用户建立的规则限制。
13. 一种用于保密由第一用户分发到至少一个接收用户的 data 的系统, 包括 :
 - 被安排为响应来自第一用户的请求用密钥来加密 data 的模块 ; 和 ,
 - 被安排为把密钥的位置记录到数据库中的例程, 其中一旦数据库接收来自所述至少一个接收用户的要求授权的请求, 则在所述至少一个接收用户授权后向其提供密钥。
14. 根据权利要求 13 所述的系统, 其中, 数据库被安排以接收规则, 该规则被安排以限制所述至少一个接收用户与 data 的交互。
15. 根据权利要求 13 或 14 所述的系统, 其中, 所述例程将所述至少一个接收用户的标识配置文件与预定标准比较, 其中, 如果预定标准匹配标识配置文件, 所述至少一个接收用户被授权。
16. 根据权利要求 15 所述的系统, 其中, 所述标识配置文件包括至少一个描述了所述至少一个接收用户的特征的标准。

17. 根据权利要求 15-16 中任一个所述的系统, 其中, 第一用户与客户端应用程序交互, 客户端应用程序向中央源要求密钥。
18. 根据权利要求 17 所述的系统, 其中, 所述至少一个用户与至少一个接收端应用程序交互, 所述至少一个接收端应用程序被安排为向中央源要求授权以解密数据。
19. 根据权利要求 15-18 中任一个所述的系统, 其中, 密钥由中央源和客户端应用程序两者之一产生。
20. 根据权利要求 15-19 中任一个所述的系统, 其中, 中央源包括网闸服务器组件, 其被安排为保护服务器免于未授权用户的影响。
21. 根据任意权利要求 20 的系统, 其中, 中央源进一步包括日志服务器组件, 其被安排以记录所述接收用户对数据采取的任何行为。
22. 根据权利要求 15-21 中任一个所述的系统, 其中, 数据作为加密的数据串, 被包含在文件包中。
23. 根据权利要求 22 所述的系统, 其中, 文件包是安全文档, 其被安排为由接收端机应用程序处理。
24. 根据权利要求 22 或 23 所述的系统, 其中, 为数据对象提供安全信封, 安全信封被安排用来封入数据, 以使得当数据在信封中时, 所述至少一个接收用户与数据的交互被第一用户建立的规则限制。
25. 一种计算机程序, 包括至少一个指令, 用于控制计算机系统, 以实现根据权利要求 1 到 12 中任一个所述的方法。
26. 一种计算机可读媒介, 提供权利要求 25 的计算机程序。

用于保密数据的系统和方法

技术领域

[0001] 本发明涉及用于保密数据的系统和方法，并特别但不只涉及用于保密以电子形式发送的数据对象的系统和方法。

背景技术

[0002] 在线上环境中，电子数据常常被从一个点分发到另一个点。在有必要保密数据免受未授权使用或访问的情况下，特别在数据是机密的或要求保护的情况下，用户可以——在将数据在未受保护的网络上发送之前——使用一个系统来加密数据。

[0003] 一些用于加密数据的系统和方法是已知的。这些系统，允许用户选择数据对象，然后通过客户端的操作，用密码或其他类型的密钥（如 PIN（个人识别号码）、生物标记，等等）加密数据对象，以产生加密数据文件。然后这个数据文件对于未授权用户而言是“被保密的”，因为数据文件的内容不能被用户看到，除非该用户有正确的信息能够使该文件“公开”。当要求解密数据文件时，拥有密码的授权用户可以使用客户端解密数据文件。

[0004] 这样的系统在用户几乎没有或完全没有意愿分发加密的数据文件的情况下是有用的。在这种安排中，一旦数据对象被加密，数据对象就可以经由不安全的网络分发。然而，用户也必须找到一种方法来为已授权的人分发密码，以解密对象。常常是，为了效率的目的，密码经不安全的网络分发，自身没有任何加密。这增加了数据对象变得不安全的可能性，因为密码可以被拦截或分发到未授权的一方。

[0005] 进一步的考虑是由标准加密提供的保护等级是最小的，因为加密密钥存储在加密数据文件本身中。也就是，一旦文件被接收，黑客就拥有解密数据文件所需的所有数据。再者，若用户技术上不精通，选择了易破解的密码，意味着数据对象易于用“暴力”方法来解密。

[0006] 即使在更安全和更可靠的密码被用来加密数据对象的情况下，用户仍然不能够控制数据对象被使用的方式，因为一旦密码和数据对象已经被分发，对文件进行操作的许可会被完全转移到接收用户。例如，在用户加密数据对象，并经由国际互联网发送数据对象到另一地方的情况下，接收用户仍可能在对对象的安全没有任何考虑的情况下分发数据对象。例如，第三方可以将密码和加密数据对象一起自由分发，或移去全部加密并因此允许多个未知的用户访问数据对象。

[0007] 这些限制使用户很难安全地控制电子文件中的数据。

发明内容

[0008] 在本发明的第一方面中，提供一种用于保密由第一用户分发到至少一个接收用户的数据的方法，包括以下步骤：响应来自第一用户的请求用密钥来加密数据；并把密钥的位置记录到数据库中，其中一旦数据库接收来自所述至少一个接收用户的要求授权的请求，则在所述至少一个接收用户授权后向其提供密钥。

[0009] 在一个实施方案中，提供进一步的步骤：数据库接收规则，该规则被安排以限制所

述至少一个接收用户与数据的交互。

[0010] 在一个实施方案中,授权的步骤包括以下进一步的步骤:将至少一个接收用户的标识配置文件(identification profile)与预定标准比较,其中,如果所述预定标准匹配所述标识配置文件,则所述至少一个接收用户被授权。

[0011] 在一个实施方案中,标识配置文件包括至少一个描述了所述至少一个接收用户的特征的标准。

[0012] 在一个实施方案中,第一用户与客户端应用程序交互,客户端应用程序向中央源要求密钥。

[0013] 在一个实施方案中,至少一个用户与至少一个接收端应用程序交互,所述至少一个接收端应用程序被安排为向中央源要求授权以解密数据。

[0014] 在一个实施方案中,密钥由中央源和客户端应用程序两者之一产生。

[0015] 在一个实施方案中,中央源包括网闸服务器组件,其被安排为保护服务器免受未授权用户影响。

[0016] 在一个实施方案中,中央源进一步包括日志服务器组件,其被安排以记录接收用户对数据采取的任何行为。

[0017] 在一个实施方案中,数据作为加密的数据串,被包含在文件包中。

[0018] 在一个实施方案中,文件包是安全文档,被安排为由接收端应用程序处理。

[0019] 在一个实施方案中,为数据对象提供安全信封,安全信封被安排用来封入数据,以使得当数据在信封中时,所述至少一个接收用户与数据的交互被第一用户建立的规则限制。

