[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 11/30 (2006.01)
G06F 12/14 (2006.01)
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 03822497.6

[45] 授权公告日 2008 年 4 月 9 日

[11] 授权公告号 CN 100380337C

[22] 申请日 2003.8.9 [21] 申请号 03822497.6

[30] 优先权

[32] 2002. 8. 9 [33] US [31] 60/402,287

[86] 国际申请 PCT/US2003/025795 2003.8.9

[87] 国际公布 WO2004/015576 英 2004.2.19

[85] 进入国家阶段日期 2005.3.21

[73] 专利权人 威斯托公司

地址 美国加利福尼亚州

[72] 发明人 丹尼尔·门德斯 梅森·NG

[56] 参考文献

US4882752 1989.11.21

US5150407A 1992.9.22

US5265159A 1993.11.23

US6151606A 2000.11.21

审查员 李 佳

[74] 专利代理机构 北京中安信知识产权代理事务所

代理人 张小娟

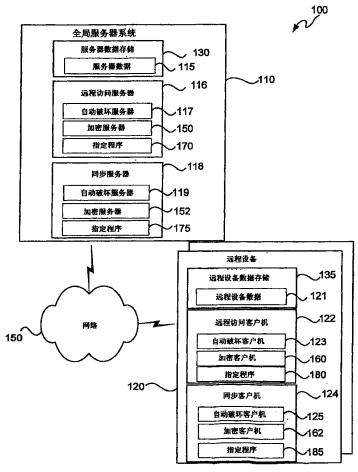
权利要求书 5 页 说明书 33 页 附图 11 页

[54] 发明名称

用于阻止访问被破解的远程设备上的数据的系统和方法

[57] 摘要

本发明揭露一种系统(100)和方法，其用于当远程设备被破解或管理远程设备(120)的漫游用户的权限级别被更改时，选择性地擦除、加密和或复制远程设备(120)上的数据(121)。



1、一种在远程设备和网络设备之间同步安全数据的方法，包括:

在服务器接收远程设备被破解的指示，服务器与远程设备交换数据;

从所述远程设备选择至少一个数据子集进行同步；以及

从服务器响应指示、传输指令到所述远程设备，所述指令为阻止从远程设备访问所述至少一个进行同步的数据子集。

2、如权利要求 1 所述方法，其中所述指令包括擦除所述至少一个进行同步的数据子集。

3、如权利要求 1 所述方法，其中所述指令包括加密所述至少一个进行同步的数据子集。

4、如权利要求 1 所述方法，其中所述指令还为传输所述至少一个数据子集到另一个位置。

5、如权利要求 1 所述方法，其中所述至少一个进行同步的数据子集包括非同步数据。

6、如权利要求 1 所述方法，其中所述至少一个进行同步的数据子集包括个人数据。

7、如权利要求 1 所述方法，其中所述至少一个进行同步的数据子集包括应用程序。

8、如权利要求 1 所述方法，进一步包括：从服务器响应所述指示传输断开指令到所述远程设备，所述指令为防止所述远程设备与网络之间的连接，使得服务器中止对于至少一个进行同步的数据子集的进一步通讯。

9、如权利要求 1 所述方法，其中所述指示由所述远程设备传输。

10、如权利要求 1 所述方法，其中所述至少一个进行同步的数据子集包括所述远程设备上的所有数据。

11、一种在远程设备和网络设备之间同步安全数据的网络系统，包括：

一程序文件，说明用于阻止远程设备上至少一个进行同步的数据子集被访问的方法；以及

一服务器，通信地连接到所述程序文件和所述远程设备，能够接收远程设备被破解的指示，从所述远程设备选择至少一个进行同步的数据子集，以及传输指令到所述远程设备，所述指令为根据所述程序文件阻止访问所述至少一个进行同步的数据子集。

12、如权利要求 11 所述的系统，其中所述指令包括擦除所述至少一个进行同步的数据子集。

13、如权利要求 11 所述的系统，其中所述指令包括加密所述至少一个进行同步的数据子集。

14、如权利要求 11 所述的系统，其中所述指令还为传输所述至少一

个进行同步的数据子集到另一个位置。

15、如权利要求 11 所述的系统，其中所述至少一个进行同步的数据子集包括非同步数据。

16、如权利要求 11 所述的系统，其中所述至少一个进行同步的数据子集包括同步数据。

17、如权利要求 11 所述的系统，其中所述至少一个进行同步的数据子集包括个人数据。

18、如权利要求 11 所述的系统，其中所述至少一个进行同步的数据子集包括应用程序。

19、如权利要求 11 所述的系统，其中所述服务器进一步能够响应指示，传输断开指令到所述远程设备，所述指令为防止所述远程设备与网络之间的连接，使得服务器中止对于至少一个进行同步的数据子集的进一步通讯。

20、如权利要求 11 所述的系统，其中所述指示由所述远程设备传输到所述服务器。

21、一种在远程设备和网络设备之间同步安全数据的系统，包括:

在服务器用于接收远程设备被破解的指示的装置，服务器与远程设备交换数据;

用于从所述远程设备中选择至少一个进行同步的数据子集的装置；以及

用于从服务器答复指示传输阻止访问所述至少一个从远程设备进行同步的数据子集的指令的装置。

22、一种系统，包括：

一数据跟踪器，能够跟踪远程设备上数据位置和类型；以及

一客户机，通信地连接到所述数据跟踪器，当所述远程设备被破解时能够接收阻止访问所述远程设备上至少一个数据子集指令，以及根据所述数据跟踪器产生的信息执行阻止访问所述至少一个数据子集的所述指令。

23、如权利要求22所述的系统，其中所述指令包括擦除所述至少一个数据子集。

24、如权利要求22所述的系统，其中所述指令包括加密所述至少一个数据子集。

25、如权利要求22所述的系统，其中所述客户机进一步能够：

在所述远程设备接收指令，所述指令为传输所述至少一个数据子集到另一个位置；以及

传输所述至少一个数据子集到另一个位置。

26、如权利要求22所述的系统，其中所述至少一个数据子集包括非同步数据。

27、如权利要求22所述的系统，其中所述至少一个数据子集包括同步数据。

28、如权利要求22所述的系统，其中所述至少一个数据子集包括个人数据。

29、如权利要求22所述的系统，其中所述至少一个数据子集包括应用程序。

30、如权利要求22所述的系统，进一步包括一远程设备切断装置，其能够：

在所述远程设备接收指令，所述指令为切断所述远程设备与网络之间的连接；以及

切断所述远程设备与所述网络之间的所述连接。

31、如权利要求22所述的系统，其中所述至少一个数据子集包括所述远程设备上的所有数据。

用于阻止访问被破解的远程设备上的数据的系统和方法

交互参考

本申请依照 35 U. S. C. § 119 要求对美国的临时专利申请: No. 60/402, 287, ,由发明人 Daniel J. Mendez 和 Mason Ng 于 2002 年 8 月 9 日递交, 名称为 "System, Method, and Computer Program Product for Cleaning Up A Remote Device That Is No Longer Authorized To Access A Global Server System" 的权利, 其被包含于此作为参考。

技术领域

本发明涉及远程数据访问领域, 尤其是, 涉及用于远程设备上可用数据的自动破坏技术, 该远程设备已经被破解并被没有权限的用户使用。

背景技术

数据的可访问性和一致性常常是计算机用户重点关心的问题。

当一个漫游到远程位置的漫游用户需要浏览或处理诸如电子邮件或文件之类的数据时, 漫游用户必须将数据传送到远程位置或者远程地访问工作站。由于维护包含必要数据的数据库的准确副本可能是一个麻烦的过程, 系统设计者已经开发各种用于通过计算机网络将远程设备连接到存储数据的服务器的技术。

数百万的人们, 包括公司以及机构的雇员, 将远程访问技术用于执行工作中的数据通信。公司以及机构常常处于这种压力下, 即利用现有的和通常种类不同的通信平台和设备, 找到快速并且成本合算地将移动

雇员连接到关键的机构信息的方法。解决这种关于远程访问技术的访问、同步，以及安全性的问题对于这些机构可能是至关重要的。

用于数据通信的远程访问技术的使用可能是导致同步技术重要性增加的因素之一。当相同数据的复件存在于多个地方时，由于这些地方之一的数据复件的值被改变，其它地方的相同数据复件的值也必须被更新，以反映最新的变化。同步处理涉及更新数据值以反映值的最近变化的处理。例如，数据值可能被远程用户通过向远程设备输入新值而更改。通过使用同步处理，服务器位置上的相同数据复件的值被更改以反映远程设备上的变化。

也可以在服务器位置改变数据值。在那种情况下，就需要同步处理更改远程设备上相应数据复件的值，以反映在服务器位置的变化。总之，同步处理可以被用于更新旧的数据值从而变为与新值相等。

互联网上电子邮件的同步和诸如文件、联系簿，以及日历等的其它工作面数据的一般同步由适当的应用程序处理。由于用户依赖于可能位于不同地方的多个智能设备传输和组织他们的关键数据，因此他们需要同步这些在不同地方搜集或从不同地方传输的数据，从而确信他们访问最新版本的数据。经常地，通过同步帮助访问和更新远程用户的数据使得远程设备拥有服务器数据库最新的可用数据。

同步也允许将远程位置对数据的任何变化传回服务器。同样地，管理远程设备的用户可以更改服务器上的可用数据，该远程设备与中央存储库通信服务器的数据。

由于通过同步，远程用户对数据的改变可能导致中央存储库中数据的改变，因此远程位置对数据未授权的改变危害中央存储库中的数据。在一些实例情况下，远程设备可能丢失或被盗或者管理设备的用户可能失去授权资格。在任何远程设备进入未授权控制的情况下，远程设备上

的数据和服务器上的数据都有无权限而被使用、错误地更改，或删除的危险。这些情况中的任何一种可以至少导致事务的延迟和损失，更有甚者是对机构的生存和业务的灾难。尽管传输加密技术可以被用于确保传输中数据的保密性；但是传输加密通常与在远程设备本身被破解或远程用户失去授权资格的情况下所需要的安全措施无关。

发明内容

本发明实施例为管理诸如公司、政府机关、私人协会等机构中数据的用户，提供一种方法、系统，以及计算机程序产品，从而如果远程设备被破解或远程用户失去授权资格时，可以阻止对远程设备上数据的错用，而该远程设备与位于例如该机构中央位置的全局服务器系统通信。

在本发明的一个实施例中，揭示了用于从被破解的远程设备上擦除数据的方法，其包括：a）通过网络与远程设备交换数据，其中远程设备在其中存储一种或多种类型的数据；b）接收远程设备被破解的指示；c）在远程设备中选择一种或多种数据类型中的至少一种用于擦除；以及d）通过网络将擦除数据的命令传输到远程设备。在该实施例中，命令确定至少一种将在远程设备中擦除的数据类型，并且在远程设备接收到命令后，命令所确定的数据类型的数据在远程设备中被删除。

本发明的其它实施例可以包括用于自动破坏远程设备上数据（远程设备数据）的系统，该远程设备与存储相同数据复件（服务器数据）的服务器通信，该系统包括用于存储和处理服务器数据和远程设备数据的全局服务器，以及一个或多个用于存储和处理远程设备数据的远程设备。全局服务器和远程设备能够通过网络通信。服务器数据包括非同步和同步类型的数据。远程设备数据也包括非同步和同步类型的数据。全局服务器包括用于存储服务器数据的数据存储、用于与远程设备通信的远程

访问服务器，以及用于与远程设备通信的同步服务器。而远程设备服务器具有用于自动地破坏非同步类型远程设备数据的自动破坏服务器，以及同步服务器具有用于自动地破坏同步类型远程设备数据的自动破坏服务器。远程设备包括用于存储远程设备数据的数据存储、用于与远程访问服务器通信的远程访问客户机，以及用于与同步服务器通信的同步客户机。远程访问客户机具有用于自动地破坏非同步类型远程设备数据的自动破坏客户机；以及同步客户机具有用于自动地破坏同步类型远程设备数据的自动破坏客户机。远程设备与服务器之间的通信包括远程访问服务器与远程访问客户机之间的通信，以及同步服务器与同步客户机之间的通信。远程设备也可以相互通信。

在本发明的另一个实施例中，自动破坏服务器可以进一步包括用于控制哪个远程设备数据将被破坏的擦除控制器，用于请求远程设备切断其与网络的连接的远程设备连接切断请求器，以及用于切断全局服务器与网络的连接的服务器连接切断装置。

在另一个实施例中，自动破坏客户机可以进一步包括用于追踪数据传输并记忆数据存储最终位置的数据跟踪器，用于擦除所有或部分远程设备数据的数据擦除器，用于重新格式化远程设备的重新格式化器，以及用于切断同步客户机或远程访问客户机与网络的连接的远程设备连接切断装置。

本发明的实施例包括用于数据的自动破坏的方法，在服务器的至少一个数据类目中存储数据，存储在服务器中的每个数据类目（服务器数据）或者是非同步类型或者是同步类型；在远程设备的至少一个数据类目中存储数据，存储在远程设备中的每个数据类目（远程设备数据）或者是非同步类型、同步类型，或者是个人拥有的类型；通过服务器的远程访问服务器与远程设备的远程访问客户机之间的远程访问连接，通信

