(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105247529 B
(45)授权公告日 2018.07.31

(21)申请号 201480024568.5

(22)申请日 2014.04.30

(65)同一申请的已公布的文献号
申请公布号 CN 105247529 A

(43)申请公布日 2016.01.13

(30)优先权数据
13/873,882 2013.04.30 US

(85)PCT国际申请进入国家阶段日
2015.10.30

(86)PCT国际申请的申请数据
PCT/US2014/036004 2014.04.30

(87)PCT国际申请的公布数据
WO2014/179386 EN 2014.11.06

(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州

(72)发明人 J·M·卢克 A·N·戈登
R·N·希克卡玛盖勒
Z·埃尔马基 S·古本克
G·钱德尔 A·索马塞卡莱
M·D·萨塔戈潘

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 杨洁

(51)Int.Cl.
G06F 21/31(2006.01)
H04L 9/32(2006.01)

(56)对比文件
US 2013/0080765 A1,2013.03.28,
EP 1429228 A2,2004.06.16,
US 6986038 B1,2006.01.10,
CN 1409835 A,2003.04.09,
US 2004/0019786 A1,2004.01.29,
US 2008/0235772 A1,2008.09.25,

审查员 罗捷

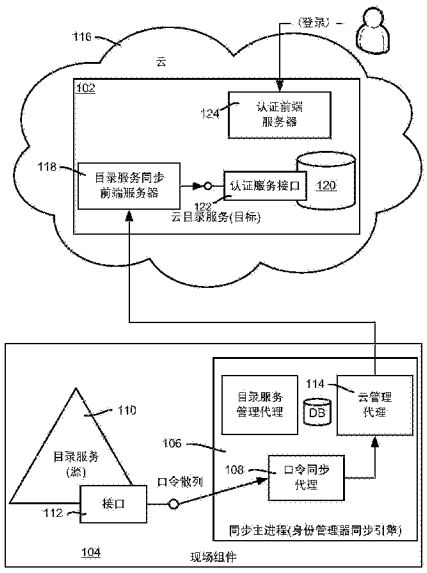
权利要求书1页 说明书9页 附图8页

(54)发明名称

在目录服务之间同步凭证散列

(57)摘要

本发明涉及将在源位置(例如,现场目录服务)处改变的口令安全地同步到目标位置(例如,云目录服务),使得相同凭证可被使用来登录到源和目标位置,但无需让每个域控制器处理该同步。明文口令未被展示,相反,使用从中计算的散列值来表示口令相关的数据。目标可接收主散列的次级散列,并且因此仅接收并存储口令团块。通过在目标服务处使用相同散列算法以计算团块并与经同步的团块进行比较来完成认证。还描述了密码灵活性和/或改变散列算法而不需要用户口令改变。



CN 105247529 B

1.一种在计算环境中用于同步凭证集合的方法,所述方法包括:

提供对应于上一次同步的同步时戳;

接收仅包括自上一次同步起所作的改变的经散列的凭证的集合;以及

将所述经散列的凭证的集合导出到目标服务,以用于身份认证。

2.如权利要求1所述的方法,其特征在于,所述经散列的凭证的集合用主散列算法来计算,并且所述方法还包括,使用次级散列算法将所述经散列的凭证的集合次级散列成受秘密保护的团块,所述次级散列算法对应于所述散列的凭证的集合以用于导出到所述目标服务。

3.如权利要求2所述的方法,其特征在于,将所述经散列的凭证的集合次级散列成所述受秘密保护的团块包括使用随机盐和迭代数量。

4.一种用于同步凭证集合的系统,包括:

目标目录服务;

具有多个域的域网格;

耦合到所述域网格的同步主进程,所述同步主进程配置用于与所述网格以外的所述目标目录服务同步在所述域网格中接收到的口令改变,包括:

接收表示来自所述域网格的明文口令的散列值;

使用次级散列算法对所述散列值进行附加散列以生成受秘密保护的团块;以及

将所述受秘密保护的团块导出到所述目标目录服务。

5.如权利要求4所述的系统,其特征在于,所述同步主进程通过次级散列算法和随机盐将所述散列值处理成所述受秘密保护的团块。

6.如权利要求4所述的系统,其特征在于,所述同步主进程耦合到网格服务以确定联系一个或多个域中的每一个中的哪个域控制器寻找口令改变数据。

7.如权利要求4所述的系统,其特征在于,所述散列值通过至少一个次级散列算法由运行在以下的同步主进程的至少一部分处理成所述受秘密保护的团块:

a)在每个域控制器上,

b)在耦合到现场服务器域网格的分开的机器上,或

c)在云机器或与所述域网格地理上分开的其它机器上。

8.如权利要求4所述的系统,其特征在于,所述目标目录服务配置有密码灵活性以在一身份的认证期间使用与该身份相关联的多个散列算法或散列算法组合的任何一种。

9.一种在目录服务之间同步凭证散列的方法,包括:

在目标服务维护包括对应于明文口令的受秘密保护的团块的数据的多个集合,每个受秘密保护的团块与一身份相关联,其中每个受秘密保护的团块从明文口令用至少两个散列算法的组合来计算并同步到所述目标服务;

在所述目标服务接收包括对应于身份和口令的凭证的登录尝试;

基于对所述口令执行至少一个散列算法来计算第一值;以及

将所述第一值与所述身份相关联的至少一个与受秘密保护的团块进行比较,以认证所述身份。

10.如权利要求9所述的方法,其特征在于,进一步包括将与身份相关联的团块用从至少一个不同散列算法计算的另一个团块来代替。

在目录服务之间同步凭证散列

[0001] 背景

[0002] 越来越多的组织正在使用云服务应用及资源而不是只使用现场应用和资源(其中与云相反,“现场”指在组织的控制下,不考虑任何物理位置)。与现场应用和资源一样,用户需要凭证来访问现存云服务。注意某些(通常很小的)组织仅将云用于他们基于凭证的身份基础结构和应用,并且这样使用云来处理基于凭证的认证。

[0003] 很大的组织现场运行目录服务(其一个示例是微软公司的包括其域控制器服务器的Active Directory®)来认证用户,并使应用发现用户帐户以及帐户之间的联系。此外,这允许这样的组织为安全的目的保留对它们的凭证相关的数据的完全控制而不是将数据提供给云。大的组织使用(例如,在Active Directory®场景中)可被称为联盟/联盟服务,其包括用于个体用户利用他们的现场凭证来访问云中的资源的机制。

[0004] 凭证不被同步;相反,云将登录请求等引导到现场身份基础结构以认证,允许用户仅登录一次。

[0005] 然而,联盟的安装和维护相对来说很昂贵,并且因此仅大组织趋向使用联盟。许多较小组织想要使用相同用户名和密码来访问现场资源和应用以及云资源和应用。然而,没有联盟,需要某种方式来处理现场凭证和云凭证。

[0006] 一种解决方案是截取明文用户口令来传输到目标目录服务。明文用户口令可被复制到身份基础结构中的全部服务器/数据库。然而,这可能是不安全的,特别是当云目录服务是目标时。此外,软件需要在目标目录服务的每个服务器上被配置以捕捉全部用户口令改变事件。除了其它缺点,这还是低效且不便于维护的。

[0007] 出于安全的理由,许多公司不想要将现场凭证数据释放到云,这导致认证问题。一种解决方案是发行一个凭证集合供用户来访问云应用,而另一凭证集合用于用户访问现场应用。这也是低效且不便于维护的。