[0020] 在本发明的第二方面中,提供一种用于保密由第一用户分发到至少一个接收用户的数据的系统,包括:被安排为响应来自第一用户的请求用密钥来加密数据的模块;和,被安排为把密钥的位置记录到数据库中的例程,其中一旦数据库接收来自所述至少一个接收用户的要求授权的请求,则在所述至少一个接收用户授权后向其提供密钥。

[0021] 在第二方面的一个实施方案中,数据库被安排以接收规则,该规则被安排以限制所述至少一个接收用户与数据的交互。

[0022] 在第三方面的一个实施方案中,提供一种计算机程序,包括至少一个用来控制计算机系统以实施本发明第一方面的方法的指令。

附图说明

[0023] 现在仅通过举例方式参考附图,描述本发明的实施方案。在附图中:

[0024] 图1是依照本发明的一个实施方案的系统的方块图;并且

[0025] 图2是依照图1实施方案的系统的一个方面的操作的流程图;并且

[0026] 图3是依照图1实施方案的系统的第二方面的操作的流程图;并且

[0027] 图4是图解了图1的实施方案的多个服务器组件的方块图;并且

[0028] 图5是依照本系统实施方案的文件包的实施例;并且

[0029] 图6是图解说明依照本系统实施方案的安全数据对象的实施例;并且

[0030] 图7是图解说明依照本系统实施方案的安全数据对象的另一个实施例。

具体实施方案

[0031] 参考图 1, 本发明的一个实施方案被安排以提供用于保密数据的系统, 该系统包括中央源 100, 其被安排以响应来自第一用户的请求用密钥来加密数据, 该系统还包括授权服务器组件——其被安排以接收授权请求, 并且一旦接收用户被授权, 则将接收用户引导至该密钥, 以解密数据。

[0032] 在这个实施方案中, 依照本发明的这个实施方案的系统和方法和相关的软件和 / 或硬件应用程序可以在诸如图 1 中所示出的示例设备上执行。在图 1 中, 示出中央源的示意图, 在这个实施方案中, 中央源是适合用于本发明的实施方案的服务器 100。服务器 100 可以用于执行应用程序和 / 或系统服务, 所述应用程序和 / 或系统服务如本发明的实施方案的用以保密数据的系统和方法。

[0033] 参见图 1, 服务器 100 可以包括接收、存储和执行合适的计算机指令所需的适当组件。这些组件包括处理器 102, 只读存储器 (ROM) 104, 随机存取存储器 (RAM) 106, 输入 / 输出设备例如磁盘驱动器 108、输入设备 110 (如以太网接口, USB 接口, 等等)、显示器 112 例如液晶显示器、发光显示器或任何其他适合的显示器, 和通信链路 114。服务器包括可以安装在 ROM 104、RAM 106 或磁盘驱动器 108 中且可以由处理器 102 执行的指令。可以提供多个通信链路 114, 其各自与一个或多个计算设备例如服务器、个人计算机、终端、无线或手持计算设备等连接。通过电话线或其他类型的通信链路, 多个通信链路中的至少一个可以与外部计算网络连接。

[0034] 在一个具体的实施方案中, 设备可以包括存储设备, 例如磁盘驱动器 108, 其可以包含固态驱动器、硬盘驱动器、光驱动器或磁带驱动器。服务器 100 可以使用单个磁盘驱动器或多个磁盘驱动器。服务器 100 也可以使用适合的操作系统 116, 其存在于服务器 100 的磁盘驱动器上或 ROM 中。

[0035] 在一些实施方案中, 第一用户使用计算机 120 执行客户端应用程序 130。在一个实施例中, 计算机可以是使用 Intel/AMD 芯片组, 具有如 WindowsTM、MAC OSTM 或 Linux 操作系统或者是本领域技术人员注意到的操作系统的个人计算机, 计算机可以是被安排用于执行计算功能的移动设备, 例如, PALMTM 或 IPAQTM 设备。

[0036] 在这个实施方案中, 客户端应用程序是用任何计算机语言实现的软件程序, 其被安排为存在计算机 120 的存储设备上。客户端应用程序 130 的实现的其他实施例是可行的, 其中包括, 但不仅限于存储在 ROM、可编程阵列、光驱、智能卡、存储单元、永久性记忆模块中的计算指令。在一个实施例中, 客户端应用程序 130 具有为用户安排的用于引导任何输入或输出的接口, 或者, 在其他实施例中, 客户端应用程序与已存在的软件或操作系统应用程序——例如但不限于 Open OfficeTM 或 Microsoft OfficeTM——嵌在一起, 且因此将附加的功能添加到这些软件中。

[0037] 客户端应用程序 130 有通信端口, 其被安排以和服务器 100 通信。当用户启动应用程序 130 时, 应用程序 130 经由安全连接, 如 SSL 或 SSH 连接, 与服务器 100 接触。在一个实施例中, 该应用程序发送自身唯一的识别码, 或 I P 地址或其他信息, 以便服务器 100 能够识别该用户和用户在其中进行操作的计算机 120。这使服务器 100 能够控制系统在保密数据方面的安全性——通过, 在支持客户端应用程序 130 和服务器 100 之间的通信会话之前, 实现对这种通信会话的授权。

[0038] 在一些实施方案中,参照图 2,第一用户使用客户端应用程序 130 来选择要求加密的数据 (202)。数据可能以文件 101、地址、指针或对象的形式存在。通过使用接口,第一用户能够拖放或指向和选择需要的数据,一旦文件被选择,客户端应用程序 130 能够开始为保密数据而所需的保密过程。

[0039] 在此处描述的实施方案中,保密过程开始于封装数据 (204),以创建数据对象,从而使得所有的数据(以文件、对象、地址、指针或任何组合存在)可以被集成并被认为是单个安全数据对象 140。一旦安全数据对象 140 被创建,则安全数据对象 140 随后被用户描述,此处用户可以指定权限或规则来描述对象 (206)。权限或规则被安排以控制数据对象 140 被交互或被操作的方式。在一个实施例中,权限可以要求安全数据对象 140 中的数据文件是只读的或仅可以打印的。在另一个实施例中,权限或规则可以包括,在任何具体 IP 地址范围内使用特定类型计算机的何等级别的用户能够访问文件。