非同步类型数据；跟踪每个服务器数据和每个远程设备数据的位置、类目，以及类型；执行同步处理；被称为同步事件；在用于破坏的远程设备中接收指示，其标记至少一个数据类目，或可选地至少一种数据类型，或在用于破坏的远程设备中接收指示，其标记至少一种数据类型；以及请求远程设备激活指定程序，以破坏至少一个标记为破坏的数据类目。

在一个实施例中，服务器数据和远程设备数据的值可以包括时间戳，表示该值被最后更改的时间。

在另一个实施例中，数据类目的类型可以由同步类型变换为非同步类型。类型被变换为非同步的同步数据类目可以包括应用程序和时间表数据。数据类目的类型也可以由非同步类型变换为同步类型。类型被变换为非同步的同步数据类目的例子包括应用程序和时间表数据。

数据类目可以包括电子邮件数据类目、日历数据类目、文件数据类目、书签数据类目、任务数据类目、销售自动化数据类目、客户关系管理数据类目、公司目录数据类目、个人信息管理数据类目，以及应用程序数据类目中的至少一种。

非同步数据类目包括雇员薪水和口令，同步数据类目包括日历数据和公司目录数据。

在其它的实施例中，数据类型的变换可以由管理变换数据类型的用户传输到跟踪器，其中随后的同步事件中跟踪器发现数据类型的变换。

同步可以利用时间戳来确定相应于每个数据的最新数据值，其中对同步类型数据进行同步包括如果同步类型数据的值在一个位置被更改，就通过服务器的同步服务器与远程设备的同步客户机之间的同步连接，在另一个位置更新相应的值，以反映同步类型数据的数据值的最新更改。同步可以自动地发生，而不需由用户启动。同步可以在预定的时间发生。同步可以周期地发生。当检测到远程设备数据值变化，服务器系统数据

值变化，或检测到来自用户的指示时，同步都可以发生。

在其它的实施例中，破坏可以包括将标记为破坏的远程设备数据的完全擦除，为标记为破坏的远程设备数据加标签，或者指向标记为破坏的远程设备数据。

在其它的实施例中，指定程序可以包括破坏远程设备上同步类型数据；请求远程设备重新格式化；请求擦除远程设备上个人拥有的数据；请求擦除远程设备上的应用程序；请求擦除远程设备上非同步数据；请求擦除远程设备上同步数据；请求加密远程设备上所有数据、同步类型数据、个人拥有的数据、非同步数据和/或应用程序；切断远程设备与服务器之间的远程访问连接；切断远程设备与服务器之间的同步连接；和/或切断远程设备与服务器之间的远程访问连接和同步连接。

在其它的实施例中，远程设备的重新格式化可以包括请求从远程设备擦除所有数据和切断服务器与远程设备之间的连接，以及使远程设备的操作系统保持原样，从而使远程设备仍为一个思维机（thinking machine）。

附图说明

下图描述根据本发明实施例的各种系统和方法的例子：

图 1 是说明网络系统的方块图；

图 2 是说明计算机系统一个例子的方块图；

图 3 是说明服务器数据类目例子的方块图，其中服务器数据可以作为同步或非同步类型数据存储在全局服务器系统中；

图 4 是说明服务器数据类型的方块图；

图 5 是说明远程设备数据类型的方块图；

图 6A 是说明自动破坏服务器系统的方块图；

图 6B 是说明加密服务器系统的方块图；

图 7A 是说明自动破坏客户机系统的方块图；

图 7B 是说明加密客户机系统的方块图；

图 8A 和图 8B 一起描述说明一个示例程序的流程图，该程序用于自动地破坏远程设备上的数据和应用程序，并切断远程设备与服务器系统之间的连接；以及

图 9A 和图 9B 描述说明一个示例程序的流程图，该程序用于自动地破坏远程设备上的数据和应用程序，并切断远程设备与服务器系统之间的连接。

具体实施方式

背景技术部分问题的叙述阐明需要一种系统和方法，用于阻止未授权使用远程设备上的数据，该远程设备与诸如服务器系统的数据中央存储库通信。这里提出一种系统、方法，以及计算机程序产品，其处理未授权访问远程设备上或与远程设备通信的服务器上数据的问题。

图 1 是说明根据本发明实施例的网络系统 100 的方块图。如图 1 所示，网络系统 100 包括全局服务器系统 110，其通过网络 150 与一个或多个远程设备 120 通信。通过诸如无线或有线（光纤、同轴电缆、ISDN、铜线等）连接的任何适当类型的连接，服务器系统 110 可以被连接到网络 150。同样地，通过任何适当的连接，远程设备 120 可以被连接到网络 150。任选地，通过有线或无线连接，可以连接远程设备 120 和服务器系统 110。同样地，远程设备 120 可以是移动的或固定的。

移动设备是便携式的和方便地由用户四处携带的设备。移动设备的例子包括移动电话、掌上计算机，以及膝上型电脑。利用网络 150 远程设备 120 可以与其它远程设备通信。

应该指出本发明实施例能够提供对很多类型远程设备的访问，其可以是固定的或移动的计算机设备，与使用最广泛的诸如微软的 Outlook 和莲花的 Notes 的企业信息应用程序一起使用。适当网络 150 的例子包括 WAN（广域网）、LAN（局域网）、电话网、互联网，或者任何其它有线或无线通信网络。

全局服务器系统 110 可以包括服务器数据存储 130、远程访问服务器 116，以及同步服务器 118。服务器数据存储 130 可以被用于存储服务器数据 115，其与远程设备数据 121 同步或另外地被远程设备 120 访问。远程访问服务器 116 进一步包括自动破坏服务器 117、加密服务器 150，以及指定程序文件 170。同步服务器 118 进一步包括自动破坏服务器 119、加密服务器 152，以及指定程序文件 175。

远程设备 120 可以类似地包括远程设备数据存储 135、远程访问客户机 122，以及同步客户机 124。远程设备数据存储 135 可以被用于存储远程设备数据 121。远程访问客户机 122 进一步包括自动破坏客户机 123 和加密客户机 160。同步客户机 124 进一步包括自动破坏客户机 125 和加密客户机 162。

服务器系统 110 和远程设备 120 的远程访问服务器 116、同步服务器 118、远程访问客户机 122、同步客户机 124，以及安全系统（未显示）可以支持任何合适的协议，例如其可以包括 WAP（无线应用协议）、WML（无线标记语言）、HDML（手持设备标记语言）、SMS（短消息系统）、HTML（超文本标记语言）、HTTP（超文本传输协议），和/或 SMTP（简单邮件传输协议）。

远程访问服务器 116 存在于服务器系统 110 上，例如其可以位于诸如机构总部的中央位置，远程访问客户机 122 存在于远程设备 120 上，例如位于漫游客户的终端。远程访问客户机 122 允许远程设备 120 通过

远程访问服务器 116 访问服务器数据 115。

相同数据 115/121 的复件，或其子集，可以分别地存在于服务器 110 和远程设备 120 上。当相同数据的复件存在于多个位置时，由于这些位置中一个上的数据值被改变，其它位置上相同数据的复件必须被更新，以反映最新的变化。同步处理可以被用于同步数据，即，更新旧的数据值从而变为与新值相等。

同步服务器 118 存在于服务器系统 110 上，而同步客户机 124 存在于每个远程设备 120 上。同步服务器 118 和同步客户机 124 控制服务器 110 上数据 115 的复件（或子集）与远程设备 120 上相同数据 121 的复件（或子集）的同步。同步处理可以被自动地执行，而不需要任何来自用户的启动。例如，同步服务器 118 和同步客户机 124 可以被设置为在预定时间、预定间隔，或检测到一方数据变化时执行同步处理。作为另一个选择，可以在收到用户指令时执行同步。

每当执行同步程序时，同步事件发生。因此，在预定的时间间隔，每当一个终端的数据值被改变时，每当一个终端的用户需要时，或根据一些其它标准，同步事件可以发生。

同步服务器 118 和同步客户机 124 控制将较旧的数据值替换为相应的较新的数据值。利用诸如时间戳的各种方法，可以区分较旧的数据值与较新的值。例如，如果每个数据值被另外地用时间戳限定，同步服务器 118 和同步客户机 124 可以使用时间戳之间的比较，识别最新的数据值并更新较早的数据值，以反映对该值的最新更改。使用时间戳，同步服务器 118 或客户机 124 选择可以替代较早版本的最新数据值。

可以被用于执行同步程序的同步方案的示例性例子被揭示在美国专利号 6,023, 708，授予 Mendez et al.的名称为“System and Method for Using a Global Translator to Synchronize Workspace Elements Across a Network”

的专利，美国专利号 6, 151, 606，授予 Mendez 的名称为 “System and Method for Using a Workspace Data Manager to Access, Manipulate and Synchronize Network Data” 的专利，以及美国专利号 6,085, 192，授予 Mendez et al.的名称为 “System and Method for Securely Synchronizing Multiple Copies of a Workspace Element in a Network” 的专利中，所有这些被包含于此作为参考。

当远程设备 120 的用户失去使用设备 120 的权限或当设备 120 被破解（例如，丢失、被盗）时，远程访问服务器 116 的自动破坏服务器 117 传输擦除和其它指令到远程访问客户机 122 的自动破坏客户机 123。指令可以被包括在显示将执行的程序的指定程序文件 170 中。在一个实施例中，远程访问客户机 122 擦除远程设备数据 121 中的数据子集，其包括从远程访问服务器 116 远程存取的数据，但不一定与服务器数据 115 同步。可选地，数据子集可以被看作单向同步，即，服务器数据 115 中相应数据子集的改变导致远程设备数据 121 中子集的更新，但反之则不然。该子集的例子可以包括公司目录数据。远程访问客户机 122 也可以擦除远程设备数据 121 中的个人数据和应用程序。指定程序文件 170 中的其它指令可以包括格式化指令、通信连接切断指令、加密指令、复制等。在本发明的另一个实施例中，自动破坏服务器 117 可以通知自动破坏客户机 123 首先将规定的数据（例如，非同步和/或个人数据）传输到服务器数据存储 130 进行存储，接着通知自动破坏客户机 123 擦除数据。下面将进一步详细讨论自动破坏服务器 117 和客户机 123。

加密服务器 150 与自动破坏服务器 117 一起可以将指定程序文件 170 中的指令传输到加密客户机 160。用于加密服务器 150 的指令可以包括加密来自远程设备数据 121 的所有数据或数据子集，从而保存数据但阻止未授权的用户访问远程设备 120 上的远程设备数据 121。如果远程设备

120 恢复，则可以解密和访问被加密的数据。如果数据非常敏感并且因此如果被解密被误用的危险很大，则自动破坏服务器 117 可以代替通知自动破坏客户机 123 擦除数据，而不是加密服务器 150 通知加密客户机 160 加密数据。在可选的实施例中，数据可以首先被加密并接着被擦除，从而如果被擦除的数据以某种方式被恢复，其将仍然处于被加密的格式。以下将进一步详细讨论加密服务器 150 和客户机 160。

自动破坏服务器 119 和加密服务器 152 完全地类似于自动破坏服务器 117 和加密服务器 150，但通常地控制传输指令到自动破坏客户机 125 和加密客户机 162，其以与自动破坏客户机 123 和加密客户机 160 完全类似的方式作用于远程设备数据 121 的同步数据。指定程序文件 175 可以完全的类似于指定程序文件 170，但由于同步客户机 124 处理数据的特点，可以包括不同的指令。本领域普通技术人员应该知道远程访问服务器 116 和同步服务器可以被组合为单个部件，其将指令传输到远程设备 120 操作远程设备数据 121。该单个部件可以将指令传输到远程设备 120，从而以类似的方式操作所有远程设备数据 121，或基于类型（例如，同步、非同步、个人等）操作数据 121。同样地，在本发明的一个实施例中，远程访问客户机 122 和同步客户机 124 也可以被组合为单个部件，从而基于数据类型操作远程设备数据 121。下面将结合图 3 和图 5 进一步详细讨论远程设备数据及其类型。

在本发明的一个实施例中，远程设备 120 的远程访问客户机 122 和同步客户机 124 每个可以分别包括指定程序文件 180 和 185。

指定程序文件 180 和 185 完全类似于指定程序文件 170 和 175，并且当远程设备 120 自启动自动破坏和/或加密程序时被使用。当远程设备 120 确定其被破解时，可以自启动该程序。例如，远程设备 120 可以请求密码的定期输入。如果密码的预定输入被错过或者如果输入的密码错误，

这可以表示设备 120 已经被破解，并因此需要加密或擦除远程设备数据 121 或其子集。该程序在这种情况下是有用的，即当远程设备 120 被破解但不与全局服务器系统 110 联系，从而系统 110 不能启动指定程序文件 170 和/或 175 中的程序时。

在操作网络系统 100 期间，远程设备 120 访问来自全局服务器系统 110 的数据。对于非同步数据，远程访问客户机 122 与远程访问服务器 116 交互。对于同步数据，同步客户机 124 与同步服务器 118 交互，根据本领域已知的同步程序交换数据。服务器 118 与客户机 124 之间的同步可以以周期性的预定间隔发生，或者可以由远程设备 120 的用户或全局服务器系统 110 的操作者手动地启动。