[0008] 概述

[0009] 提供本概述以便以简化形式介绍将在以下的详细描述中进一步描述的一些代表性概念的选集。本概述不旨在标识出所要求保护的主题的关键特征或必要特征,也不旨在以限制所要求保护的主题的范围的任何方式来使用。

[0010] 简言之,在此描述的主题的各种方面指向将在源位置改变了的口令安全地同步到目标位置,使得相同的凭证可在源和目标位置被使用。在一个方面,基于明文口令计算的散列值被接收,其中散列值响应于在源服务处的口令改变事件被计算。对应于散列值的数据被导出到目标服务,以将新口令同步到目标服务供在身份认证中使用。对应于散列值的数据可以使用次级散列算法被次级散列成为受口令保护的团块。

[0011] 在一个方面,同步主进程被耦合到域网格。同步主进程被配置来将在域网格接收到的口令改变与网格外的目标目录服务(例如,云目录服务)进行同步。同步主进程从域网格获得代表明文口令的散列值、将散列值通过至少一个次级散列算法处理成受秘密保护的团块、将秘密保护的团块导出到目标目录服务。同步主进程可被耦合到网格的组件或耦合到网格的组件并获得来自网格的组件或耦合到网格的组件的散列值,其中组件被配置来接

收对应于在网格的任何域控制器处作出的口令改变的经复制的口令改变数据。

[0012] 在一个方面，包括对应于明文口令的受保护团块的多个数据集合被维护。每个团块与一个身份相关联，其中团块通过至少两个散列算法从明文口令计算。用另一个散列算法计算的另一个团块与身份相关联，包括通过用其它团块代替该团块。这可通过用其它散列算法为每个身份计算团块来实现，包括针对每个身份将与那个身份相关联的团块散列成针对那个身份的其它团块。这也可以通过从现场目录服务组件接收其它团块并接收标识对应于该其它散列算法的信息的信息来实现。

[0013] 结合附图阅读以下详细描述，本发明的其他优点会变得显而易见。

[0014] 附图简述

[0015] 作为示例而非限制，在附图中示出了本发明，附图中相同的附图标记指示相同或相似的元素，附图中：

[0016] 图1是根据一个示例实施例的表示配置用于将在现场目录服务处作出的口令改变同步到云目录服务的示例组件的框图。

[0017] 图2是根据一个或多个示例实施例的表示可在将在源目录服务处的口令改变安全地同步到目标目录服务中被采用的示例步骤的流程图。

[0018] 图3是根据一个示例实施例的表示配置用于通过单个组件将在任何域控制器处作出的口令改变同步到云目录服务的示例组件的框图。

[0019] 图4是根据一个示例实施例的表示可在安全口令同步操作中始终被采用的示例步骤的流程图。

[0020] 图5是根据一个示例实施例的表示可被采用以在登录尝试期间使用安全地同步了的口令相关的数据来认证用户的示例步骤的流程图。

[0021] 图6是根据一个示例实施例的表示可被采用来改变次级散列算法和为一组用户维护的口令相关数据的示例步骤的流程图。

[0022] 图7是示出其中可实现本文中描述的各个实施例的示例性非限制联网环境的框图。

[0023] 图8是示出其中可实现本文中所描述的各个实施例的一个或多个方面的示例性非限制计算系统或操作环境的框图。

[0024] 详细描述

[0025] 在此描述的技术的各方面通常涉及允许凭证的单个集合被用于现场资源访问和云资源访问两者的口令同步技术。如将理解的，该技术提供了相对直接的安装和维护现场而同时安全的解决方案。

[0026] 在一个方面，同步代理执行来自现场目录服务的与云目录服务的同步操作。在一个实现中，同步代理可被添加到域控制器网格作为(例如，运行在加入域的单个机器上的)单个组件(相对于运行在域网格中的每个域控制器上而言)。

[0027] 在一个方面，维护在现场目录服务中的凭证通过首先使用一个或多个散列算法来散列口令来与云目录服务进行同步。主散列被使用，并且可与至少一个次级散列组合使用。明文口令从不发送到云。

[0028] 在一个方面，该技术支持使得现场系统切换到新主散列算法，无需要求用户改变他们现有口令或以其他方式重新捕捉用户的明文口令。此外，如果次级散列算法受损或更

安全的次级散列算法以其他方式变得想要使用，次级散列算法可被改变无需要求用户改变他们的现有口令或以其他方式重新捕捉用户的明文口令。

[0029] 应当理解，本文中的任何示例均是非限制的。例如，在此的许多示例在目录服务环境(诸如Active Directory®)中一般地描述；然而，任何类似的身份基础结构/环境可从在此描述的技术获益。此外，尽管各示例指向安全凭证同步，需要被安全地同步的其它类型数据可从在此描述的技术获益。因此，本发明不限制于本文所述的任何具体的实施例、方面、概念、结构、功能或示例。相反，本文所述的实施例、方面、概念、结构、功能或示例中的任一个都是非限制性的，并且可用一般在数据同步、数据安全和/或云服务方面提供好处和优点的各种方式来使用本发明。

[0030] 图1是示出可被用于将包括来自现场组件的凭证数据的数据安全地同步到云目录服务102的示例组件的框图。现场组件104包括包括口令同步代理108的同步主进程106(例如，身份管理器同步引擎)。一般而言，同步主进程106包括主动驱动来自源目录服务110的凭证的检索和导出的进程。

[0031] 在一个实现中，同步通过口令同步代理108来实现，其通过合适的接口112调用现场(本地)目录服务108以获得如下面描述的包括经散列的口令的凭证相关数据。为了仅获得自上一次同步时间起经改变的经散列的口令(增量)，，调用可提供同步时戳。例如，Active Directory®具有公开建档的API(IDL_DRSGetNCChanges)，在被调用时其检索并返回自所提供的时戳起的改变的列表，所提供的时戳是口令同步代理108提供的上一次同步时间。在改变数据包括口令相关数据以外的内容的情形中，同步代理108解析/过滤所返回的数据来确定自上一次同步时间起的经更新的凭证集合。

[0032] 经改变的凭证的集合作为经散列的凭证的集合被返回到口令同步代理108。在一个实现中，这些散列不被同步主进程106或口令同步代理108持久存储，并且仅临时用于将凭证散列同步到目标目录服务(例如，图1中的云目录服务102)的尝试中。在一个实现中，在被发送到目标(云)目录服务102之前，使用随机生成的(盐)值和迭代数量来对现场口令散列进行次级散列。

[0033] 在一个实现中，口令同步代理108尝试仅将范围内(其中范围是身份体系结构中的公知概念)身份的凭证同步到目标目录服务102。属于范围外身份的凭证不被同步到目标目录服务102。此外，属于未被提供给目标目录服务102的凭证也不被同步；相反它们可在稍候时间当该身份已经被在目标目录服务102中被成功地提供时被同步。

[0034] 在图1中，被表示为云管理代理114的目标目录连接器组件负责处理经散列的凭证到云116的导出。为此，云前端组件118(例如，目录服务同步前端服务器)接收更新凭证的请求，并接着尝试通过(例如，私有)编程性接口122将经散列的凭证持久存储在目标目录服务存储系统120中。如果凭证散列成功地持久存储在目标目录服务中，成功状态被返回前端组件118并且前端组件118将成功状态返回给同步主进程106。在接收到“成功”响应时，同步主进程106认为凭证成功地同步到目标目录服务102。如果遇到失败响应，该导出可被排队以在稍候时间重新尝试。