[0040] 一旦权限已经被第一用户设定,客户端应用程序 130 向第一用户提供建立访问控制列表 (208) 的功能,该列表列出了被授权为接收和与安全数据对象 140 交互的接收用户。在一个实施例中,访问控制列表也可以限定为鉴别接收用户所需的鉴别机制。例如,该机制可以要求接收用户正通过具有特定识别码的计算机来操作,或者用户正操作特定的本地网络,或者该接收用户已经被一些形式的生物特征扫描认可。本领域的技术人员也会注意到其他鉴别接收用户的变体方式。

[0041] 在这个实施方案中,当访问控制列表建立时,客户端应用程序 130 开始加密过程 (210)。在一个实施例中,加密过程使用 AES(高级加密标准)、或美国联邦信息处理标准 (FIPS)(例如参见 ‘<http://www.nist.gov/aes>’) 或其他本领域的技术人员可以注意到的加密方法。为启动加密过程 (210),客户端应用程序 130 可以自己产生用于加密的密钥,或者在其他实施例中,从服务器 100 中获取密钥。在加密过程中,密钥没有和数据对象 140 一同加密,因此任何加密的安全数据 140 中均将不含有密钥。这提供了较的程度的保护,因为密钥不在安全数据对象 140 中,希望解密安全数据对象 140 的黑客不能利用暴力方法等方法解密安全数据对象 140。加密安排设置了只有拥有从与安全数据对象 140 分立的且独立的源中提取的密钥的用户才可以解密安全数据对象 140。

[0042] 当完成加密过程 (210) 后,客户端应用程序 130 将返回完全加密的安全数据对象 140 (212)。在一个实施例中,通过把加密的数据文件放在文件包 500 中来创建安全数据对象 140,这可以用 XML 或其他适合的计算机语言完成。在此实施例中,图 5 中示出的文件包 500 提供元数据 502 来描述安全数据对象 140,以致当对象被接收者或用户的客户端应用程序打开时,应用程序被告知一些与安全数据对象 140 相关的信息,以对这里所描述的保密过程进行支持。安全数据对象作为文件存储在计算机 120 上的存储器或存储设备中。第一用户可以有经分布通道 135 分布对象的权利,通道 135 的形式有电子邮件、FTP、SSH、存储器、CD、USB 设备、永久性存储器或其他电子形式。

[0043] 在一个实施方案中,存在于接收用户计算机 122 上的接收端应用程序 132 被安排解密安全数据对象 140。当获得安全数据对象 140 后,接收用户启动接收端应用程序 132,在一个实施例中,接收端应用程序可以集成到电子邮件软件中,并因此而在安全数据对象 140 经由电子邮件被接收时,自动启动。参考图 3,接收端应用程序与服务器 100 通信,并建立与服务器 100 的安全连接 (302)。服务器 100 开始授权过程 (304),由此,在一个实施例中,接

收端应用程序 132 发送识别码到服务器,以使得接收用户被识别。

[0044] 在一个实施例中,接收用户被要求输入足以被鉴别的细节。鉴别方法是那些当安全对象 140 被创建时已经被第一用户限定的方法,且如上文所限定的,这些方法可以涉及生物特征扫描、密码、问题、或本领域技术人员可以注意到的其他形式的鉴别方法。

[0045] 在成功鉴别接收用户 (304) 后,接收端应用程序 132 向服务器 100 请求由第一用户许可给接收用户的与一些具体权利有关的权限和访问权限 (306)。一旦接到这些权利,接收用户被限制仅以第一用户限定的权限和规则交互。在一些实施例中——其中接收用户仅被允许查看安全数据对象 140 之内的数据文件——浏览器被接收端应用程序 132 启动。浏览器被安排为仅显示文件,并拒绝接收用户去编辑文件的任何尝试。

[0046] 在这个实施方案中,接收端应用程序 132 开始解密过程 (308),首先向服务器 100 请求被引导至解密密钥,该密钥是用于加密安全数据对象的密钥。服务器 100 可在服务器中存储密钥,在这种情况下,密钥被传送到接收端应用程序 132。然而,在一些实施例中,密钥可以存储在位于不同位置的分立的服务器中,并相应地,服务器 100 仅向接收端应用程序 132 发送从该分立的服务器获得密钥的指示。在另一个实施例中,密钥可以存储在不同的存储介质中,例如智能卡或 USB 锁或 CD ROM,在这种情况下,服务器 100 向接收端应用程序发送指示,指导用户寻找包含密钥的相关存储介质。

[0047] 在成功获得密钥 (308) 后,接收端应用程序 132 解密安全数据对象 (310) 并将数据发送到接收用户,所述接收用户受限于已经由第一用户所安排的权限和规则建立的限制 (312)。接收用户对数据的每个操作或交互被记录,并且日志返回到服务器 100 以供存储和查看 (314)。

[0048] 参考图 4,在一些实施方案中,服务器 100 包括一些服务器组件,包括,但不仅限于;

- [0049] • 网闸服务器组件 410 ;
- [0050] • 授权服务器组件 412 ;
- [0051] • 管理服务器组件 414 ;
- [0052] • 身份服务器组件 416 ;
- [0053] • 数据库服务器组件 418 ;和,
- [0054] • 备份服务器组件 419。

[0055] 这些服务器组件中的每一个可以被配置在单个服务器上,或者在图 4 所示的实施例中作为服务器 100 中以计算机语言、机器码或 ROM 实现的计算机软件而存在,用以提供这些服务器组件中的每一个的功能。这些服务器组件均被安排与其他服务器组件通信并被组合以提供服务器 100,以提供依照本发明的一个实施方案的用于保密数据的系统和方法。

[0056] 在这里描述的实施方案中,当客户端应用程序或接收端应用程序在与服务器 100 通信时,网闸服务器组件 410 启动应用程序 (130, 132) 与服务器 100 之间的会话。一旦被初始化,网闸服务器组件 410 引导所述应用程序连接到鉴别服务器组件 412,以鉴别用户。

[0057] 通过引导所有的初始连接经过网闸服务器组件 410,进一步增强了服务器上安全性,因为网闸服务器组件 410 进一步被安排为过滤掉可能损害服务器组件 400 的安全性的恶意和 / 或列入黑名单的网络连接。本领域的技术人员可以理解,可以实施许多网闸服务器组件 410 得以实施的变体,所述变体包括,但不限于能分析即将到来的通信的硬件和 / 或