如果远程设备 120 已经被破解（例如，丢失、被盗，或用户不再有授权访问数据），远程访问服务器 116 和同步服务器 118 可以将指令分别传输到远程设备 120 的远程访问客户机 122 和同步客户机 124，以加密和/或擦除所有远程设备数据 121 或其子集。此外，远程访问服务器 116 和同步服务器 118 可以分别将指令传输到远程访问客户机 122 和同步客户机 124，以将所有远程设备数据 121 或其子集的复件传输到全局服务器系统 110 或其它用于存储和赋值的位置。此外，如上所述，如果远程设备 120 被破解，远程设备 120 可以自启动擦除和/或加密程序。

图 2 是说明示例性计算机系统 200 的方块图，该系统可以被用于执行本发明的实施例。服务器系统 110、远程设备 120，以及这些系统的部件可以包括这种计算机系统 200 或其部分。计算机系统 200 包括一个或多个处理器 202、输入设备 203、输出设备 204、用于读取计算机可读存储媒质的读取器 205、计算机可读存储媒质 206、通信接口 207、存储介质 208，以及进一步包括操作系统 291 和其它程序 292 的工作存储器 209。总线 201 将这些部件连接到一起。

处理器 202 通常控制所有其它的部分，并通常可以包括控制单元、数学逻辑单元，以及存储器（寄存器、高速缓存器、RAM 和 ROM）和各种暂时缓冲器和其它逻辑电路。控制单元从存储器取指令并译出指令，以生成控制计算机系统其它部分的信号。处理器 202 的一些示例性例子包括英特尔的奔腾和赛扬处理器、摩托罗拉的 14500B，等等。

输入设备 203 或外围设备可以被用于传输数据到计算机系统或从计算机系统传输数据。一些输入设备可以由用户直接操作，例如键盘、鼠标、触摸屏、游戏杆、数字化输入板，或话筒。其它输入设备可以包括将外部信号转换为数据的检测器或传感器，例如，诸如话筒的模数转换器。

输出设备 204 可以包括连接到计算机系统的电子的或电子机械的设备，并可以被用于将数据以文本、图像、声音或其它媒质的形式从计算机传输到通信接口 207，其可以是显示屏、打印机、扩音器或存储设备 208。诸如磁盘驱动器和磁带驱动器的大多数现代存储设备可以作为输入和输出设备，其它的则只是输入设备。

通信接口 207 可以被用于将总线 201 连接到计算机网络 150，可以包括以太网卡、调制解调器，或其它类似软件或硬件。

以太网是一种局域网，通过同轴电缆携带的无线频率信号发送其信息。每个计算机检查是否另一个计算机正在传输和等待传输的机会。以太网系统使用的软件协议不同，但包括 Novell 公司的 Netware 和 TCP/IP 协议。调制解调器将计算机互相连接，从而通过电话线发送信息。调制解调器将计算机的数字数据调制为在电话线上发送的模拟信号，接着在另一端将其解调回被计算机读取的数字信号。

计算机可读存储介质读取器 205 可以被用于访问和存储计算机可读存储介质 206 上的信息。计算机可读存储介质读取器 205 可以包括磁盘

驱动器、光盘驱动器，或数字光盘播放机。计算机可读存储介质 206 可以包括软盘、光盘，或数字化视频盘。

存储器 208 或记忆装置是一种设备，数据可以被输入其中，被保存在其中，以及之后可以从其中被重新找到。存储器 208 可以包括计算机系统 200 的硬盘空间，其能够永久地存储数据和应用程序。

工作存储器 209 可以包括随机存取存储器（RAM），其依次存储操作系统 291 和其它程序 292。RAM 可以由半导体集成电路制成，其可以是静态的（SRAM）或动态的（DRAM）。尽管也可以使用非易失的随机存取存储器，RAM 通常是易失的。

操作系统 291 是处理各种任务的低层软件，例如与外部硬件连接、安排任务、分配存储区，以及当不运行应用程序时通常为用户呈现默认界面。操作系统 291 的一些例子可以包括 UNIX、XENIX、Linux、OS2/WARP、DOS、Windows、Windows 95、Windows 98、Windows CE、Windows NT、Windows 2000、Macintosh System 7、IBM 的 VM 以及 VS/VME，或特别地为手持设备设计的操作系统，例如 PalmOS、EPOC、Windows CE、FLEXOS、OS/9 以及 JavaOS，或任何能够操作各种类型计算机的其它类型的操作系统。

图 3 是说明各种类目的服务器数据 115 例子的方块图。

分别存储在服务器数据存储 130 和远程设备数据存储 135 中的服务器数据 115 和远程设备数据 121，可以包括一个或多个类目。例如这些类目可以包括电子邮件数据 310、日历数据 320、文件数据 330、书签数据 340、任务数据 350、销售自动化数据 360、客户关系管理数据 370、公司目录数据 380、个人信息管理（PIM）数据 390、各种应用程序 395，以及其它数据类型。

电子邮件数据 310 的例子可以包括电子邮件的内容，邮件被发送和

接收的日期，发送者和接收者的地址，以及电子邮件的名称。日历数据320 的例子可以包括每个日期的时间和安排的事件以及每个日期的其它特征，如日期是否为假日。文件数据 330 的例子可以包括文件名，内容，创建文件的日期，以及文件位置。书签数据 340 的例子可以包括书签位置的互联网地址和相应于该地址的标识符或名称。任务数据 350 的例子可以包括关于将被执行的任务的信息和执行的日期以及被分配为执行每项任务的人员。销售自动化数据 360 的例子可以包括关于组织中销售人员销售活动自动化的数据。客户关系管理数据 370 的例子可以包括关于组织各种客户的各种类型数据。公司目录（或其它组织类型）数据 380 可以包括名称、职位、位置，以及为组织工作的人员的联系信息。个人信息管理（PIM）数据的例子可以包括对人员的生活和活动进行日常管理的人员所使用的数据。各种应用程序 395 的例子可以包括诸如微软的 Word 或 WordPerfect 的文字处理应用程序，诸如 Lotus 1-2-3 和 Excel 的电子数据表应用程序，诸如 Autocad 的制图应用程序，等等。服务器数据 115 和远程设备数据 121 可以包括整个数据文件，应用程序，或其它数据单元。

图 4 是表示全局服务器系统 110 的服务器数据 115 的方块图。服务器数据 115 可以包括两种类型的数据，非同步类型数据 410 和同步类型数据 420。

非同步服务器数据 410 可以被定义为不会根据远程设备 120 上数据的更改而更改的数据类型。非同步数据 410 由远程访问服务器 116 提供给远程访问客户机 122。该数据可以是远程设备不可访问（甚至不可见）的数据，或者是远程设备 120 可以访问和存储但不能变化和改变的数据。

同步处理不影响该类型的数据，并且当远程设备位置上相应数据值被改变时，服务器位置上该类型的数据值不被更新。非同步数据 410 的

例子可以包括敏感数据，例如，与诸如口令和加密信息，或雇员薪水的保密信息有关的数据。

同步数据 420 可以被定义为可以利用同步处理被同步的数据类型。同步服务器 118 可以将该数据提供给同步客户机 124。如上所述，通常希望保护一些数据值不被现场的用户改变；这些数据或者应该保持不变或者仅被具有中央权限的人在中央位置改变。在另一方面，同步数据是这种类型的数据，即允许被远程设备 120 的漫游用户更改，并且在后来的同步事件中数据值的改变将被传输到相应的服务器数据 115。同步数据的例子可以包括由使用远程设备的漫游用户定期地收集的数据。该数据可以根据组织类型不同，可以包括销售数据、技术数据、时间安排数据、人口普查数据，等等。在这些情况下，漫游用户通常处于更新数据值的最适当的位置，并希望将这种更新传输到中央位置。

图 5 是表示远程设备数据 121 类型的方块图。远程设备数据 121 包括非同步远程设备数据 510、同步远程设备数据 520，以及个人拥有的远程设备数据 530。

如同在上下文中对服务器数据类型的解释，如果和当远程设备上的数据值被分为非同步数据类型 510 时，则这些数据将不会被服务器系统 110 上相应数据值的改变所影响。相反地，远程设备 120 上数据值的改变将不会自动影响服务器系统 110 上相应的数据值。然而，在可选的实施例中，非同步数据类型 510 实际上可以是单向同步。即，服务器数据 115 的变化将改变远程设备数据 121，但反之则不然。通过使用远程访问客户机 122 和远程访问服务器 116，非同步服务器数据 410 可以被远程设备 120 访问。

非同步远程设备数据 510 可以包括非同步服务器数据 410 的相同类目，也可以进一步包括不同于非同步服务器数据 410 的数据类目。特别

地，非同步远程设备数据 510 可以属于控制服务器系统的机构。非同步远程设备数据 510 的例子可以包括敏感数据，例如，与诸如口令和加密信息，或雇员薪水的保密信息有关的数据。

在同步期间，即使相应的同步服务器数据 420 的值已经被更改，由于最新的同步事件，也可以更新同步远程设备数据值 520。同时，在后来的同步事件中，同步远程设备数据 520 的任何更改将导致同步服务器数据 420 的相应改变。可以被远程设备 120 的用户自由更改的数据类目通常被归为同步类型。同时，当漫游用户访问数据类目的最新值很重要时，该类目必须被划分为同步数据 520，必须周期地被服务器系统 110 上的改变更新。

日历数据和公司目录数据是被归为该类型的数据类目的例子。

与以上的类型相反，个人拥有数据 530 属于远程设备的用户，理论上讲，不应该被负责处理数据和服务器系统的用户访问和修改，例如公司的信息技术管理员。在示例的情况下，漫游用户保管的远程设备 120 属于管理服务器系统 110 的组织，并由负责控制服务器系统的用户控制。组织可以授权漫游用户在分配给他们的远程设备上安装个人数据或应用程序。在这种情况下，负责控制服务器系统的用户可能希望操作避开存储在远程设备上个人拥有数据 530。因此，该数据被赋予固有类型。

每种数据类目可以被分配为同步或非同步类型。各种数据类目 310、320、330、340、350、360、370、380、390、395 等可以被管理数据的用户分配为同步类型 410 或非同步类型 420。

一般地讲，日历数据 320、一些文件数据 330、书签数据 340、销售自动化数据 360，以及客户关系管理数据 370 是需要由用户访问和更改的数据类目，其中的用户维护远程设备 120 使数据最新。

这些数据类目可以被管理数据的用户设置为同步类型 420。

同样地，远程设备 120 上这些类目之一中数据 121 的改变将通过服务器系统 110 上同步数据 420 中的相应改变反映在服务器系统 110 上，其中数据 121 的改变由漫游用户，例如可能为现场雇员，造成。在另一方面，普通的应用程序 395 通常是，但不总是非同步数据 510。

负责处理该数据的用户可以将服务器系统 110 上的数据类目转变为或转变出非同步类型 410。换句话，可以根据情况改变服务器系统 110 上每个数据类目的类型。结果，远程设备 120 上相应当数据类目也可以被转变为或转变出非同步类型 510。

将数据类目转变为或转变出非同步类型 510 的例子是将客户机信息数据保存在非同步类型 510 中，直到负责处理服务器位置上数据的用户校验它们，其中的客户机信息数据是由现场的漫游用户输入到远程设备 120 的。在这种方式中，被漫游用户输入的客户机信息数据可以不影响服务器位置上的相应数据。只要现场被输入数据被设置为非同步类型，在同步事件期间，数据值的变化将不会被传输到服务器位置。在负责处理服务器位置数据的用户确定现场的输入可信之后，相应的服务器数据 115 可以被现场的输入安全地更新。只有在那时，数据类目可以从非同步类型 510 被转变为同步类型 520。并且只有在那时，服务器数据 420 将与新更新的远程设备数据 520 同步。

可以将数据类目转变为或转变出非同步类型 510 的另一个例子可以包括诸如文字处理程序或电子数据表程序的应用程序。例如，每当应用程序的新版本被安装在服务器系统 110 上时，管理服务器数据的用户可以将应用程序类目的类型变换为同步 420，从而通过同步远程设备 120 也可以更新其应用程序的版本。在所有远程设备同步其相应的应用程序之后，通常更希望将应用程序保存为非同步类型 510，从而远程设备用户安装的应用程序的版本不会被允许破坏服务器位置的中央复件。

可能需要从同步类型变换为非同步类型并再变换回去的数据类目的另一个例子是公司雇员的时间表输入。

每个雇员的时间表输入可以在整个月中被同步，但是在每个月末，信息技术管理员可以将时间表输入变换为非同步数据类型，并阻止雇员用户进一步更改其输入。

在许多情况下，在同步类型 420 和非同步类型 410 之间转变数据类目是有利的。例如，本发明实施例可以处理多种危险情况。例如，如果在远程设备 120 上意外地发生擦除，只要在同步事件期间删除不被传回服务器系统，就不会产生永久丢失。为了阻止服务器系统 110 上数据的意外或恶意地擦除，通常不被远程设备 120 的用户更改的敏感数据类目可以被设置为非同步类型 410。在积极监督期间，如果数据需要不时地被更新，当负责处理数据的用户能够确保服务器数据 115 是根据远程设备数据 121 的可信更改而被更改时，他可以将数据类型变换为同步类型 420。接着，负责处理数据的用户可以将数据类型变回非同步类型 410，保护其不被远程设备更改。