[0035] 图2将上面的操作作为示例步骤集合来示出。这些步骤中的一些针对单个凭证示出，然而，如能够被容易地理解的，凭证同步可被批量处理，和/或步骤中的某些或全部可并

行执行。

[0036] 在步骤202，口令同步代理108(图1)请求并从源目录服务110接收(自给定时戳起的)改变。请求在同步时作出，其可以是周期性的或以其它方式。如上面描述的，口令用主散列函数，例如Ha(口令)，诸如MD4(口令)来进行散列。

[0037] 在接收改变之后，如在步骤204所表示的，口令同步代理108解析改变以确定哪些要被同步，例如，是范围内提供的身份的口令改变。如上面所提及的，考虑在此时仅一个凭证正被处理。

[0038] 步骤206表示次级散列经散列的口令，例如H1(Ha(口令))诸如SHA256(MD4(口令))。以下进一步描述次级散列。

[0039] 步骤208将经散列的凭证导出到目标目录服务102，目标目录服务102尝试持久存储它。步骤210将导出请求的结果作为返回的状态来接收；如果在步骤212如估计的那样接收到成功，凭证被成功地同步到目标目录服务(步骤214)且进程结束。如果通过步骤212检测到失败，该导出可被排队以在稍候时间重新尝试，如步骤216所表示的。

[0040] 如一般地由图3所表示的，现场域网格330包含(具有域1控制器1－域1控制器j的)域1到(具有域n控制器1－域n控制器k的)域n。在一个方面，网格可添加(例如加入或以其他方式耦合到)运行在机器等上面的组件，该组件作为目录服务域控制器定位器服务332来运行。如所知的，口令改变在一个域控制器处作出(例如，离用户最近的，尽管其它方案是可行的)并复制到该域的其它域控制器。如在此描述的，用主散列进行散列的改变了的口令被复制，而非明文口令。

[0041] 同步主进程106与目录服务域控制器定位器服务332进行通信来确定控制器实例，从中检索凭证改变数据。例如，存在在每个域中被标识的一个域控制器来向同步主进程106提供改变。以此方式，现有的网格复制方案可被利用来执行与云服务的口令改变同步；(注意这与其中组件/代码扩展DLL需要在与源目录/网格相关联的所有机器上注册以确保全部凭证改变被捕捉并同步到目标目录的现有系统相反)。

[0042] 图4一般地概述了与图3的实现相关的示例步骤和域控制器操作。步骤402表示以明文接收口令改变，其通常在距离用户最近的域控制器处(尽管其它方案，诸如基于负载平衡，是可行的)。步骤404表示在那个域控制器处使用主散列，例如Ha(口令)被散列的口令。步骤406表示将经散列的口令复制到其它域控制器。

[0043] 步骤408表示同步主进程106与目录服务域控制器定位器服务332进行通信来确定联系哪个(些)域控制器来寻找改变数据。一般而言，来自每个域的一个域控制器由域控制器定位器服务332向同步主进程106标识。

[0044] 步骤410表示从目录服务域控制器检索改变后的口令散列的口令同步代理。注意作为替换，改变可被推送到口令同步代理用于按需或以某个其它安排同步。同步主进程运行在与目录服务域控制器定位器服务332相同机器上是可行的，尽管如上面描述的，同步主进程不持久存储所需之外的经散列的口令以执行与目标服务的同步。

[0045] 尽管与目标同步并存储经散列的口令是可行的，进行次级散列提供了在此描述的若干益处。步骤412表示次级散列，例如H1(Ha(口令))。在一个方面，次级散列生成受保护的口令团块，其包括散列算法名称和版本，加上随机盐，迭代计数加上摘要。此次级散列的结果在目标目录服务被同步(步骤414)并被存储(步骤416)。注意，云还可执行这样的次级散

列，诸如在存储前再次散列。

[0046] 转到登录方面，当一身份例如通过认证前端服务器(AuthN front end sever)124(图1)试图访问与目标目录服务相关联的服务或软件(如果凭证在目标目录服务的认证平台中被标记为“从源目录同步”)时，认证平台理解以执行合适的登录验证过程，并将由该身份所呈现的凭证与从源目录同步的凭证散列进行比较。

[0047] 目标认证平台被指令来使用算法以匹配现场散列算法，但这可以是任何一个算法或算法集合。这便于多个情形，包括密码灵活性。一般而言，密码灵活性允许多个散列算法，和/或散列算法的组合被使用。结果，主散列算法可随时间改变，次级散列算法可随时间改变，不同服务(例如，第三方)的算法可被使用，等等。

[0048] 图5示出了与在云服务处的登录操作相关的某些示例步骤，在步骤502开始，其中接收用凭证登录的尝试。如果在步骤504，凭证不被标识为“从源目录同步”等，那么例如云正被不是现场目录服务的部分的用户(诸如仅使用云来进行认证和资源访问的很小的组织的用户)访问。而且，用户可以是现场目录服务的部分但不使用在此描述的技术，并且因此凭证不被标记为经同步。如果这样，步骤506以其他方式处理此请求，例如通过传统云登录。

[0049] 如果相反，步骤504检测凭证被标记为“从源目录同步”，那么步骤508，例如基于用户身份来查询哪个散列算法/数据来使用。步骤510确定这个散列的参数，例如，盐和迭代。注意，在其中仅存在一个散列算法的情形中，步骤508和510不需要，但是可以容易地理解，这些步骤提供密码灵活性。

[0050] 步骤512将登录口令数据转换到受保护的口令团块，步骤514将受保护的口令团块与存储在目标服务的数据库上的团块进行比较。如果存在匹配(步骤516)，则经由步骤518允许访问，否则，访问经由步骤520被拒绝。

[0051] 注意，密码灵活性支持新现场(主)散列算法(Ha)而不影响服务并且无需重新捕捉用户的明文口令。例如，考虑现场系统从Ha切换到Hb(例如，目录服务的下一个版本拒绝MD4有利于更现代的某些事情)。任何新口令/经改变的口令将被计算并同步为(H1(Hb(口令)))。在登录时，当用户键入他们的用户名和(明文)密码时，系统确定(H1(Ha))或(H1(Hb))是否存在在数据库中，并将合适的一个应用到明文密码来进行比较。

[0052] 此外，认证平台可按需对存储的散列执行附加的散列。这促进了对有密码灵活性的静止口令的耐久的数据保护。作为示例，考虑次级散列算法(H1)受损，即，不在被认为足够安全。H1散列算法可被有效地代替，无需重新捕捉用户的明文口令。

[0053] 作为示例，考虑当前计算的和存储的数据团块是H1(Ha(口令))。为了安全，新的次级散列算法(H2)被引入。如在图6的步骤602、604和606所表示的，对于每个用户，目标系统解析整个数据库，计算(H2(H1(Ha(口令)))，并存储新值。当随着在步骤608被评估解析完成时，系统在步骤610为全部用户删除(H1(Ha(口令)))并切换以使用(H2(H1))算法。因此，目标系统不再存储所包括的静止散列。注意在步骤606代替现有团块是可行的，然而，如果解析过程冗长，用户可能被阻止登录直到解析过程完成。

[0054] 在登陆时，从用户的角度看诸事如从前一样进行。随着用户登录，目标确定(H2(H1(Ha)))是要为所提供的口令计算散列值的散列算法并将散列值与所存储的进行比较。