软件防火墙服务器组件。

[0058] 如果用户计算机 120、122 和服务器 100 之间的连接满足网闸服务器组件 410 的要求，则鉴别服务器组件 412 会试图检验和授权该用户。这首先涉及服务器组件从身份服务器组件 416 获取一些记录，身份服务器组件 416 存储识别标志，包括但不限于用户配置文件、用户鉴别手段、密码等等。在读出数据之后，用户，不论是第一用户还是接收用户，必须被鉴别以继续对服务器 100 的访问。在一些实施例中，鉴别服务器组件 412 可以要求用户输入密码、配置文件细节或可以检测用户 ID、IP 地址、计算机识别码、生物特征验证或其他能够和身份服务器组件 416 中的数据交叉参照的内容，以鉴别和授权客户端会话，以使得用户可以继续访问服务器组件 400。

[0059] 一旦成功完成鉴别过程，服务器 100 就能够继续前进到为客户端应用程序 130 或接收端应用程序 132 处理任何请求，以便提供此处描述的保密数据的系统和方法。如果创建安全数据对象 140 的第一用户已经选择包括一些权限或规则去限制接收用户与安全数据对象交互和操作安全数据对象的方式，管理服务器组件 414 提供使这些权限和规则可以被输入、存储和执行的功能。

[0060] 在这个实施方案中，管理服务器组件 414 允许客户端应用程序 132 输入和存储至少一个会限制接收用户对数据对象的后续使用的权限。管理服务器组件具有一个接口，对客户端应用程序 130 开放，指向第一用户创建的安全数据对象。在接口的一个实施例中，第一用户可以从权限列表中进行选择，以描述安全数据对象 140。这些规则包括，但不限于：

- [0061] - 数据对象的读、写、打印权限；和，
- [0062] - 数据对象的拷贝权限；和，
- [0063] - 数据对象的分享权限；和，
- [0064] - 数据对象的重分配；和，
- [0065] - 允许访问数据对象的特定时间段；和，
- [0066] - 允许访问数据对象的人或人群；和，
- [0067] - 允许备份数据对象的人、或环境；和，
- [0068] - 允许访问数据对象的计算机的位置，包括计算机的网络位置或地理位置。

[0069] 一旦规则被第一用户建立，用户能够选择经由接口保存规则。用户可以选择触发数据库服务器组件 418 的提交按钮或开关，以将关于安全数据对象 418 的规则和权限记录到数据库中。数据库，如本领域技术人员可以理解的，包括，但不限于，关系数据库管理系统 (RDBMS)（例如 Oracle™ 或 Microsoft Access™），面向对象数据库系统、平面文件 (flat file) 或其他文件结构。一旦这些规则和权限被写入数据库，当接收用户获得对相关的安全数据对象的访问时，这些规则和权限可以被获取。

[0070] 系统的操作可以参考图 2 和 3 所概括的过程来描述。首先，第一用户准备和选择要求被加密和分发的数据。在一个实施例中，数据可以是一个或多个数据文件，其包括文档、电子数据表、电子邮件、文本、图表、多媒体或其他形式的计算机数据。选择数据后，第一用户开启客户端应用程序 130，在一个实施例中，客户端应用程序作为软件应用程序运行在第一用户的计算机上 (202)。一旦应用程序被初始化，客户端模块接触服务器 100，其中网闸服务器组件执行一系列的检验，以确认连接的完整 (203)。一旦网闸服务器组件 410 允许该连接，授权服务器组件 412 被运行，以鉴别该用户，从而使得该用户可以被识别为安全对象

的已授权创作者。当用户通过匹配授权服务器组件的要求（例如，输入密码、密钥或生物特征扫描）而被授权后，客户端应用程序继续保持与服务器 100 的连接并允许用户加入要求加密的数据文件以形成安全数据对象。在一些实施例中，用户可以将一个或多个文件拖进客户端应用程序 132 的接口并选择关闭数据对象，以使文件接着被结合形成单个数据对象 (202)。

[0071] 在这个实施方案中，第一用户被引向服务器的管理服务器组件 414，由此，第一用户被给予描述数据对象 140 被接收用户操作的方式的机会。在一个实施例中，第一用户访问接口，并被提供各种规则和权限，以便控制数据对象被操纵的方式。这些操纵的一些实施例之前已经描述了。规则和权限被接收端应用程序 132 执行，该接收端应用程序被接收用户用于访问安全数据对象 140。一旦输入和选择规则和权限，用户可以选择触发经由服务器 100 的数据库服务器组件而被写入数据库的规则的提交开关或按钮。在权限被写入数据库的该实施例中，权限以访问控制列表 (ACL) (208) 的形式写入，该访问控制列表然后由服务器 100 的数据库服务器组件 418 存放回。

[0072] 一旦完成数据文件或对象的权限和规则的选择，用户可以加密对象 (210)。在一个实施例中，客户端应用程序 130 随后创建密钥，以加密数据，形成安全数据对象。加密过程保证密钥不嵌入进安全数据对象中，从而使安全对象自身不会以任何形式暴露加密密钥。在另一个实施例中，客户端应用程序 130 从服务器 100 请求密钥，该服务器产生适合于数据加密的随机密钥。用户可以选择在服务器 100 上存储密钥还是把密钥存储在其他地方，但指示服务器 100 密钥被存储在何处，以便将授权的接收用户引向密钥。这种安排减少了存储在服务器 100 上密钥的数量，从而将安全漏洞的危险分散到其他服务器。在这个过程中，黑客在找相关密钥方面会有额外的困难，因为所述位置不是直接被任何未授权的用户所知。

[0073] 一旦客户端应用程序已经加密了第一用户选择的数据；安全数据对象由客户端应用程序 130 形成。一旦加密过程 (210) 完成，安全数据对象 140 已准备好经分布通道 135 由任意数量的接收用户采用。在一些实施例中，第一用户可以仅把安全对象用电子邮件发送到单个或多个接收者，或者可以把对象分布在压缩磁盘上、通用串行总线 (USB) 锁或其他计算机可读媒介。本安排的一个直接优势是允许用户经过任意不安全通道分布安全对象，因为黑客会发现，在没有找到密钥来解密数据对象的同时，来破解安全数据对象 140 是非常困难的。因为安全数据对象 140 已经以加密密钥不在安全数据对象 140 内的方式被加密，因此安全数据对象 140 很难被解密。