图 6A 是说明自动破坏服务器系统 600 的方块图。该方块图涉及包括在远程访问服务器 116 中的自动破坏服务器 117 或包括在同步服务器 118 中的自动破坏服务器 119。自动破坏服务器系统 117 和 119 都具有类似的部件，其通常执行相同的操作。

因此，一起讨论两个自动破坏服务器系统 117 和 119 的部件。在说明其共同点之后讨论其区别。

自动破坏服务器系统 117、119 被用于通知远程设备 120 破坏远程设备数据 121。自动破坏服务器系统 117、119 包括擦除控制器 610、远程设备连接切断请求器 620，以及服务器连接切断装置 630。

擦除控制器 610 将一组擦除指令传输到远程设备 120，并根据指定程

序文件 170 或 175 中的指令控制将删除来自远程设备数据 121 的哪个数据。擦除控制器 610 可以是远程设备 120 上的应用层，其使用依赖于远程设备操作系统（平台）的合适的操作系统，其中远程设备操作系统可以在 Windows、Palm、Epoch 等之间变换。擦除指令可以是平台相关的，数据的擦除可以是完全擦除而不是加标签或指向仅仅标记为删除的数据。

远程设备连接切断请求器 620 请求远程设备 120 切断其与网络 150 的连接，其中网络 150 与服务器系统 110 连接。响应请求器 620 的请求，远程设备 120 切断其与网络 150 的连接，从而切断与其它远程设备和服务器系统 110 的连接。一旦连接被切断，自动破坏服务器系统 117、119 的服务器系统 110 和擦除控制器 610 就不能访问远程设备 120 和控制数据的进一步擦除。然而，由于只有那些被破解或未授权的一个或多个远程设备被切断连接，服务器系统 110 仍然可以访问与网络 150 保持连接的其它远程设备。

服务器连接切断装置 630 断开服务器系统 110 与网络 150 之间的连接，因此断开服务器系统 110 与现场所有远程设备间的连接。当所有远程设备被破解，服务器系统 110 需要切断与所有设备 120 间的连接时，可以使用装置 630。使用装置 630 的另一个示例情况是当在服务器系统 110 中检测到诸如病毒攻击的错误时。阻止错误或病毒的传播需要服务器系统 110 与连接设备隔离，例如所有远程设备 120。总之，当服务器系统 110 被破解时，或所有远程设备 120 被破解时，而不是单个远程设备 120 或所有远程设备 120 的一个子集被破解时，通常使用装置 630。

在本发明的另一个实施例中，通过删除用于特定的未授权远程设备 120 的所有权限密码和/或相关数据（例如，用户帐户、MAC 帐户、口令等），服务器连接切断装置 630 阻止远程设备 120 访问服务器系统 110。

两个自动破坏服务器之间的区别是自动破坏服务器 117 的擦除控制器 610 存在于远程访问服务器 116 内，用于服务器非同步数据 310，而自动破坏服务器 119 的擦除控制器 610 存在于同步服务器 118 内，用于服务器同步数据 320。然而，本领域普通技术人员应该知道自动破坏服务器 117 和 119 可以被组合为单个部件。

图 6B 是说明加密服务器系统 650 的方块图。该方块图涉及远程访问服务器 116 中的加密服务器 150 或同步服务器 118 中的加密服务器 152。加密服务器 150 与加密服务器 152 完全类似，通常具有以类似方式操作的相同部件。加密服务器系统 650 包括加密控制器 660、加密算法 670，以及加密密钥 680。

加密控制器 660 发送指令到远程设备 120 的加密客户机 160 和/或 162，加密远程设备数据 121 或其子集。加密控制器 660 可以被系统 110 的操作者启动，可以执行指定程序文件 170 和/或 175 中列出的程序。加密控制器 660 使用的指定程序可以包括发送指令到远程设备 120 以加密所有远程设备数据 121 或其子集。指定程序也可以确定使用加密算法 670 中列出的哪种类型的加密算法。用于加密和/或解密数据的密钥被存储在密钥 680 中。

图 7A 是说明自动破坏客户机系统 700 的方块图。该方块图涉及包括在远程访问客户机 122 中的自动破坏客户机 123 或包括在同步客户机 124 中的自动破坏客户机 125。自动破坏客户机系统 123 和 125 都具有相同的部件，其通常执行相同的操作。因此，一起讨论两种自动破坏客户机系统 123 和 125 的部件。在说明其共同点之后讨论它们之间的区别。

自动破坏客户机系统 700 被用于擦除远程设备数据 121 或其子集。自动破坏客户机系统 700 包括数据跟踪器 710、数据擦除器 720、重新格式化器 730，以及远程设备连接切断装置 740。

数据跟踪器 710 系统跟踪数据的传输并记录数据存储在存储器 208、工作存储器 209、计算机可读存储介质 206，或其它地方的最终位置。数据在远程设备 120 与服务器系统 110 之间，或被允许互相通信的远程设备 120 之间传输。被传输的数据被归为各种类型和类目。

每个被传输的数据可以被分配为非同步类型 410、510，或同步类型 420、520。个人拥有数据 530 通常不在设备之间传输。然而，被归为该数据类型的数据可以被跟踪，也可以区分于其它类型。来自诸如电子邮件数据 310、日历数据 320 等的每个数据可以进一步被归为特殊类型的非同步类型 410、510，同步类型 420、520，或个人拥有类型 530。

将被同步的数据 410 可以首先被管理数据的用户识别和标记。当同步类型数据 410 被传输到远程设备 120 时，数据跟踪器 710 跟踪数据的位置和类型。如果管理数据的用户后来改变分配给该数据的类型，在下一个同步事件中，数据跟踪器 710 发现数据不再是同步类型 410 ，并改变分配给数据的类型。在另一个选项中，当改变发生时，数据类型的改变可以被服务器系统传输到数据跟踪器 710。同样地，当接收到只用于同步数据的擦除指令时，数据跟踪器 710 知道哪个数据被分配为同步类型并需要被擦除，而哪个不是。数据跟踪器 710 进一步记录将被擦除的数据位置，这些数据位于存储器 208、工作存储器 209、计算机可读存储介质 206，或可以存储数据的计算机系统 200 上的任何其它物理位置。

数据跟踪器 710 的功能可以比作列表的功能。实际上，数据跟踪器 710 为远程设备 120 提供各种数据类型的列表，并且当某个数据单元的类型改变或当数据单元的存储位置改变时动态地保存这些列表。根据设置发生同步的频率：每当服务器系统 110 发出同步命令，以管理数据的用户或远程设备的用户设定的同步间隔，每当更新远程设备 120 端的数据单元，和/或根据一些其它规则，数据跟踪器 710 确定必须与同步服务器

数据 420 同步的同步远程设备数据 520。

根据来自系统 110 的指令或根据遵循指定程序 180 和/或 185 的自启动，数据擦除器 720 系统能够擦除所有或部分远程设备数据 121。如数据跟踪器 710 指示，数据擦除器 720 控制将从远程设备数据 121 中删除哪个数据。例如，数据擦除器可以只擦除同步数据 520 或只擦除个人数据 530。数据擦除器可以使用依赖于远程设备操作系统（平台）的适当的操作系统，其中远程设备操作系统可以在 Windows、Palm、Epoch 等之间变换。擦除指令可以是平台相关的，数据擦除可以是完全擦除，而不是只加标签或指向标记为删除的数据。

重新格式化器 730 重新格式化远程设备 120 的存储区域 208。这样，重新格式化器 730 擦除所有数据并切断远程设备 120 与网络 150 之间的连接。重新格式化器 730 不区分数据类型或类目。重新格式化器 730 的操作也擦除远程设备 120 的个人拥有数据 530。在本发明的实施例中，重新格式化器 730 不擦除远程设备 120 的操作系统 291，因此将远程设备 120 保留为没有原始数据或应用程序 121 的思维机和操作机。

远程设备连接切断装置 740 切断同步客户机 124 或远程访问客户机 122 与网络 150 的连接。作为操作装置 740 的结果，远程设备 120 可能不再与服务器系统 110 或其它远程设备 120 传输特殊类型数据。如果连接切断装置 740 在数据擦除器 720 或重新格式化器 730 被通知操作前启动，则其保持远程设备数据 121 不被改变。如果远程访问客户机 122 的自动破坏客户机 123 的连接切断装置 740 操作，非同步数据 510 的传输将结束。如果同步客户机 124 的自动破坏客户机 125 的连接切断装置 740 操作，同步数据 520 的传输将结束。在可能的情况下，远程访问客户机 122 的自动破坏客户机 123 的连接切断装置 740 可以切断非同步数据 510 的传输。

如果数据类型接着被管理数据的用户更改，由非同步 410 变换为同步 420，则相同的数据将被传输到同步客户机 124。

同样地，连接切断装置 740 的操作关于不进行传输的数据类型是可选的。

包括在远程访问客户机 122 中的自动破坏客户机 123 和包括在同步客户机 124 中的自动破坏客户机 125 之间的区别，是包括在远程访问客户机 122 中的自动破坏客户机 123 的数据擦除器 720 用于客户机非同步数据 510 和个人拥有的远程设备数据 530，而包括在同步客户机 124 中的自动破坏客户机 125 的数据擦除器 720 用于客户机同步数据 520。

远程访问客户机 121 的自动破坏客户机 123 和同步客户机 124 的自动破坏客户机 125 之间的另一个区别是，存在于远程访问客户机 122 中的自动破坏客户机 123 的数据跟踪器 710 跟踪客户机非同步数据 510，存在于同步客户机 124 中的自动破坏客户机 125 的数据跟踪器 710 跟踪客户机同步数据 520。每个数据跟踪器 710 跟踪数据，该数据被传输到远程设备 120 或被用户通过输入设备 203 输入到远程设备。如果数据单元（点（point）、文件、应用程序等）被管理数据的用户从同步类型 420 转换为非同步类型 410，一旦数据被传输到远程设备 120，跟踪器 710 就得知改变。在一种情况下，同步数据 420 被同步服务器 118 传输到远程设备 120，并被远程设备 120 端的同步客户机 124 接收。自动破坏客户机 125 上的跟踪器 710 跟踪数据的位置和类型。管理数据的用户接着将数据类型变换为非同步类型 410。收到来自远程访问客户机 122 的请求后，远程访问服务器 116 将数据及其有关类型传输到远程访问客户机 122。自动破坏客户机 123 的跟踪器 710 记录数据的位置和类型，从而收到指令后可以破坏数据。在另一种选项中，在每个同步事件期间，同步服务器 118 可以将数据类型的改变传输到同步客户机 124 的自动破坏客户机 125 的

跟踪器 710。

同步客户机 124 的自动破坏客户机 125 的跟踪器 710 可以将数据类型的改变传输到远程访问客户机 122 的自动破坏客户机 123 的跟踪器 710。两个跟踪器之间的通信使其都被通知每个数据单元的位置和类型。

一般地，当设备 120 首先被破解时，远程设备 120 与位于组织总部的服务器系统 110 同步。如果设备 120 丢失或被盗或如果管理设备 120 的雇员失去授权地位，则设备 120 可能被破解。一个例子可以是当雇员被解雇但仍保持拥有远程设备 120 时。为了应对这种情况，本发明实施例提供的方法使组织中管理数据的用户远程地破坏设备 120。例如，在解雇雇员的情况下，组织中管理数据的用户可以指示远程设备 120 该雇员的帐户不再有效，并且该雇员不能访问数据。

根据管理数据的用户的猜测，本发明实施例采取多种方法。本发明可以只切断远程设备 120 与服务器 110 之间的连接。该方法切断远程设备 120 对服务器 110 上可用数据的访问，而保持已经在远程设备 120 上的数据对未授权的用户公开。本发明也可以既切断连接又擦除远程设备 120 上可用的所有同步数据。当数据没有失去其时效，并且远程设备上的数据不可落入陌生人手中时，使用该选项。本发明可以切断连接、删除数据，以及删除远程设备 120 上的应用程序。在这种情况下，应用程序也是敏感的和私有的，不应被破解。此外，如上所述，远程设备 120 可以自启动擦除/加密程序。

图 7B 是说明加密客户机系统 750 的方块图。该方块图涉及包括在远程访问客户机 122 中的加密客户机 160 或包括在同步客户机 124 中的加密客户机 162。加密客户机系统 160 和 162 具有相同的部件，通常执行相同的操作。因此，一起讨论两个加密客户机系统 160 和 162 的部件。

加密客户机系统 750 包括加密装置 760、加密算法 770 以及加密密钥

780。响应来自系统 110 的指令或当自启动时，加密装置 760 加密远程设备数据 121 或其子集。将被加密的数据在服务器 110 的指定程序文件 170 和/或 175 中或远程设备 120 的指定程序文件 180 和/或 185 中被确定。例如，指定程序文件 180 能够确定所有非同步数据 510 和所有个人拥有数据 530 的加密。