[0055] 目标系统还可针对新口令切换到另一散列函数。例如，考虑另一散列算法H3被开发，其被认为在某些方面相比现有的高级，例如，H3远好于和/或快于H1。在此示例中，改变

不是安全问题，并且因此(H1(Ha(口令)))是安全的，并且保留不变。同步主进程(和目标服务)被更新以支持任何新用户/经改变的口令(H3)。改变他们的口令的用户因此使用(H3(Ha(口令)))来被同步。未改变他们的口令的用户继续通过(H1(Ha(口令)))算法来认证。

[0056] 口令历史可被维护在云服务中并且在登录时被使用以避免将用户锁出。例如，考虑已经在一个设备上改变了他或她的口令的用户，导致将团块同步到云服务，但是还没有在另一设备上改变口令。该另一设备可能有规律地使用先前的口令与登录服务进行通信，这可能导致问题。为避免这个问题，用户提供的明文口令可与存储为“当前口令”的现有团块进行比较，并且如果不匹配就与存储为“先前口令”的团块进行比较。一个或多个口令团块的任何想要的数量的先前集合可被维持，例如当前口令加上前两个口令也可行，等等。

[0057] 此外，口令历史限制可以用静止散列来加强，例如，对不在现场改变他们的口令的用户。例如，考虑用户不被允许重新使用他们五个先前口令中的任何口令的策略。云服务存储最新口令团块，诸如(H3(Ha(当前口令)))，以及口令历史，诸如(H3(Ha(前一口令)))、(H1(Ha(前二口令)))；(H2((H1(Ha(前三口令)))等，直到策略限制。注意这些团块不需要已经用相同散列算法生成。事实上，如果最初散列被发现不安全或以其他方式被改变，那么它们的某些可能已经被重新散列。

[0058] 在口令改变时，当新口令被收集时，服务在口令历史区域中查找算法列表，计算对应散列，并将它们与存储的摘要进行比较来确定改变是否被允许。

[0059] 示例性联网以及分布式环境

[0060] 本领域技术人员可以理解，此处描述的各实施例和方法可结合任何计算机或其它客户机或服务器设备来实现，其可被部署为计算机网络的部分或在分布式计算环境中，并且可以被连接到任何类型一个或多个数据存储。在这一点上，此处描述的各实施例可在具有任何数量的存储器或存储单元的、并且任何数量的应用和进程跨任何数量的存储单元发生的任何计算机系统或环境中实现。这包括但不限于具有部署在具有远程或本地存储的网络环境或分布式计算环境中的服务器计算机和客户计算机的环境。

[0061] 分布式计算通过计算设备和系统之间的通信交换来提供计算机资源和服务的共享。这些资源和服务包括信息的交换、对于诸如文件之类的对象的高速缓存存储和盘存储。这些资源和服务还包括多个处理单元之间的处理能力共享以便进行负载平衡、资源扩展、处理专门化等等。分布式计算利用网络连接，从而允许客户机利用其集体力量来使整个企业受益。就此，各种设备可具有可如参考本发明的各实施例描述地参与资源管理机制的应用、对象或资源。

[0062] 图7提供了示例性的联网或分布式计算环境的示意图。该分布式计算环境包括计算对象710、712等以及计算对象或设备720、722、724、726、728等，这些计算对象或设备可包括如由示例应用730、732、734、736、738表示的程序、方法、数据存储、可编程逻辑等。可以理解，计算对象710、712等以及计算对象或设备720、722、724、726、728等可包括不同的设备，诸如个人数字助理(PDA)、音频/视频设备、移动电话、MP3播放器、个人计算机、膝上型计算机等。

[0063] 每一个计算对象710、712等以及计算对象或设备720、722、724、726、728等可通过通信网络740直接或间接与一个或多个其他计算对象710、712等以及计算对象或设备720、722、724、726、728等进行通信。尽管在图7中被示为单个元素，但通信网络740可包括向图7

的系统提供服务的其他计算对象和计算设备和/或可表示未示出的多个互连网络。每个计算对象710、712等或计算对象或设备720、722、724、726、728等还可以包含应用，诸如可以利用API或其他对象、软件、固件和/或硬件的、适于根据本公开的各实施例所提供的应用的实现或与其进行通信的应用730、732、734、736、738。

[0064] 存在支持分布式计算环境的各种系统、组件和网络配置。例如，计算系统可由有线或无线系统、本地网络或广泛分布的网络连接在一起。当前，许多网络被耦合至因特网，因特网为广泛分布的计算提供了基础结构并包含许多不同的网络，但任何网络基础结构都可用于便于与如各实施例中所描述的系统的示例通信。

[0065] 由此，可使用诸如客户机/服务器、对等、或混合架构之类的众多网络拓扑结构和网络基础结构。“客户机”是使用与其无关的另一类或组的服务的一类或组中的成员。客户机可以是进程，例如大致上是请求由另一程序或进程提供的服务的指令或任务集合。客户机进程使用所请求的服务，而无需“知道”关于其他程序或服务本身的任何工作细节。

[0066] 在客户机/服务器架构中，尤其在联网系统中，客户机通常是访问另一计算机(例如，服务器)所提供的共享网络资源的计算机。在图7的图示中，作为非限制性示例，计算对象或设备720、722、724、726、728等可被认为是客户机，而计算对象710、712等可被认为是服务器，其中作为服务器的计算对象710、712等提供数据服务，诸如从客户机计算对象或设备720、722、724、726、728等接收数据、存储数据、处理数据、向客户机计算对象或设备720、722、724、726、728等发送数据，但取决于环境，任何计算机都可被认为是客户机、服务器、或两者。

[0067] 服务器通常是可通过诸如因特网或无线网络基础结构之类的远程网络或本地网络访问的远程计算机系统。客户机进程可在第一计算机系统中活动，而服务器进程可在第二计算机系统中活动，它们通过通信介质相互通信，由此提供分布式功能性并允许多个客户机利用服务器的信息收集能力。

[0068] 在通信网络740或总线是因特网的网络环境中，例如，计算对象710、712等可以是其他计算对象或设备720、722、724、726、728等经由诸如超文本传输协议(HTTP)之类的多种已知协议中的任一种与其通信的Web服务器。计算对象710、712等作为服务器还可用作例如计算对象或设备720、722、724、726、728等的客户机，分布式计算环境的特点就是如此。

[0069] 示例计算设备

[0070] 如上所述，有利地，本文所描述的技术可被应用于任何设备。因此，可理解，构想了结合各实施例使用的所有种类的手持式、便携式和其它计算设备和计算对象。因此，以下在图8中所述的通用远程计算机只是计算设备的一个示例。

[0071] 各实施例可部分地经由操作系统来实现，以供设备或对象的服务开发者使用，和/或被包括在用于执行本文中所述的各实施例的一个或多个功能方面的应用软件内。软件可以在由诸如客户机工作站、服务器或其它设备等一个或多个计算机执行的诸如程序模块等计算机可执行指令的通用上下文中描述。本领域的技术人员将理解，计算机系统具有可用于传递数据的各种配置和协议，并且由此没有特定配置或协议应当被认为是限制性的。

[0072] 图8由此示出了其中可实现本文所述的各实施例的一个或多个方面的合适的计算系统环境800的示例，尽管如上所述，计算系统环境800仅为合适的计算环境的一个示例且不旨在对使用或功能范围提出任何限制。另外，计算系统环境800也不旨在被解释为对在示