[0074] 安全数据对象被接收用户接收后，接收用户开启之前所描述的接收端应用程序 132，并加载安全数据对象 140 到接收端应用程序 132 中。在一些实施例中，这可以涉及选择安全数据对象 140 并拖放到接收端应用程序 132 提供的接口中。在其他实施例中，接收端应用程序可以集成到存在的软件包，例如，Microsoft Word™、Excel™、PowerPoint™、Access™、Internet Explore™ 或其他类似的软件包，之内。在成功加载安全数据对象 140 后，当接收端应用程序 132 连接到 100 时，接收用户被中央服务器 100 鉴别。鉴别可以是提供物理智能卡、USB 锁、生物特征数据、密码、位于用户计算机上的唯一用户 ID、IP 地址或任何组合，其中的任意一种，或其他可提供的确认技术。在接收用户成功授权和鉴别后，接收端应用程序 132 会与服务器 100 通信，并被引向访问解密密钥。解密密钥可以存储在服务器 100 上。

但是,在一些情况中,服务器仅存储指针,指针指向保存密钥的相关的分立位置。在一个实施例中,可将解密密钥存储在随后的相对于安全数据对象分立分布的智能卡中。无论如何,中央服务器 100 会引导接收用户到适合的位置,以获取解密密钥。这可能需要接收用户一方有一些额外的动作,例如访问分立的服务器或定位含有密钥的物理媒介(例如,向计算机 122 插入智能卡)。一旦成功获得解密密钥,接收端应用程序 132 就可以解密安全数据对象 140 并允许用户在一些权限和规则的限制下操作安全数据对象 140,所述权限和规则可以是已经被第一用户设置好的权限和规则。在一个实施例中,第一用户已经限制接收用户对安全数据对象内的已经被加密的一个文档的编辑能力,接收用户不能对文档做出或保存任何修改,而仅限于读、访问和打印文档。

[0075] 在可替代的实施方案中,安全数据对象可以作为图 6 所示的安全信封存在。在安全数据对象是安全信封 600 的情况下,信封作为文件被存储,该文件将存储在安全信封 600 中的各数据文件 602 封入。信封完全在前面描述的安全数据对象系统的保护下。然而,一旦信封内的文件被拖出,并从安全信封中移走,并到达用户计算机接口(例如,桌面或他们自身的文件系统)上,现有系统 610 施加的控制和保护即被撤销,允许接收用户完全与数据文件交互和操作数据文件,一如该接收用户拥有文件的买断权(outright)605 时所允许的。在这个实施例中,第一用户可以创建权限,以保证接收用户不能从安全信封中移走任何数据文件。

[0076] 在安全数据对象作为安全文档 700 存在的其他实施方案中,数据文件本身使用参考图 7 所描述的系统和方法加密。在这个情况中,整个文件 702 必须只能经客户端应用程序访问,并且,除非另外允许的,其不能被接收用户分发或完整拷贝。

[0077] 有利的是,所描述的实施方案,不以任何方式与加密的数据交互。换句话说,将要加密的数据不再“经过”或存储在中央源。这种安排消除了提供会吸引黑客的数据的中央枢纽(centralized hub)的危险。

[0078] 在一些实施方案中,系统作为服务器组件被提供给网络上或在线接口上的用户。在这个实施方案中,提供给用户下载和允许应用程序 130 的权限,以依照已经提到的步骤,加密或解密数据对象。该许可可以限制应用程序 130 的功能。在一个实施例中,自由许可会限制应用程序 130 仅解密文件,但是一旦付款,则许可可以延伸到允许应用程序 130 加密文件。在其他实施例中,许可可以限制可以加密或解密的文件的类型并从而限制用户只能访问特定的文件。这个实施例在整体或集体环境中特别有效,这里每个用户可以被授予不同的许可,以对特定数据对象加密或解密。

[0079] 尽管没有要求,这里参考图描述的实施方案可以经由应用程序程序接口(API)来实施或作为供开发人员使用的一系列函数库,来实施,并可以被包括在别的软件应用程序,例如终端或个人计算机操作系统或手持计算设备操作系统,之中。一般来说,程序模块包括例程、程序、对象、组件和执行或支持特定功能的执行的数据文件,可以理解,软件应用程序的功能可以在一些例程、对象或组件上分解,以获得与实施方案和此处所要求保护的更宽的发明相同的功能。这些改变和修改是在本领域技术人员的眼界范围内的。

[0080] 可以理解,在本发明的方法和系统由计算系统实施或部分由计算系统实施的情况下,可以采用任何适合的计算系统结构。这会包括独立计算机、网络计算机和专用计算设备。术语“计算系统”和“计算设备”被使用,而且这些术语用于覆盖任何合适的可以实施上述功能的计算机硬件安排。