加密算法 770 是被用于加密远程设备数据 121 的算法。算法 770 可以包括公开密钥算法、对称密钥算法或其它加密算法。用于加密算法 770 的密钥被存储在加密密钥 780 中。如果加密密钥 780 与解密密钥相同，则在擦除控制器 610 加密后密钥 780 被擦除，相应的密钥被存储在服务器 110 的加密密钥 680 中。如果使用加密密钥 780 不能解密被加密的数据，则在加密后不需擦除密钥 780。

图 8A 和图 8B 一起描述说明一个程序的流程图，该程序用于自动地破坏远程设备上的数据和应用程序，并切断远程设备与服务器系统之间的连接。被说明的程序只是可以利用本发明实施例执行的各种程序中的一个例子。从服务器 110 的角度说明该程序。

在图 8A 和图 8B 的程序中，与远程设备 120 通信的服务器系统 110 接收（810）指示，远程设备 120 不再被授权访问服务器系统。在各种情况和例子中，已经丢失其远程设备 120 的被授权现场用户可以通知在服务器 110 位置管理数据的用户，远程设备 120 已被破解，在服务器位置管理数据的用户可以决定现场用户不再被授权使用数据或访问服务器，或一些其它事件，其可以促使远程设备 120 失去其访问服务器系统 110 或者甚至远程设备数据 121 的权限。远程设备 120 被破解的指示可以被管理数据的用户输入服务器系统 110，或者可以被远程设备 120 本身传输到服务器系统 110。在指示是由远程设备 120 本身传输到服务器系统的情况下，远程设备 120 可以是口令保护的或可以包括一些类型的防盗机制，

万一输入错误的口令或如果另一方面触发防盗机制，远程设备 120 将信息传输到服务器系统 110。例如，如果用户在预定的时间间隔内不向远程设备 120 输入口令，远程设备 120 可以将信息传输到服务器系统 110。

服务器系统 110 请求远程设备 120 根据指定程序进行自动破坏。指定程序或者由管理数据的用户根据情况的实时评定交互地选择，或者由根据某个预定标准触发的一些预定机制选择。指定程序确定远程设备 120 请求的自动破坏的方法和范围。例如服务器系统 110 可以检查存储在远程设备 120 上的数据 121 的敏感水平，检查远程设备是否丢失、被盗、由被解雇的雇员拥有，或只是被一个雇员借给另一个雇员。根据遇到的这些预定情况的组合，服务器系统可以触发一些预定机制，其删除所有或一些数据，限制访问某些数据，切断连接，或保持连接不被改变。请求从服务器系统 110 传输到远程设备 120，由以下组成。

服务器系统 110 首先检查（815）是否选择指定程序，该程序将远程数据 121 复制到服务器 110 或其它位置。如果是，服务器 110 请求（816）远程设备 120 传输远程数据 121。在本发明的实施例中，服务器系统 110 可以请求（816）远程设备只传输远程设备数据 121 的子集。

在请求（816）传输之后或如果没有请求传输远程数据 121，服务器系统 110 检查（817）是否选择加密远程数据 121 的指定程序。如果指定程序请求加密，加密控制器 660 通过向加密装置 760 传输信息请求（818）远程设备 120 加密远程设备数据 121 或其子集。在本发明实施例中，加密控制器 660 也能够确定和/或传输将使用的加密算法和用于加密的密钥。

服务器系统 110 接着检查（819）是否选择重新格式化整个远程设备 120 的指定程序。在描述的实施例中，重新格式化整个远程设备 120 是最高级别的自动破坏。如果选择指定程序（820），则自动破坏服务器 117、

119 的擦除控制器 610 向重新格式化器 730 传输请求，重新格式化远程设备 120。重新格式化器 730 擦除包括所有应用程序的所有数据，但不需包括操作系统 291。由于重新格式化器 730 擦除保持远程设备 120 与服务器系统 110 之间通信的应用程序，因此擦除所有应用程序就自动地切断远程设备 120 与服务器系统 110 之间的连接。远程设备 120 将被保留其操作系统 291，因此将仍为思维机和操作机，但不包含任何由远程设备 120 的用户或在服务器位置管理数据的用户安装在其上的数据单元（点、文件，或应用程序等），并且不能访问服务器系统 110 重新同步丢失的数据。

该选项擦除个人拥有的数据，同样，在某些情况下不是需要和可取的。在另一方面，该选项是完全的和快速的。

如果没有选择重新格式化指定程序（819），如在指定程序中说明的，可以使用擦除远程设备数据 121 的其它程序。服务器系统 110 检查（825）选择的指定程序是否表示擦除远程设备 120 上的个人拥有数据 530。当用户未被授权在远程设备上保存个人拥有的数据但却将这种数据加载到设备上时，可以选择该指定程序。

当已破解远程设备的用户需要破坏其个人拥有的数据，但其它类型数据并不足够敏感至被破坏时，也可以选择该指定程序。当远程设备从一个用户转移到另一个用户，该用户可能使用除前一个用户的个人拥有数据外的所有数据时，也可以选择该指定程序。如果选择了该指定程序，服务器系统请求（830）擦除远程设备 120 上的个人拥有的数据 530。远程访问服务器 116 的自动破坏服务器 117 的擦除控制器 610 传输信息到远程访问客户机 122 的自动破坏客户机 123 的数据擦除器 720，只擦除远程设备的个人拥有数据。数据擦除器 720 继续擦除远程访问客户机 122 的自动破坏客户机 123 的数据跟踪器 710 标记为个人拥有数据 530 的数

据。如前所述，设定为删除的数据被完全删除。

服务器系统 110 检查（835）被选择的指定程序是否表示擦除远程设备 120 上的应用程序。如果被选择的指定程序表示擦除应用程序，服务器系统 110 通知（840）远程设备 120 擦除应用程序。应用程序是数据类目，并且可以被归为同步类型 520 或非同步类型 510。因此，远程访问服务器 116 和同步服务器 118 的自动破坏服务器 117、119 的擦除控制器 610 可以将擦除两种类型应用程序的请求传输到远程访问客户机 122 和同步客户机 124 的自动破坏客户机 123、125 的数据擦除器 720。数据擦除器 720 接着继续进行包括在远程设备数据 121 中应用程序的完全擦除。

服务器系统 110 接着检查（845）被选择的指定程序是否表示擦除非同步数据 510。如果选择的指定程序表示擦除非同步数据 510，服务器系统 110 通知（850）远程设备 120 擦除非同步数据。远程访问服务器 116 的自动破坏服务器 117 的擦除控制器 610 通知远程访问客户机 122 的自动破坏客户机 123 的数据擦除器 720 擦除非同步远程设备数据 510。数据擦除器 720 根据从数据跟踪器 710 得到的信息确定非同步数据 510，并继续进行数据的完全擦除。

服务器系统 110 检查（855）被选择的指定程序是否表示擦除同步数据 520。如果被选择的指定程序表示擦除同步数据 520，服务器系统 110 通知（860）远程设备 120 擦除同步数据。

同步服务器 118 的自动破坏服务器 119 的擦除控制器 610 通知同步客户机 124 的自动破坏客户机 125 的数据擦除器 720 擦除同步远程设备数据 520。数据擦除器 720 根据从数据跟踪器 710 得到的信息确定同步数据 520，并继续进行数据的完全擦除。

服务器系统 110 接着检查（865）被选择的指定程序是否表示切断与远程设备 120 的远程访问连接。如果被选择的指定程序表示切断连接，

服务器系统通知（870）远程设备 120 切断与服务器系统 110 的远程访问连接。远程访问服务器 116 的自动破坏服务器 117 的远程设备连接切断请求器 620 向远程访问客户机 122 的自动破坏客户机 123 的远程设备连接切断装置 740 发送请求，切断与服务器系统 110 的远程访问连接。作为响应，远程设备连接切断装置 740 继续切断服务器系统 110 与远程设备 120 之间的远程访问连接。在这种情况下，同步访问仍没有被切断。因此，只有非同步数据 510 的传输结束，同步数据 520 仍然继续在服务器系统 110 和远程设备 120 之间传输。如前所述，如果数据类型被管理数据的用户从非同步变换为同步，则由于同步连接仍然有效，其可以通过同步服务器和客户机被传输。

服务器系统 110 接着检查（875）被选择的指定程序是否表示切断与远程设备 120 的同步连接。如果选择的指定程序表示切断连接，服务器系统 110 通知（880）远程设备 120 切断与服务器系统 110 的同步连接。同步服务器 118 的自动破坏服务器 119 的远程设备连接切断请求器 620 向同步客户机 124 的自动破坏客户机 125 的远程设备连接切断装置 740 发送请求，切断与服务器系统 110 的同步连接。

远程设备连接切断装置 740 继续切断服务器系统 110 与远程设备 120 之间的同步连接。在这种情况下，非同步访问没有被切断（除非其较早被切断（870））。因此，如果远程访问连接没有被较早地切断（870），则只有同步数据 520 的传输结束，非同步数据 510 仍然可以继续在服务器系统 110 和远程设备 120 之间传输。

总之，图 8A 和图 8B 的程序中说明的指定程序允许服务器系统 110 和远程设备 120 之间连接的全部和完全切断，数据 121 的完全加密，数据 121 的复制，远程设备上数据 121 的全部和完全擦除，或连接的选择性切断和数据的选择性擦除。

图 8A 和图 8B 的程序只是提出一些可能的情况，以及切断连接和擦除数据的不同组合和匹配的情况，其也可以由本发明的实施例实现。

在一个示例性的破坏安全的情况下，保管设备 120 的未授权用户可能试图断开通信能力，从而阻止服务器系统 110 请求破坏远程设备数据 121。然而，在全局服务器的管理数据的用户请求擦除数据前，是很难这样做的。在远程设备 120 包括敏感数据的情况下，定时自动破坏特性可以被嵌入在远程设备数据擦除器 720 或重新格式化器 730 中，其可以以一定时间间隔自动地擦除由类型或类目标识的敏感数据，除非向远程设备 120 输入或传输口令。

图 9A 和 9B 描述说明一个程序的流程图，该程序用于自动地破坏远程设备 120 上的数据和应用程序，并切断远程设备 120 与服务器系统 110 之间的连接。被说明的程序只是各种程序中的一个例子，可以利用本发明实施例实现。从远程设备 120 的角度说明该程序。

在本发明实施例中，在图 9A 的程序中，与服务器系统 110 通信的远程设备 120 发送（905）远程设备被破解的指示。远程设备可以被口令保护，或包括一些类型的防盗机制，万一输入错误的口令或如果另一方面防盗机制被触发，远程设备 120 向服务器系统 110 发送信息。

如图 8A 和图 8B 中描述，远程设备 120 接着接收（910）来自服务器系统 110 的指令，根据诸如指定程序文件 170/175 中程序的指定程序，复制、擦除，和/或加密远程设备数据 121。指定程序确定来自远程设备 120 的自破坏请求的方法和范围。指定程序或者由管理数据的用户根据情况的实时评定交互地选择，或者根据某个预定标准由触发的一些预定机制选择。远程设备 120 接着处理（915）接收的指令和图 9A 中描述的方法。

在图 9B 中，远程设备 120 自发地自启动自动破坏程序。远程设备

120 首先确定（920）其是否已被破解。如果在指定的间隔没有输入口令或者如果输入错误的口令，就可以确定（920）。在可选的实施例中，可以根据在指定间隔没有收到来自系统 110 的信息做出该确定（920）。如果设备 120 没有被破解，设备 120 可以延后启动该确定（920）。否则，远程设备 120 执行指定程序文件 180 和/或 185 中规定的指定程序。

如上所述，指定程序可以包括加密、传输，和/或擦除所有远程数据 121 或其子集。指定程序也可以包括切断远程设备 120 与网络 150 之间的连接。

总之，图 9A 和图 9B 程序中执行的指定程序允许服务器系统 110 与远程设备 120 之间连接的全部和完全切断，远程设备上数据 121 的全部和完全擦除，数据 121 的复制，数据 121 的加密，和/或数据的选择性擦除。图 9A 和图 9B 的程序只提出一些可能的情况。切断连接和擦除数据的不同组合和匹配的情况也可以由本发明实施例实现。

本领域普通技术人员应该知道图 8A 和图 8B 和图 9A 和图 9B 的程序中数据 121 的擦除可以以数据类型和类目的不同组合和匹配进行。数据 121 只有某些类目可以被设定为擦除。例如只有公司目录数据可以被选择为擦除。根据数据类目是否被分配为同步或非同步类型，远程访问服务器 117 或同步服务器 119 的自动破坏服务器可以从远程设备请求擦除。数据跟踪器 710 具有每个数据的存储位置、类型，以及类目，并可以被数据擦除器 720 得到，用于选择性擦除。

本发明实施例的以上描述只是示例，本发明提供上述实施例和程序的其它变化。例如，尽管服务器系统被描述为单个设备，但服务器系统可以包括连成网络的几个计算机。使用程序通用的数字计算机、专用集成电路，或常规部件和电路互联的网络可以实现本发明的部件。