例计算系统环境800中所例示的组件中的任何一个或其组合有任何依赖。

[0073] 参考图8，用于实现一个或多个实施例的示例性远程设备包括计算机810形式的通用计算设备。计算机810的组件可包括但不限于：处理单元820、系统存储器830以及将包括系统存储器在内的各种系统组件耦合到处理单元822的系统总线820。

[0074] 计算机810通常包括各种计算机可读介质，并且可以是可由计算机810访问的任何可用介质。系统存储器830可包括诸如只读存储器(ROM)和/或随机存取存储器(RAM)之类的易失性和/或非易失性存储器形式的计算机存储介质。作为示例而非限制，系统存储器830还可包括操作系统、应用程序、其他程序模块、以及程序数据。

[0075] 用户可通过输入设备840向计算机810输入命令和信息。监视器或其他类型的显示设备也经由诸如输出接口850之类的接口连接到系统总线822。除监视器以外，计算机还可包括诸如扬声器和打印机之类的其他外围输出设备，它们可通过输出接口850连接。

[0076] 计算机810可使用到一个或多个其他远程计算机(诸如远程计算机870)的逻辑连接在联网或分布式环境中操作。远程计算机870可以是个人计算机、服务器、路由器、网络PC、对等设备或其他常见网络节点、或者任何其他远程媒体消费或传输设备，并且可包括以上关于计算机810所述的任何或全部元件。图8所示的逻辑连接包括诸如局域网(LAN)或广域网(WAN)之类的网络872，但也可包括其他网络/总线。这些联网环境在家庭、办公室、企业范围的计算机网络、内联网和因特网中是常见的。

[0077] 如上所述，尽管结合各种计算设备和网络体系结构描述了各示例性实施例，但基本概念可被应用于其中期望改进资源使用的效率的任何网络系统和任何计算设备或系统。

[0078] 而且，存在实现相同或相似功能性的多种方法，例如适当的API、工具箱、驱动程序代码、操作系统、控件、独立或可下载软件对象等，它们使得应用和服务能够利用本文中提供的技术。由此，本文中的各实施例从API(或其他软件对象)的观点以及从实现如本文中描述的一个或多个实施例的软件或硬件对象构想。由此，本文中所述的各实施例可具有完全采用硬件、部分采用硬件并且部分采用软件、以及采用软件的方面。

[0079] 本文中所使用的词语“示例性”意味着用作示例、实例、或说明。为避免疑惑，本文所公开的主题不限于这些示例。另外，在此所述的被描述为“示例性”的任意方面或设计并不一定要被解释为相比其它方面或设计更优选或有利。此外，在使用术语“包括”、“具有”、“包含”和其他类似词语的程度上，为避免疑惑，这些术语旨在当用于权利要求中时以类似于术语“包括”作为开放的过渡词的方式是包含性的而不排除任何附加或其他元素。

[0080] 如所述的，本文中所述的各种技术可结合硬件或软件或，在适当时，以两者的组合来实现。如此处所使用的，术语“组件”、“模块”、“系统”等旨在指计算机相关实体，或者是硬件、硬件和软件的组合、软件或者是执行中的软件。例如，组件可以是但不限于在处理器上运行的进程、处理器、对象、可执行件、执行的线程、程序、和/或计算机。作为说明，在计算机上运行的应用和计算机都可以是组件。一个或多个组件可驻留在进程和/或执行的线程内，并且组件可位于一个计算机上和/或分布在两个或更多的计算机之间。

[0081] 前述系统已经参考若干组件之间的交互被描述。可以理解，这些系统和组件可包括那些组件或指定的子组件、某些指定的组件或子组件、和/或附加的组件，并且根据上述内容的各种置换和组合。子组件还可作为通信地耦合到其他组件的组件来实现，而不是被包括在父组件内(分层的)。另外，可注意到一个或多个组件可被组合成提供聚集功能性的

单个组件，或被分成若干单独的子组件，且诸如管理层等任何一个或多个中间层可被提供来通信地耦合到这样的子组件以便提供集成的功能性。本文中所述的任何组件也可与本文中未专门描述但本领域技术人员一般已知的一个或多个其他组件进行交互。

[0082] 鉴于本文所述的示例性系统，可根据参考各附图的流程图还可理解根据所述的主题来实现方法。尽管为了阐述简洁起见，这些方法被示为和描述为一系列框，但是要理解和领会各实施例不受框的次序的限制，因为一些框可以与本文中所描绘和描述的不同次序发生和/或与其他框并发地发生。尽管经由流程图示出了非顺序或分支的流程，但可以理解，可实现达到相同或类似结果的各种其他分支、流程路径和框的次序。此外，一些所示的框在实现下面所述的方法时是任选的。

[0083] 结语

[0084] 尽管本发明易于作出各种修改和替换构造，但其某些说明性实施例在附图中示出并在上面被详细地描述。然而应当了解，这不旨在将本发明限于所公开的具体形式，而是相反地，旨在覆盖落入本发明的精神和范围之内的所有修改、替换构造和等效方案。

[0085] 除本文中所述的各实施例以外，要理解，可使用其他类似实施例，或者可对所述(诸)实施例作出修改和添加以便执行对应的(诸)实施例的相同或等效功能而不背离这些实施例。此外，多个处理芯片或多个设备可共享本文中所述的一个或多个功能的性能，并且类似地，存储可跨多个设备实现。因此，本发明不限于任何单个实施例，而是要根据所附权利要求书的广度、精神和范围来解释。