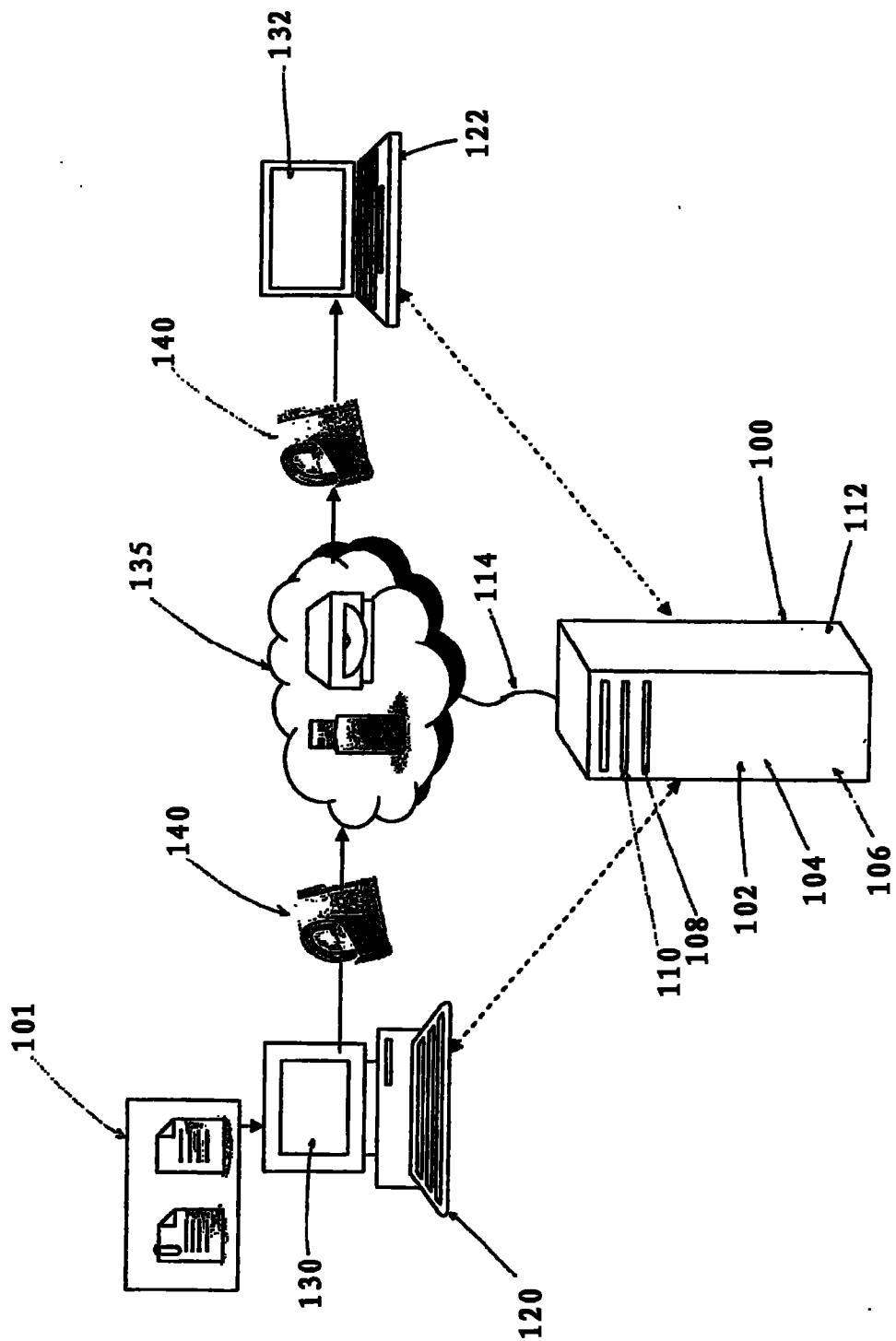


图 1

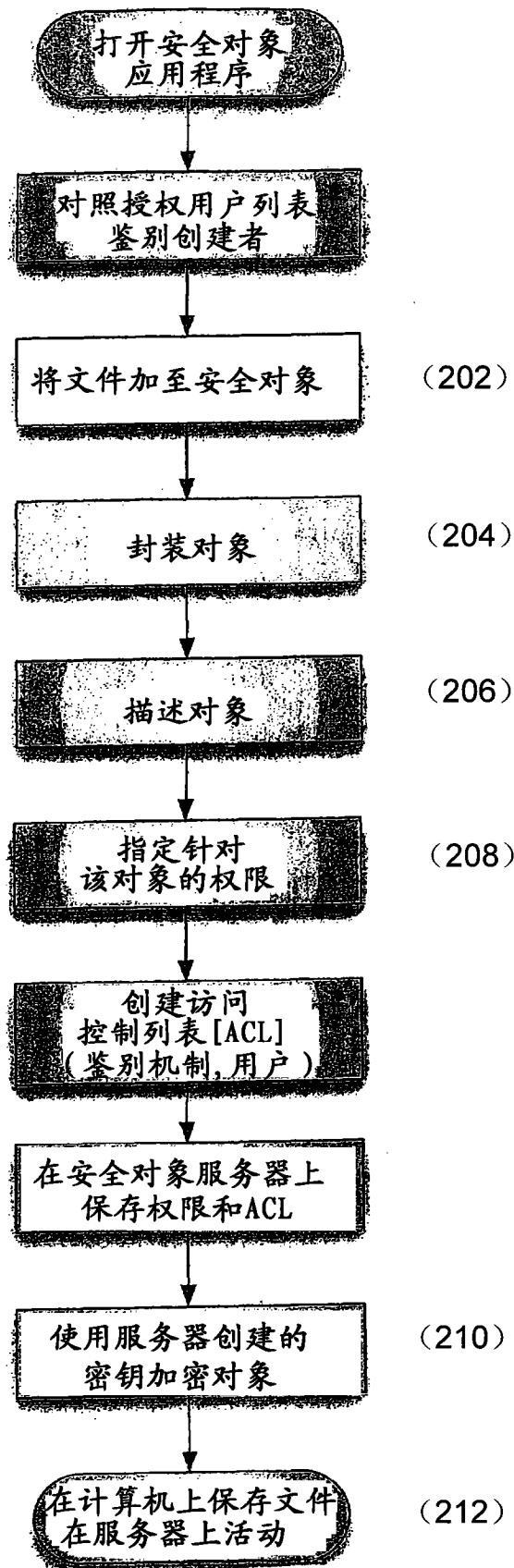


图 2

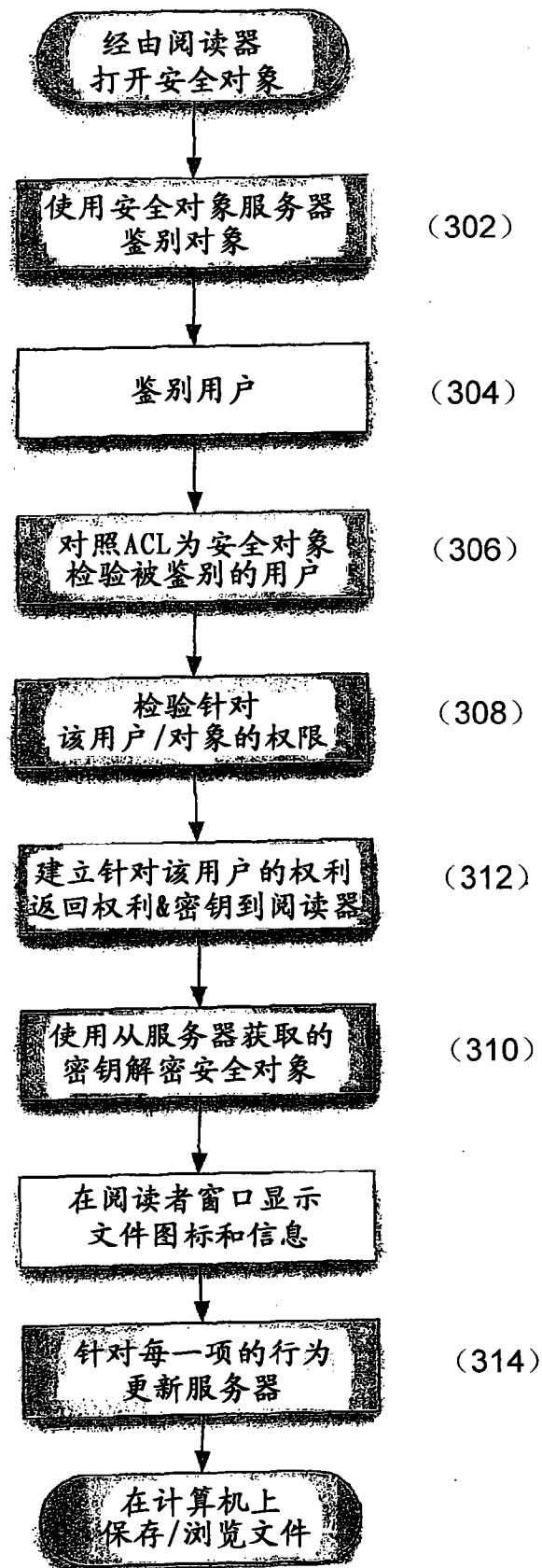


图 3

面向公共服务器组件 私有服务器组件

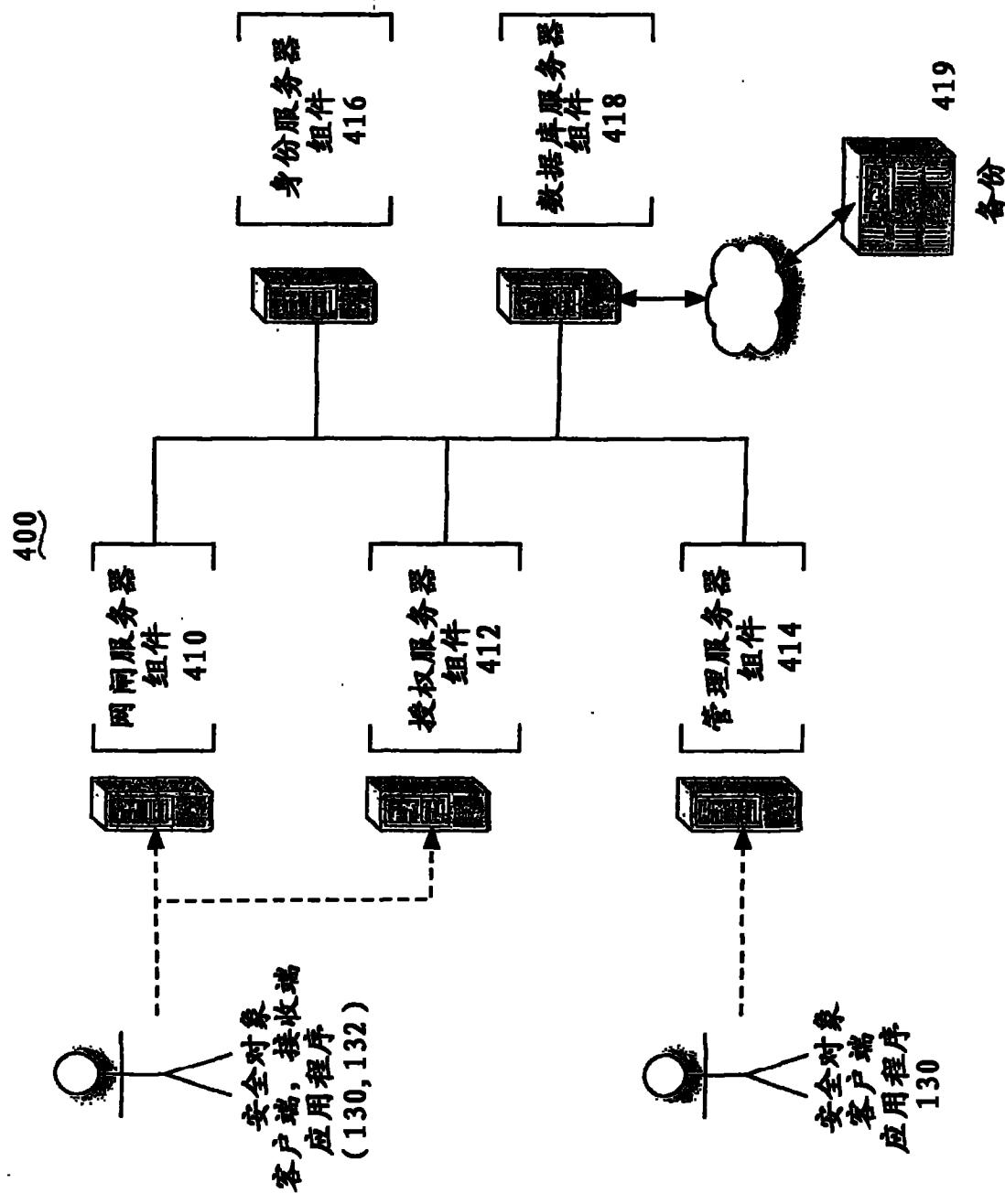


图 4

500

```
<?xml version="1.0" encoding="utf-8"?>
<secobj version="1">
    <!-- This is a Cocoon Data Secure Envelope.
        For more information visit www.cocoondata.com -->
    <header>
        <doc>SVRID-1234-5678-9012-3456-7890</doc>
        <server id="ENCRYPTED://gatekeeper.cocoondata.com">
            gatekeeper.cocoondata.com
        </server>
        <title>title</title>
        <desc>document description</desc>
        <author>document author name</author>
        <date>document creation date</date>
        <hash>header hash code</hash>
    </header>
    <manifest version="1">
        <file type="ext" size="####" date="YYYY-MMM-DD HH:MM:SS">
            [System File Name & Extension]
        </file>
        <file type="ext" size="####" date="YYYY-MMM-DD HH:MM:SS">
            [System File Name & Extension]
        </file>
    </manifest>
    <content bytes="#####">...ASCII encoded binary data...</content>
</secobj>
```