这里所述的实施例是为说明而提出的，并不用于穷举和限制。根据

前述教导许多变化是可行的。例如，上述实施例可以使用指令实现数据的擦除或连接的切断。在其它实施例中，通过删除服务器系统上的数据并通知同步也删除远程设备上的相应数据，也可以由同步事件实现数据擦除。在另一方面，如果远程设备上的数据被删除，服务器系统或远程设备中的机制可以阻止或延迟同步，直到确定这种删除并非意外发生。

作为另一个例子，在上述实施例中，数据的删除由完全删除和重写存储区域实现，而不只是加标签或指向数据。在另一个实施例中，删除可以由加标签或指向被删除的数据实现。所述方法、系统，以及计算机程序产品仅由以下权利要求限制。

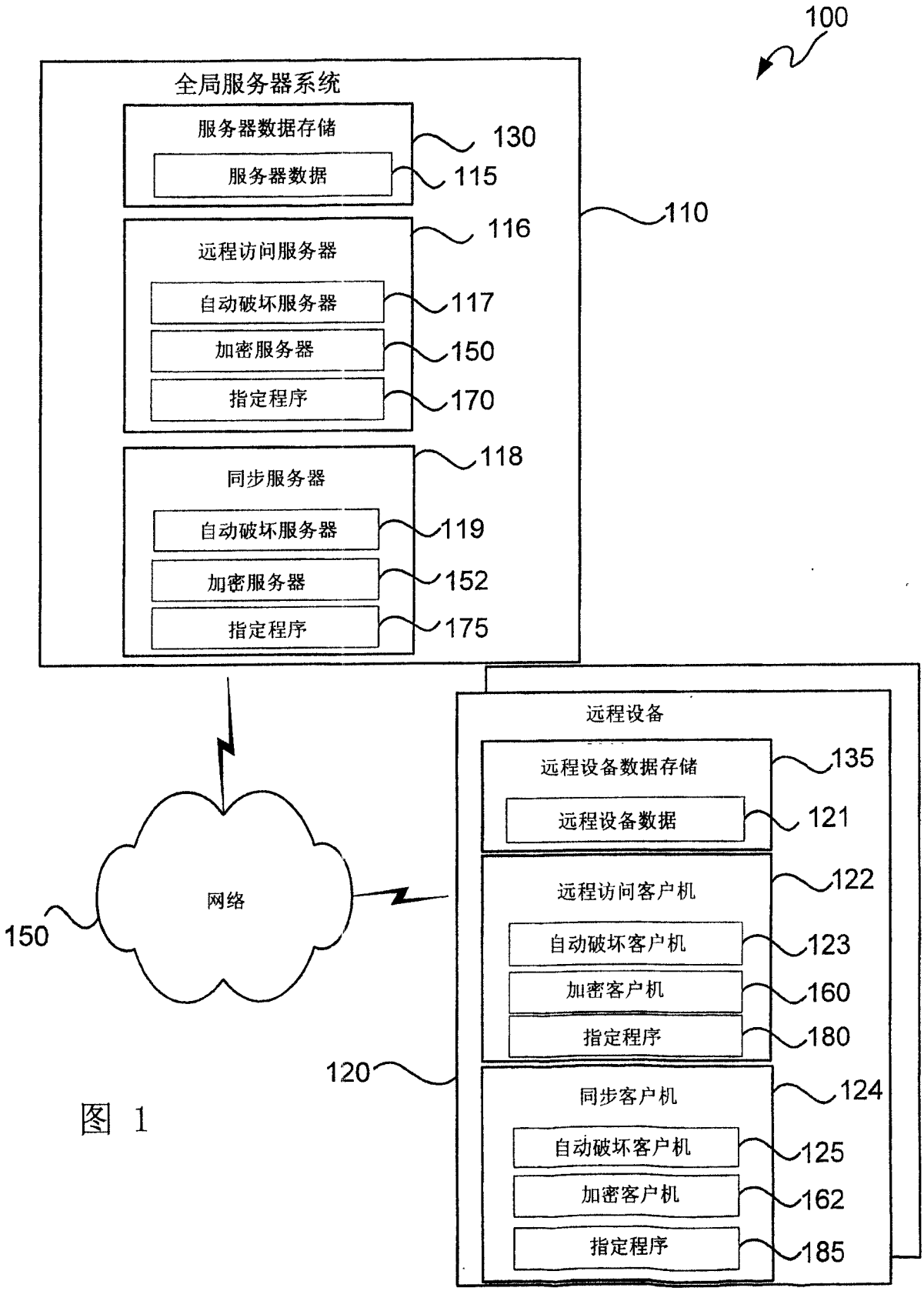

100
全局服务器系统
服务器数据存储
130
服务器数据
115
110
116
远程访问服务器
自动破坏服务器
117
加密服务器
150
指定程序
170
118
同步服务器
自动破坏服务器
119
加密服务器
152
指定程序
175
远程设备
远程设备数据存储
135
远程设备数据
121
122
远程访问客户机
自动破坏客户机
123
加密客户机
160
指定程序
180
120
同步客户机
124
自动破坏客户机
125
加密客户机
162
指定程序
185
网络
150

图 1

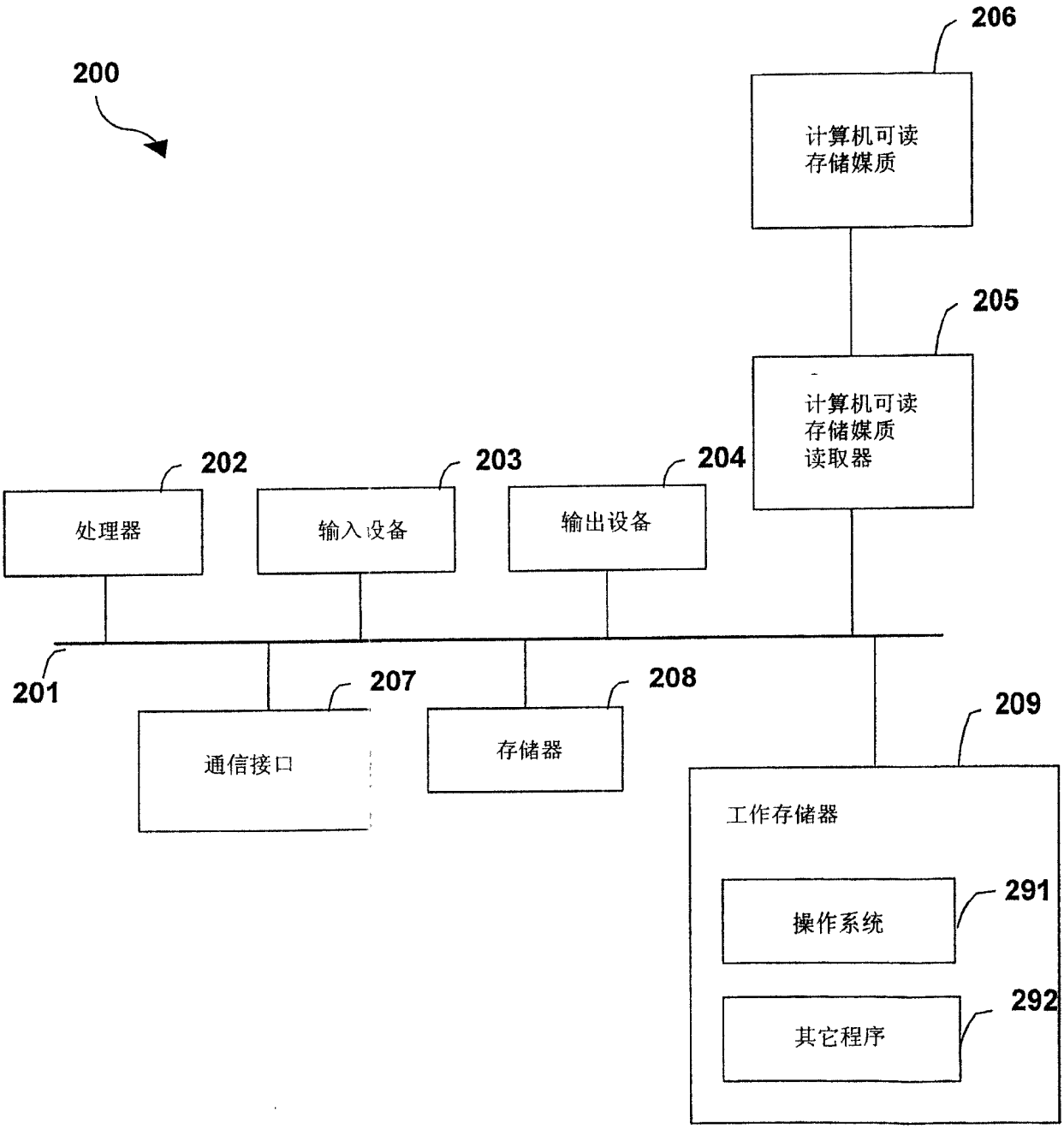

200
206
计算机可读
存储媒质
205
计算机可读
存储媒质
读取器
202
处理器
203
输入设备
204
输出设备
201
207
通信接口
208
存储器
209
工作存储器
291
操作系统
292
其它程序

图 2

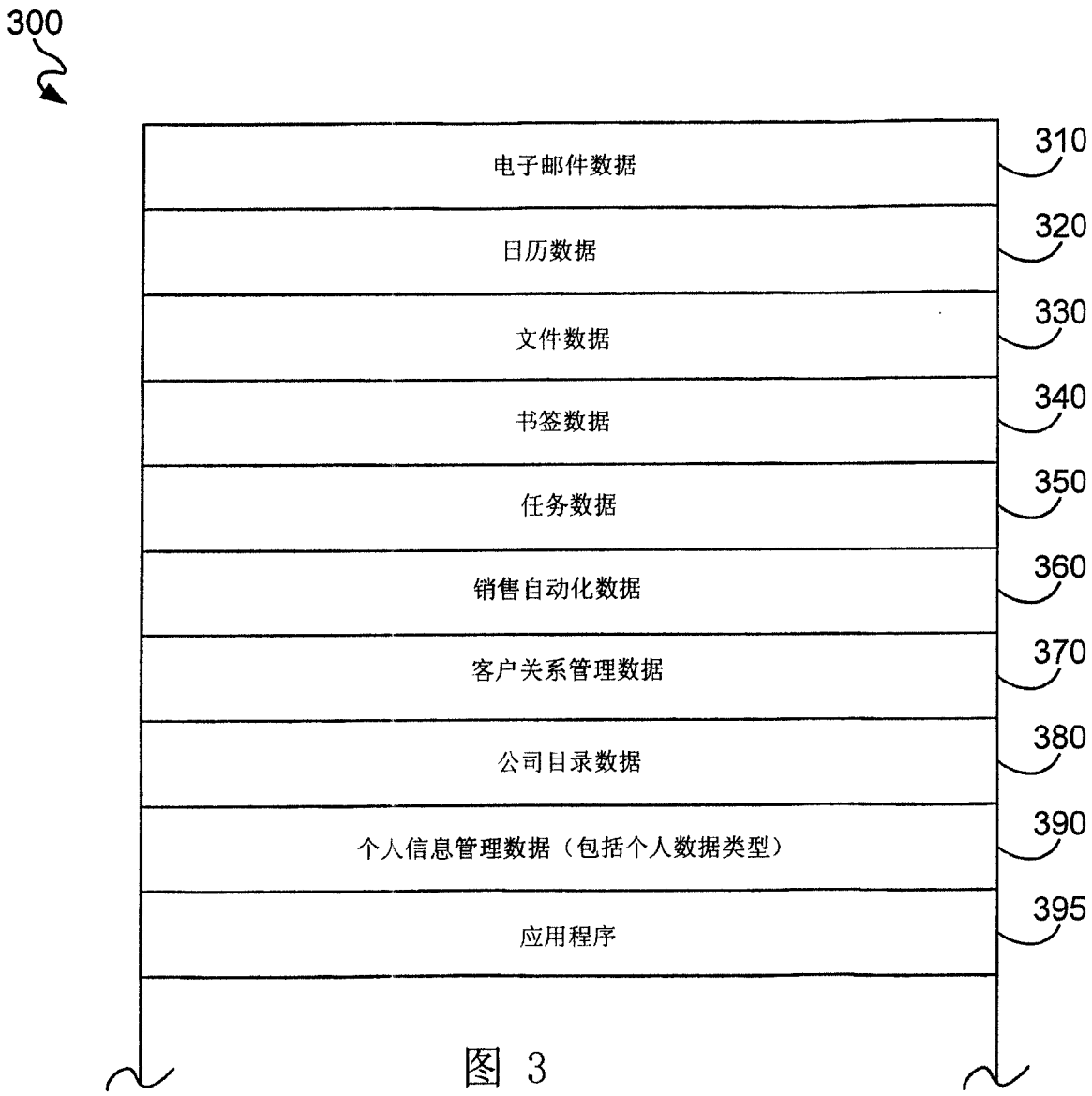

300
电子邮件数据
310
日历数据
320
文件数据
330
书签数据
340
任务数据
350
销售自动化数据
360
客户关系管理数据
370
公司目录数据
380
个人信息管理数据（包括个人数据类型）
390
应用程序
395