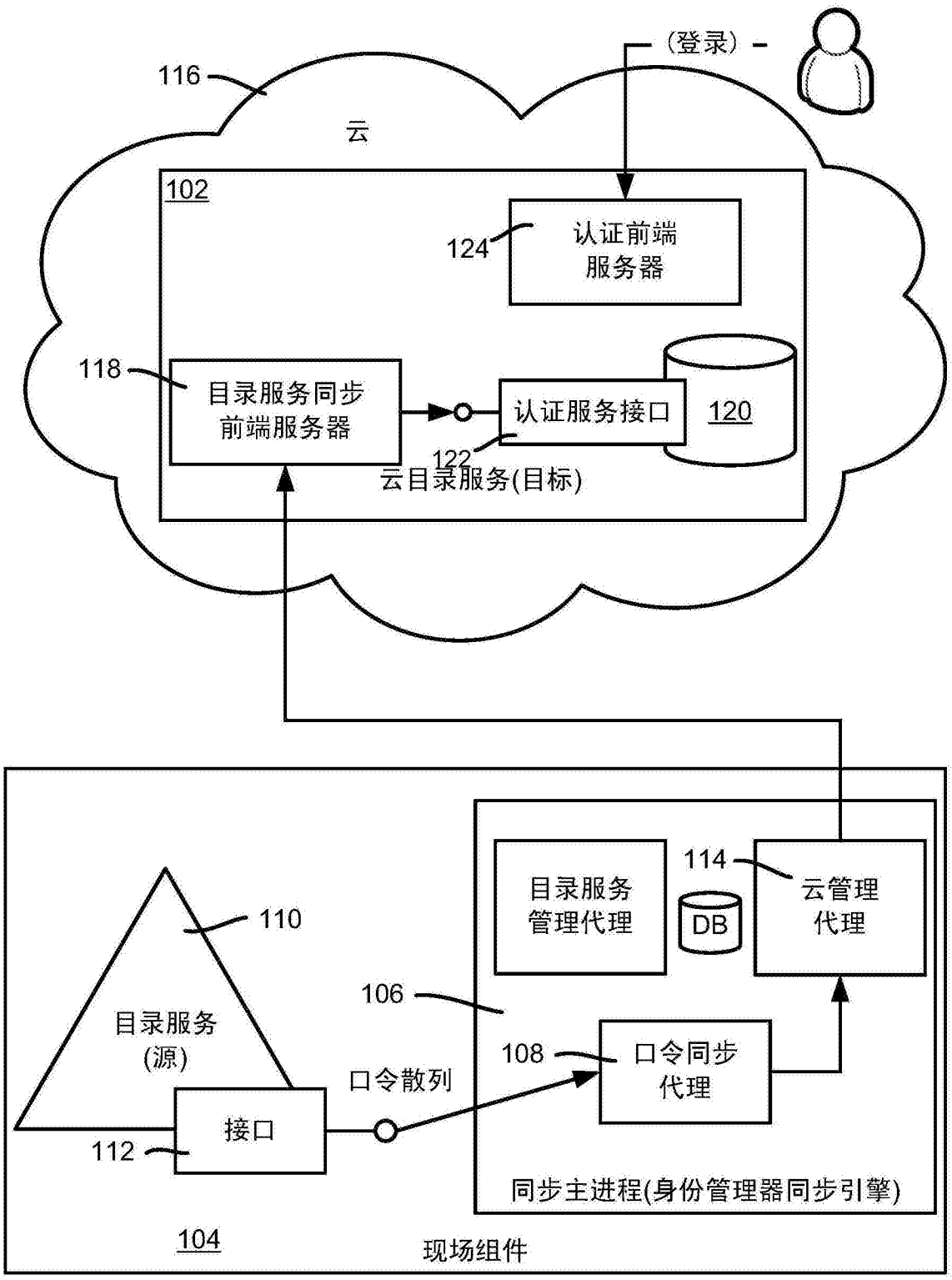

(登录)
116
云
102
124
认证前端
服务器
118
目录服务同步
前端服务器
认证服务接口
120
122
云目录服务(目标)
114
目录服务
管理代理
DB
云管理
代理
110
106
目录服务
(源)
108
口令同步
代理
口令散列
接口
112
同步主进程(身份管理器同步引擎)
104
现场组件

图1

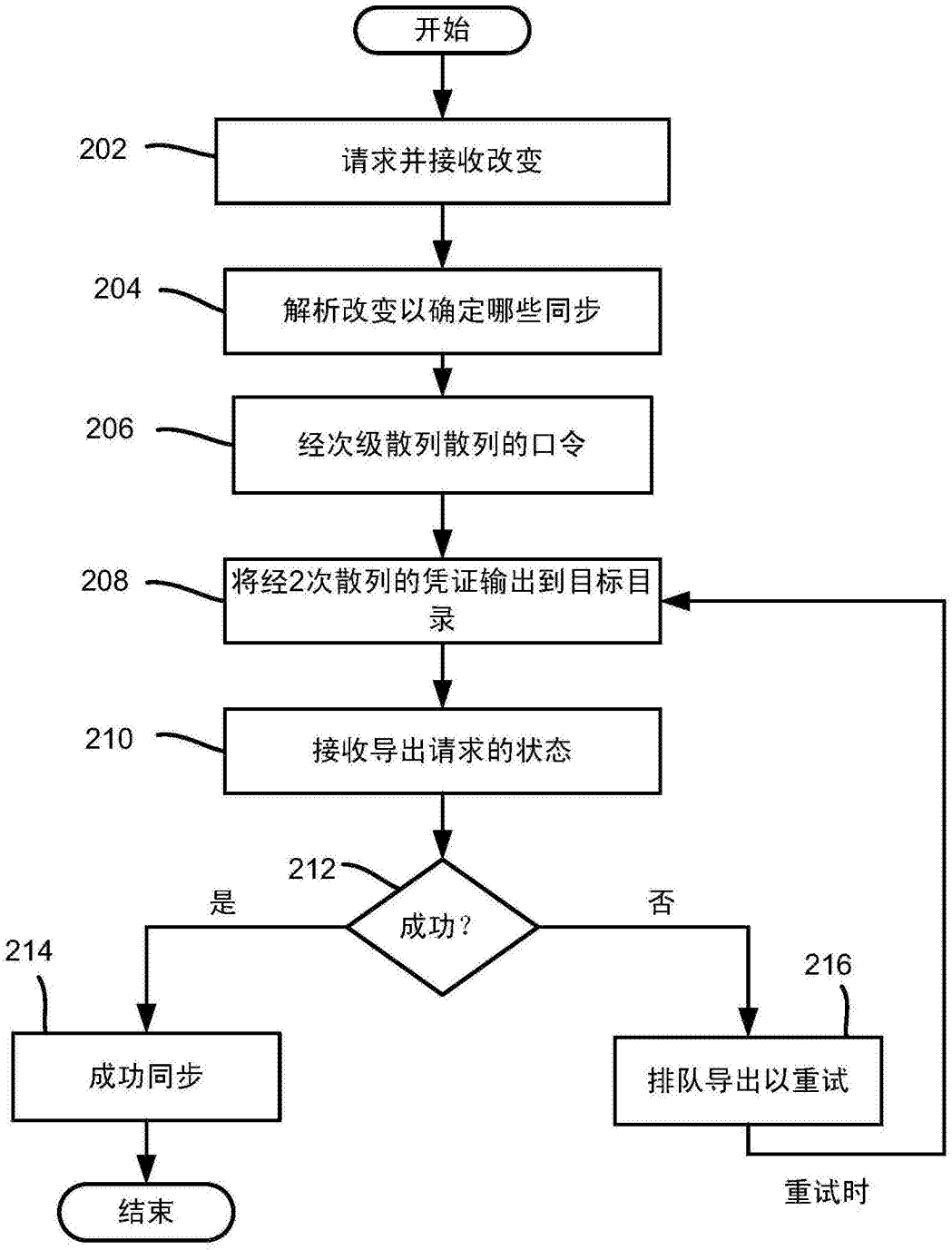

开始
202
请求并接收改变
204
解析改变以确定哪些同步
206
经次级散列散列的口令
208
将经2次散列的凭证输出到目标目录
210
接收导出请求的状态
212
成功?
是
否
214
成功同步
216
排队导出以重试
结束
重试时