502

140

图 5

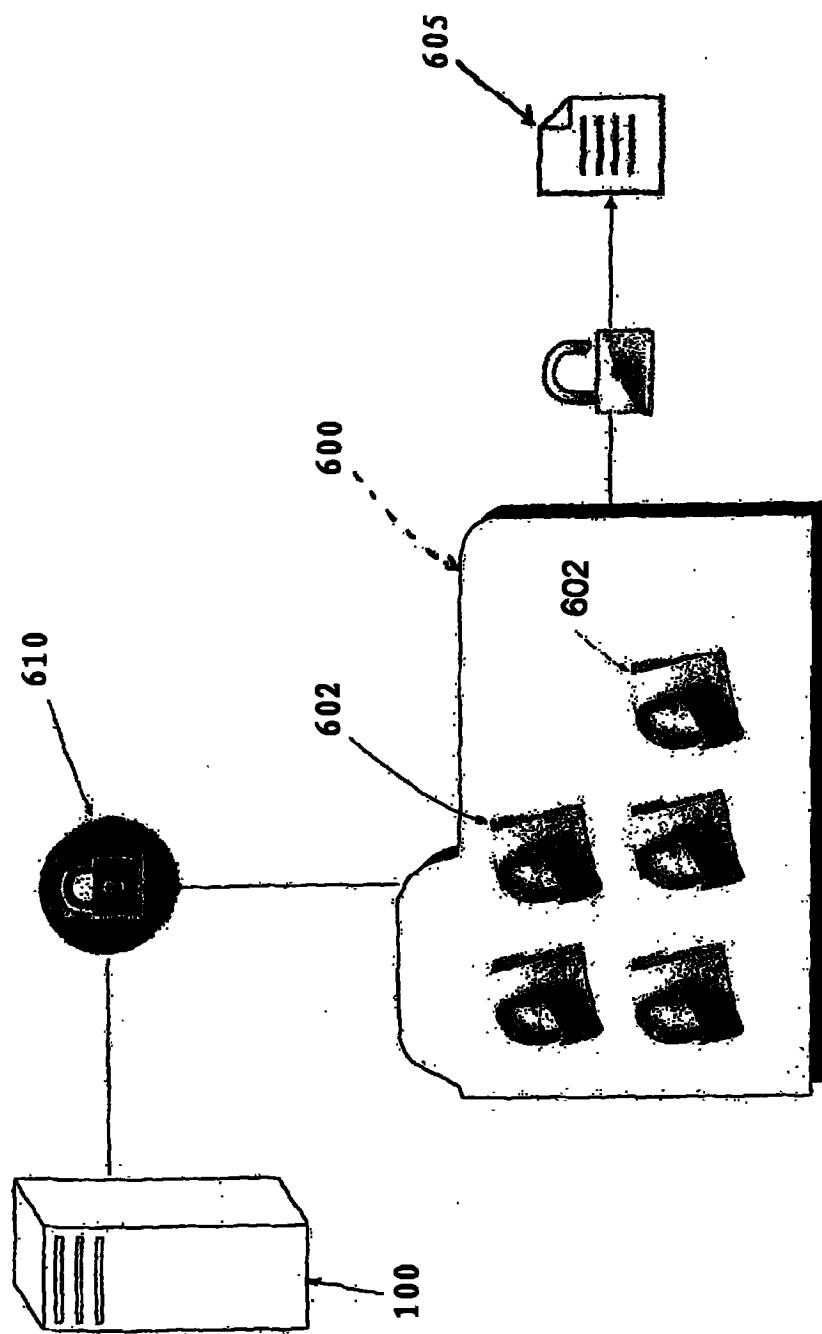


图 6

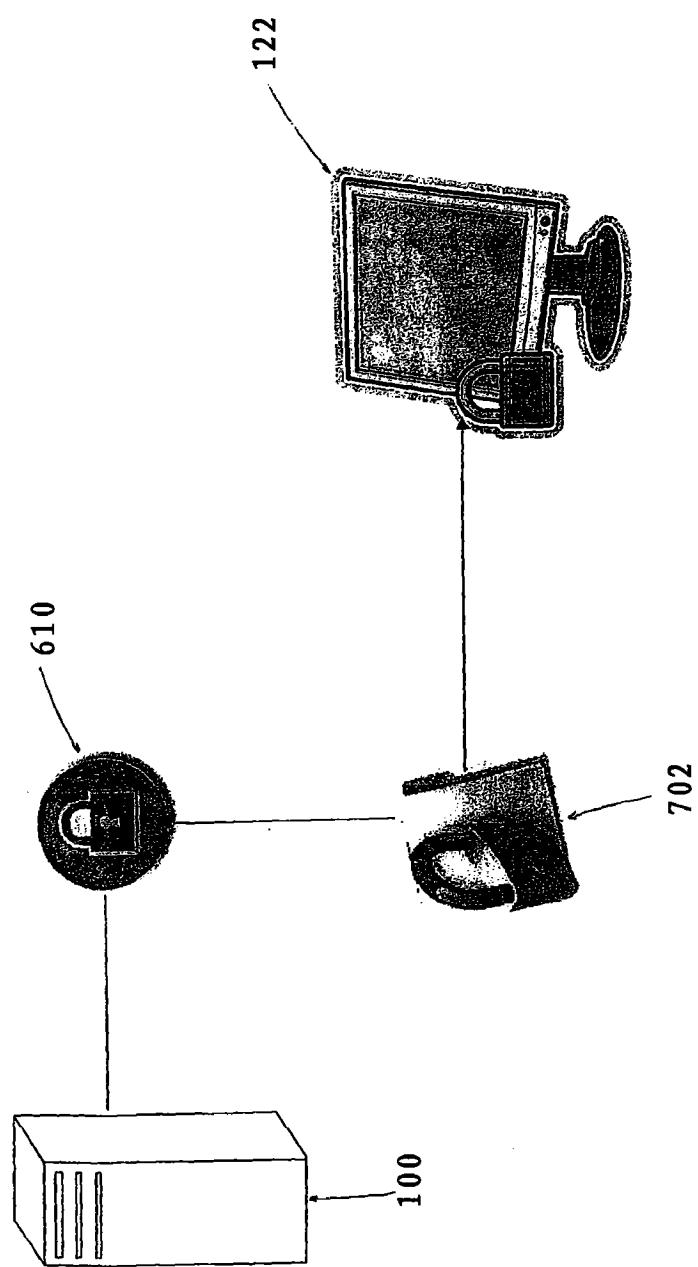


图 7