图 3

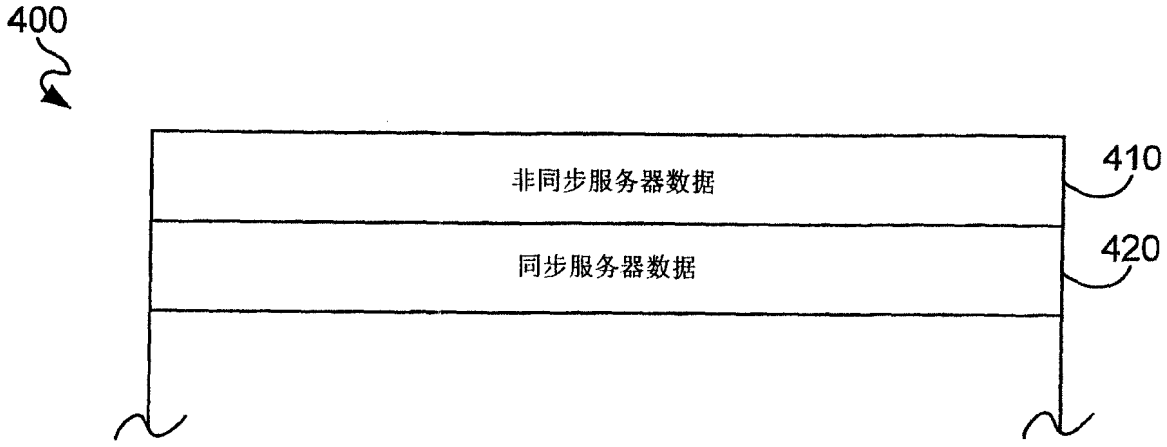


图 4

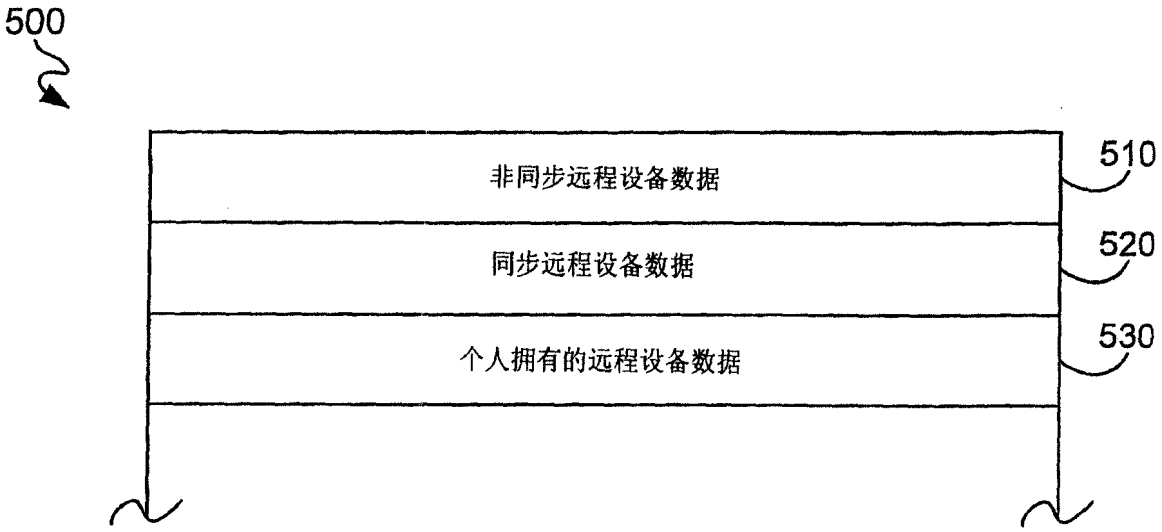


图 5

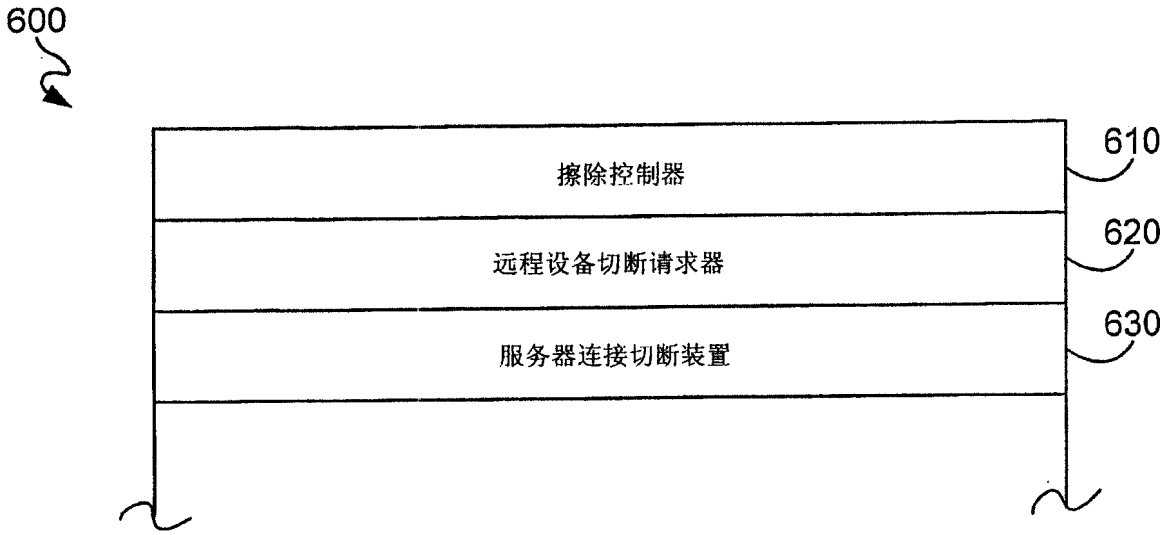

600
擦除控制器
610
远程设备切断请求器
620
服务器连接切断装置
630

图 6A

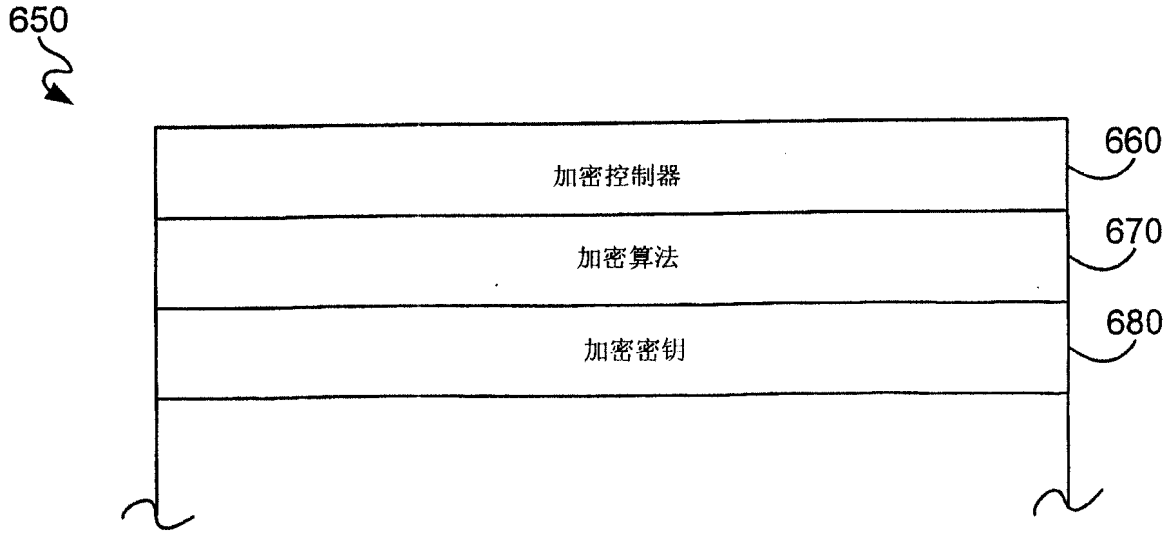

650
加密控制器
660
加密算法
670
加密密钥
680

图 6B

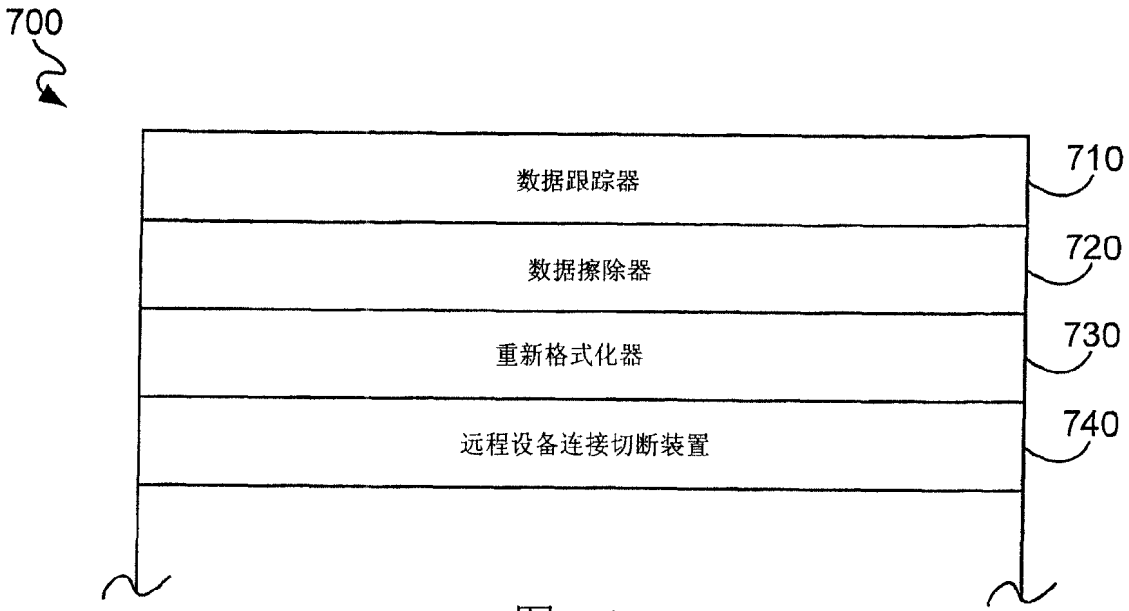

700
数据跟踪器
710
数据擦除器
720
重新格式化器
730
远程设备连接切断装置
740

图 7A

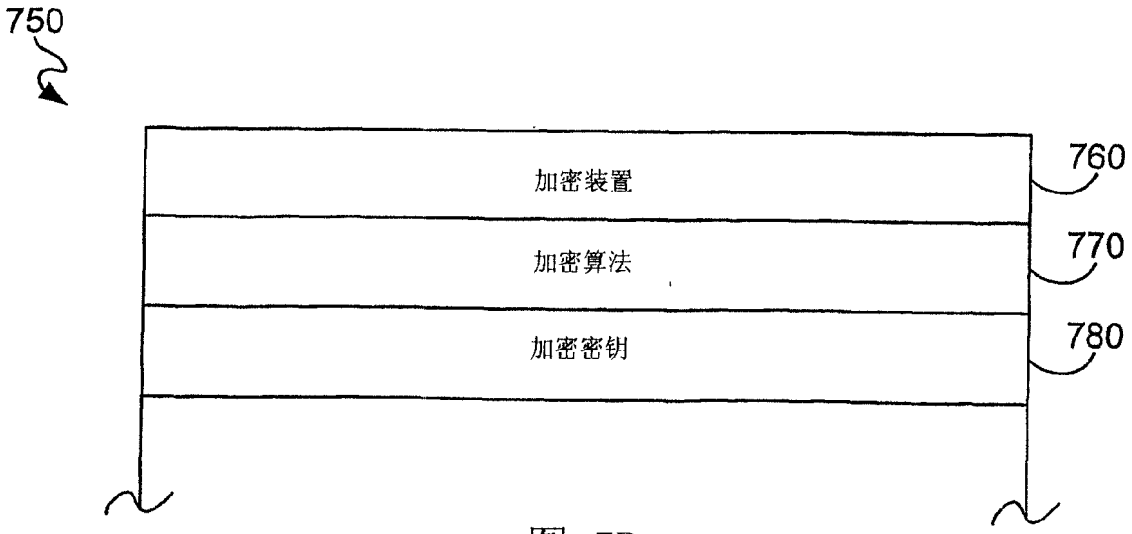

750
加密装置
760
加密算法
770
加密密钥
780

图 7B

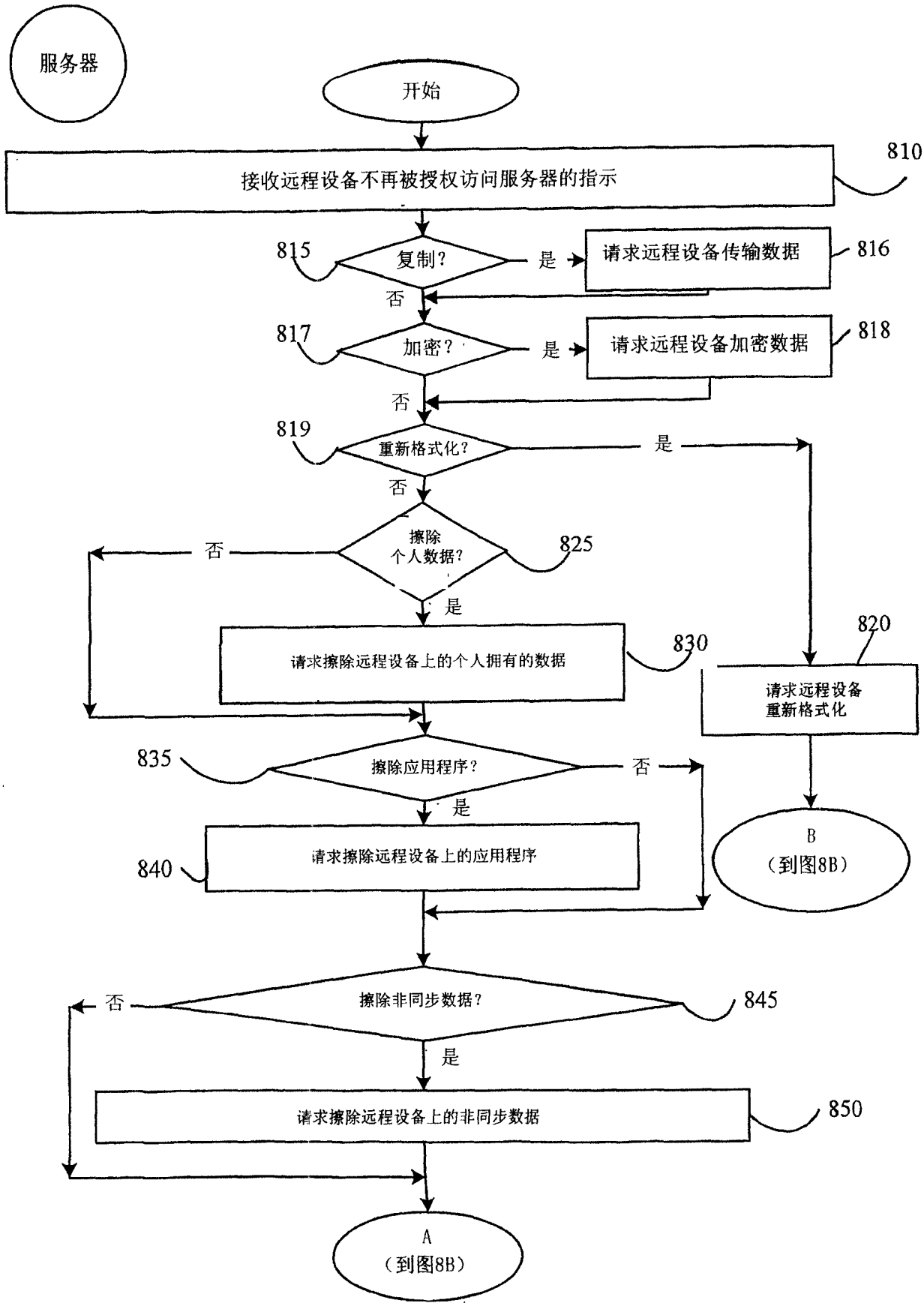

服务器
开始