图2

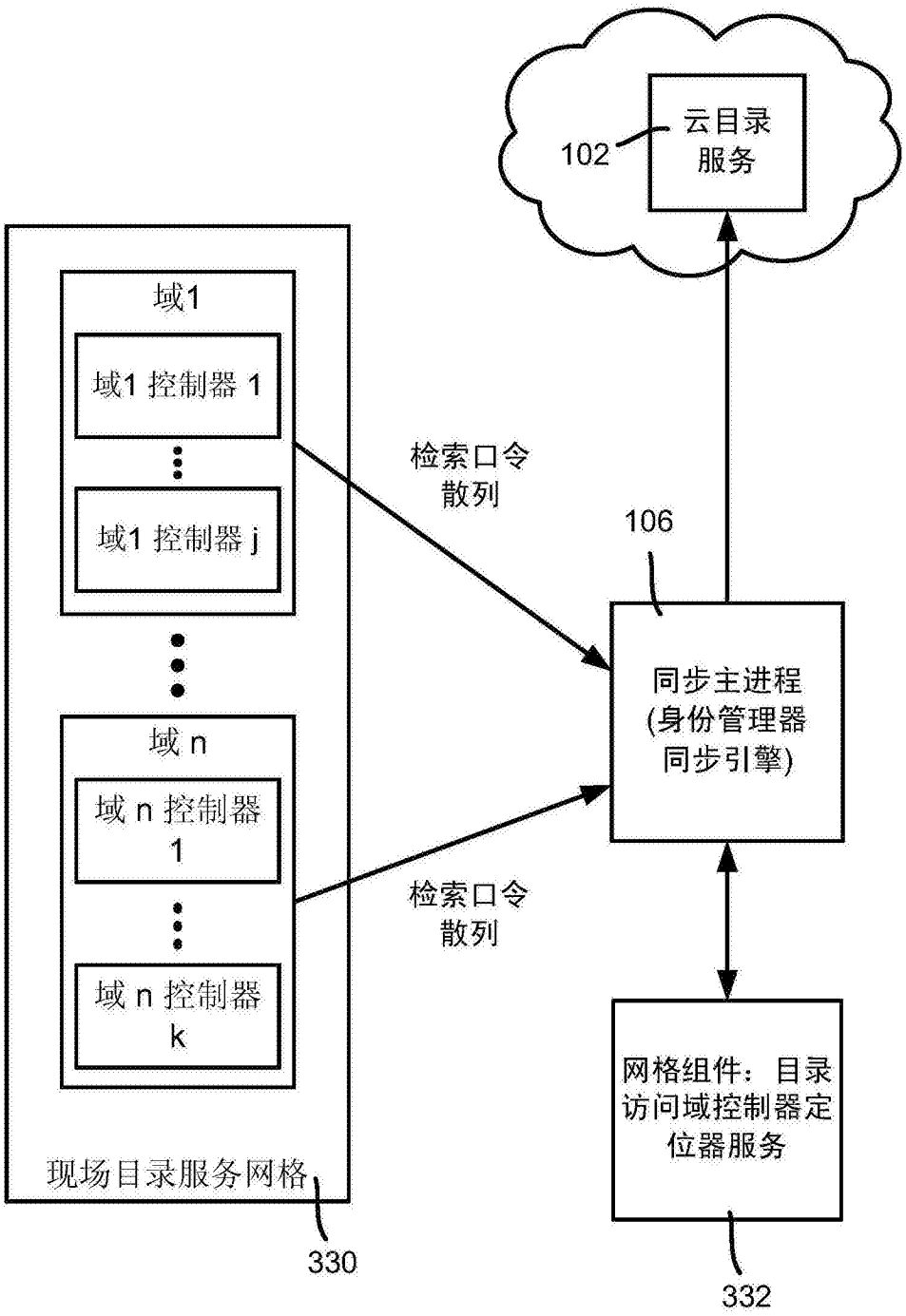

云目录
服务
102
域1
域1 控制器 1
域1 控制器 j
域 n
域 n 控制器
1
域 n 控制器
k
现场目录服务网格
330
检索口令
散列
检索口令
散列
106
同步主进程
(身份管理器
同步引擎)
网格组件：目录
访问域控制器定
位器服务
332

图3

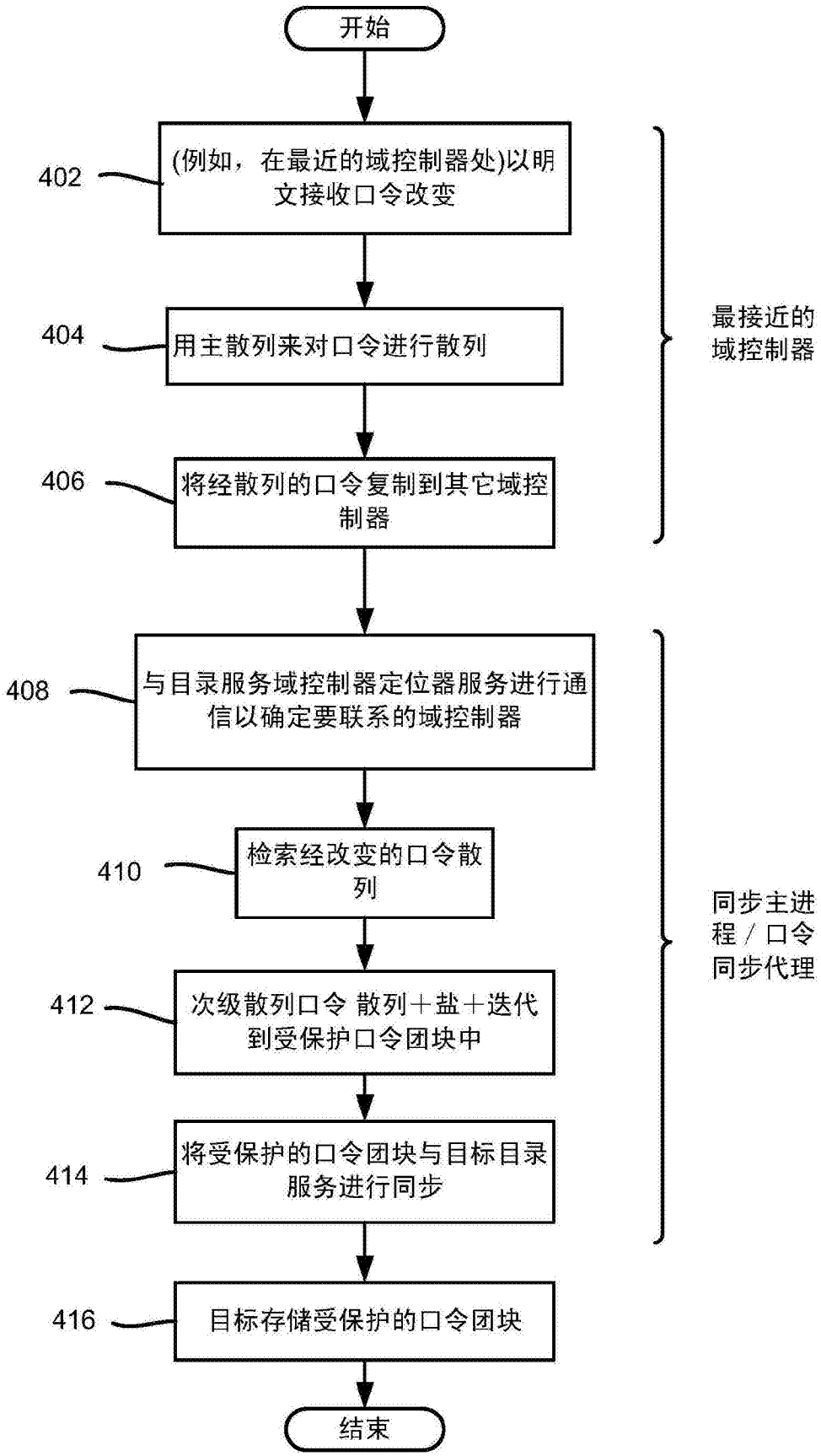

开始
402
(例如，在最近的域控制器处)以明文接收口令改变
404
用主散列来对口令进行散列
406
将经散列的口令复制到其它域控制器
最接近的域控制器
408
与目录服务域控制器定位器服务进行通信以确定要联系的域控制器
410
检索经改变的口令散列
412
次级散列口令 散列＋盐＋迭代到受保护口令团块中
414
将受保护的口令团块与目标目录服务进行同步
同步主进程 / 口令同步代理
416
目标存储受保护的口令团块
结束