接收远程设备不再被授权访问服务器的指示
810
复制?
是
请求远程设备传输数据
815
816
否
加密?
是
请求远程设备加密数据
817
818
否
重新格式化?
是
819
否
擦除
个人数据?
825
否
是
请求擦除远程设备上的个人拥有的数据
830
820
请求远程设备
重新格式化
835
擦除应用程序?
否
是
请求擦除远程设备上的应用程序
840
B
(到图8B)
擦除非同步数据?
845
否
是
请求擦除远程设备上的非同步数据
850
A
(到图8B)

图 8A

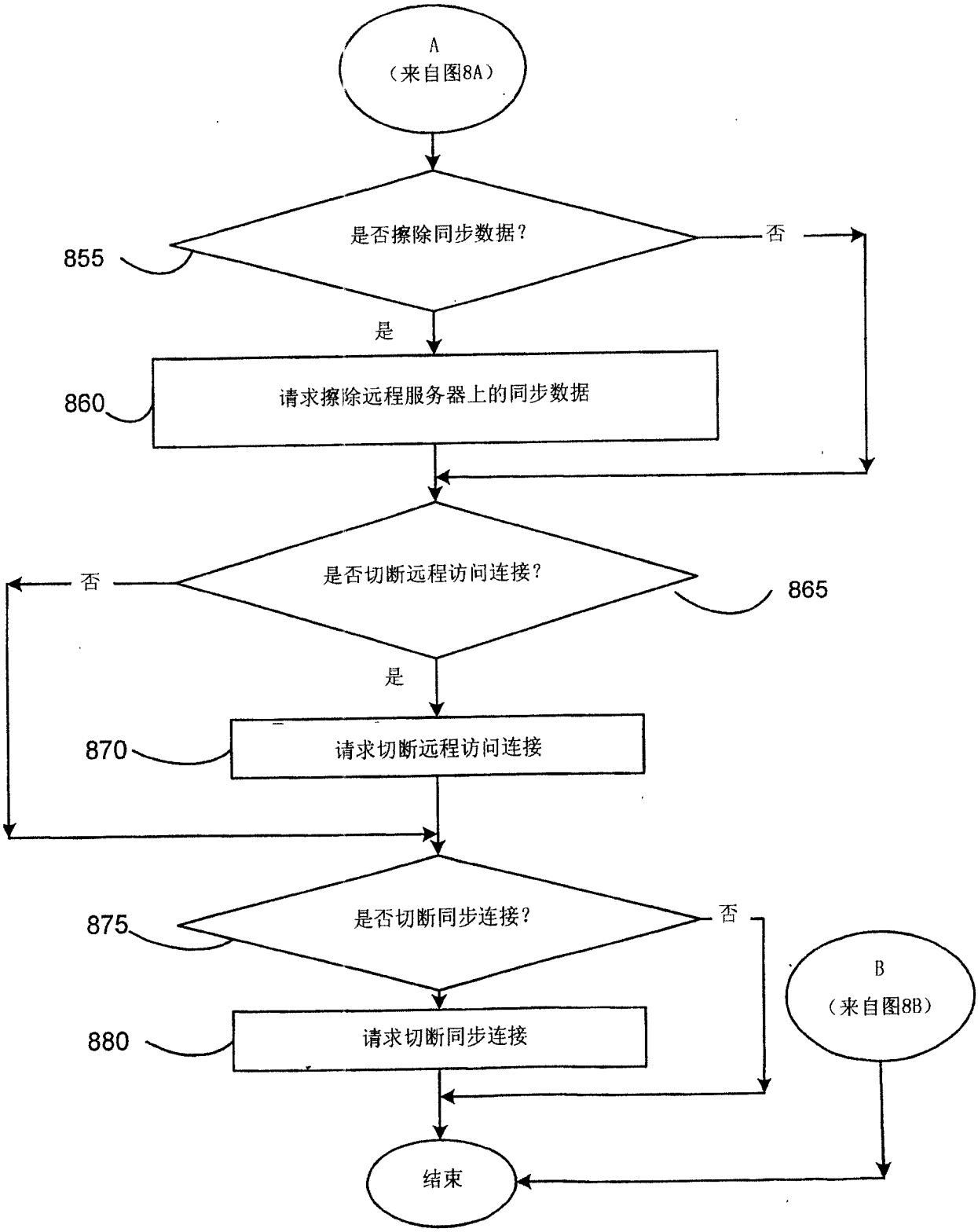

A
（来自图8A）
是否擦除同步数据？
855
否
是
请求擦除远程服务器上的同步数据
860
是否切断远程访问连接？
865
否
是
请求切断远程访问连接
870
是否切断同步连接？
875
否
请求切断同步连接
880
B
（来自图8B）
结束

图 8B

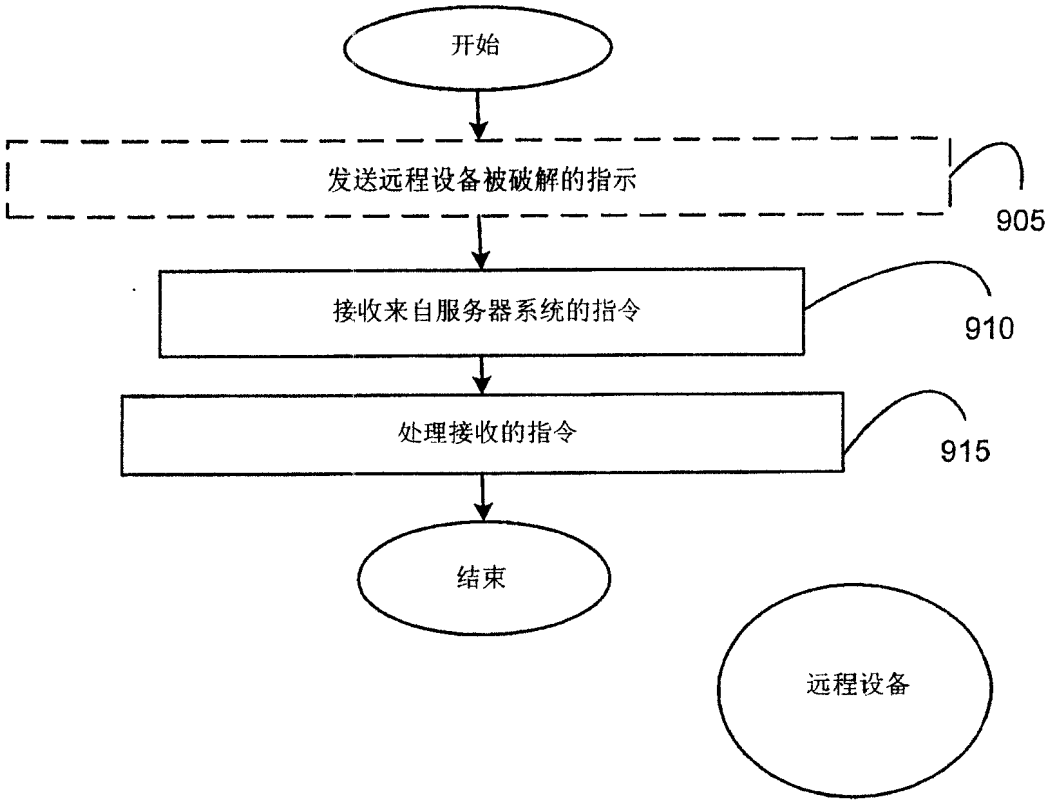


图 9A

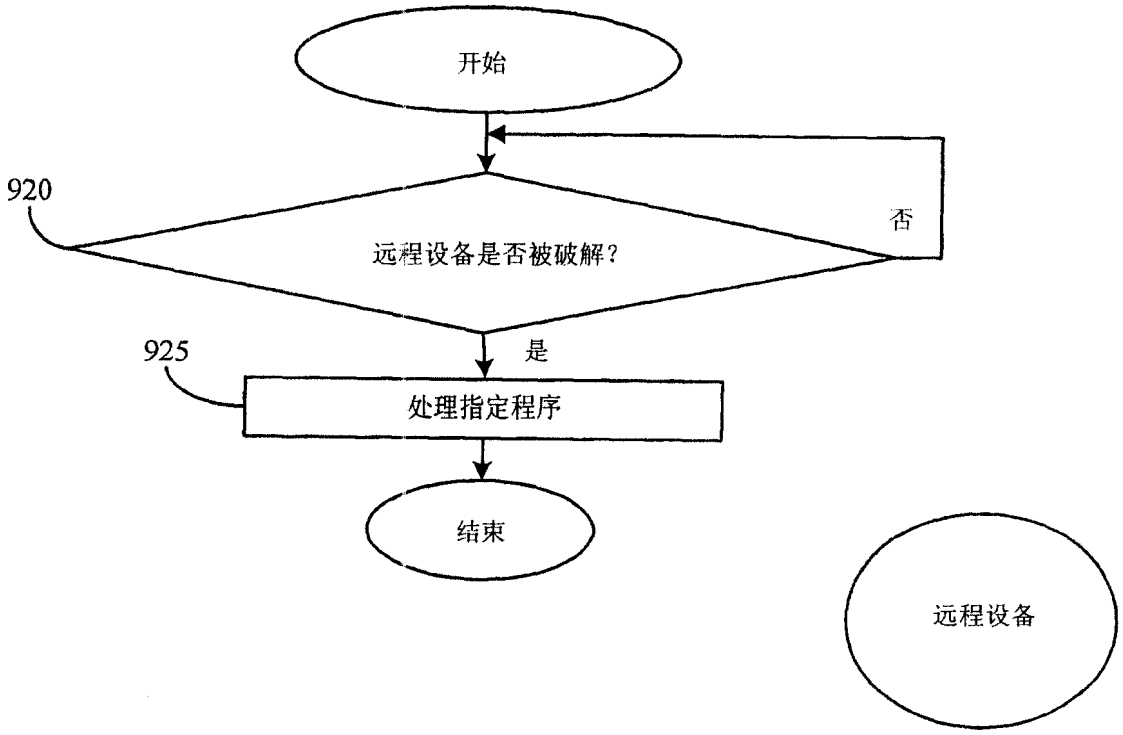


图 9B