图4

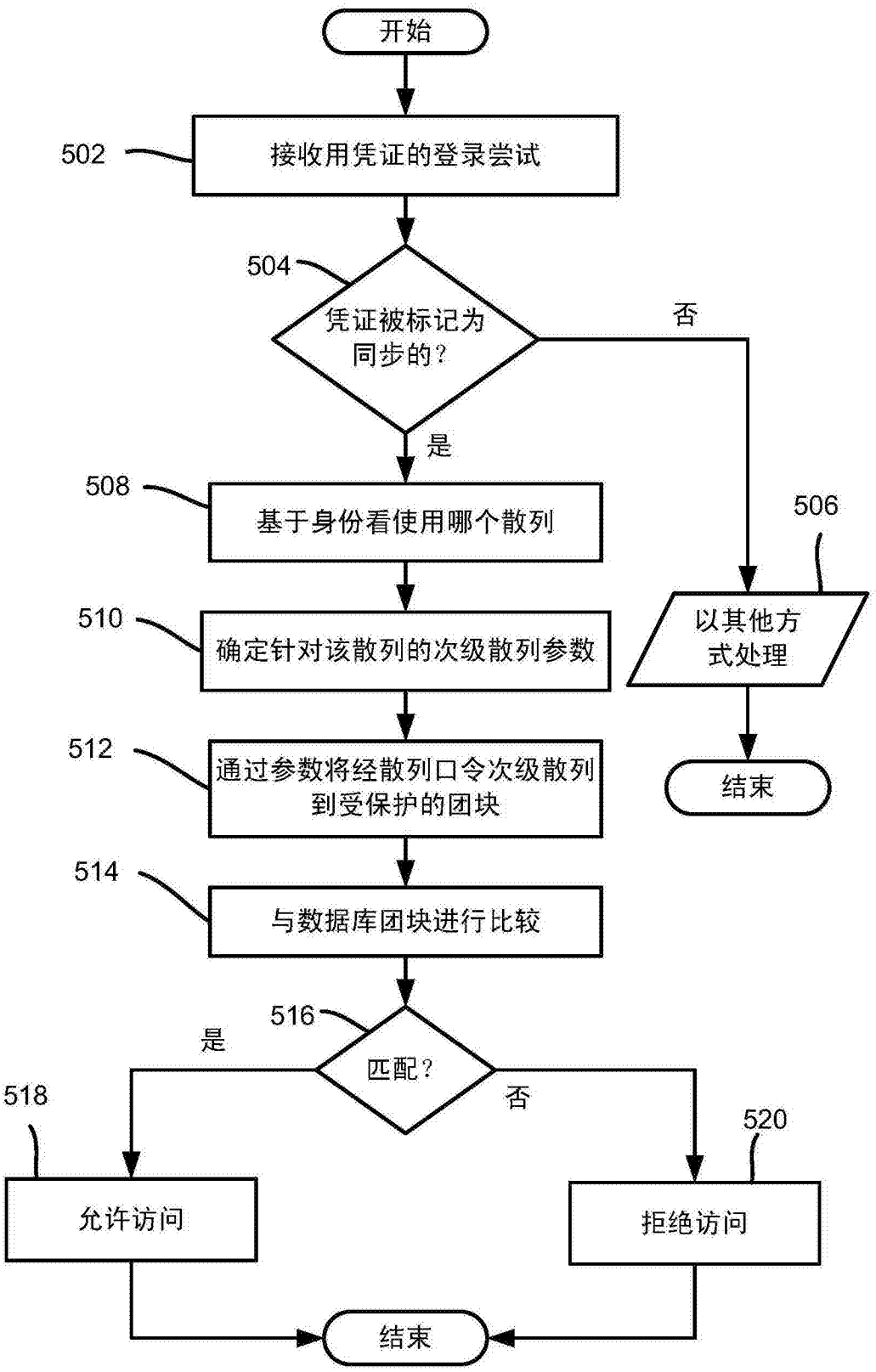

开始
502
接收用凭证的登录尝试
504
凭证被标记为同步的？
否
是
506
以其他方式处理
结束
508
基于身份看使用哪个散列
510
确定针对该散列的次级散列参数
512
通过参数将经散列口令次级散列到受保护的团块
514
与数据库团块进行比较
516
匹配？
是
否
518
允许访问
520
拒绝访问
结束

图5

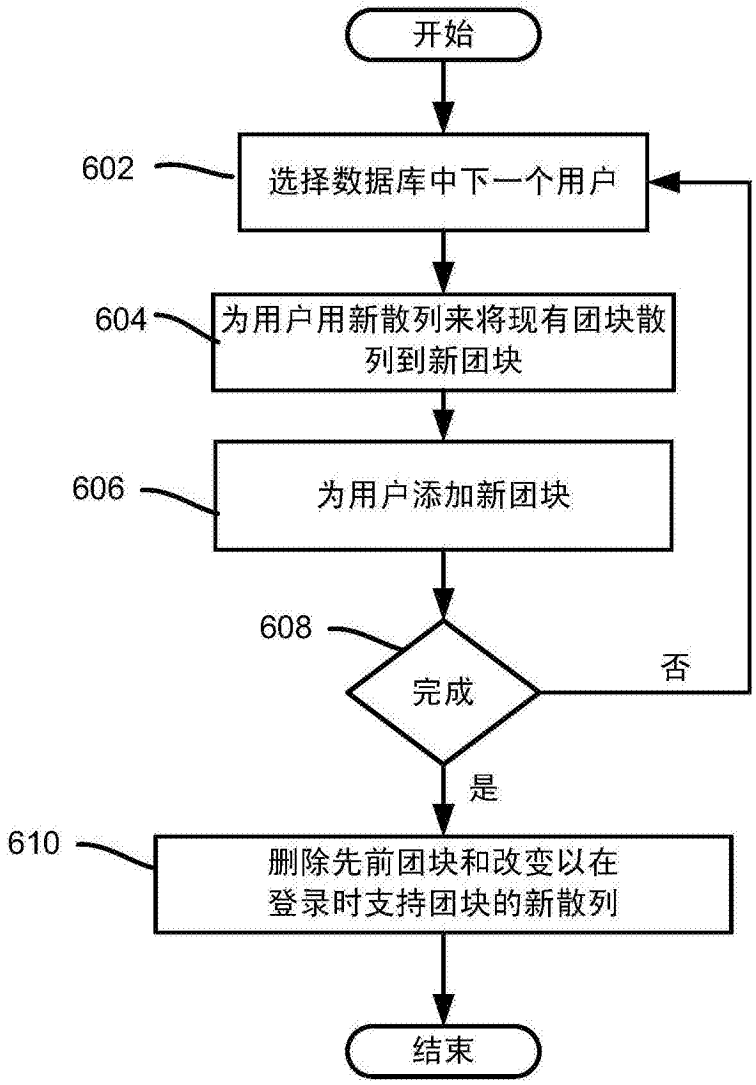

开始
602
选择数据库中下一个用户
604
为用户用新散列来将现有团块散列到新团块
606
为用户添加新团块
608
完成
否
是
610
删除先前团块和改变以在登录时支持团块的新散列
结束

图6

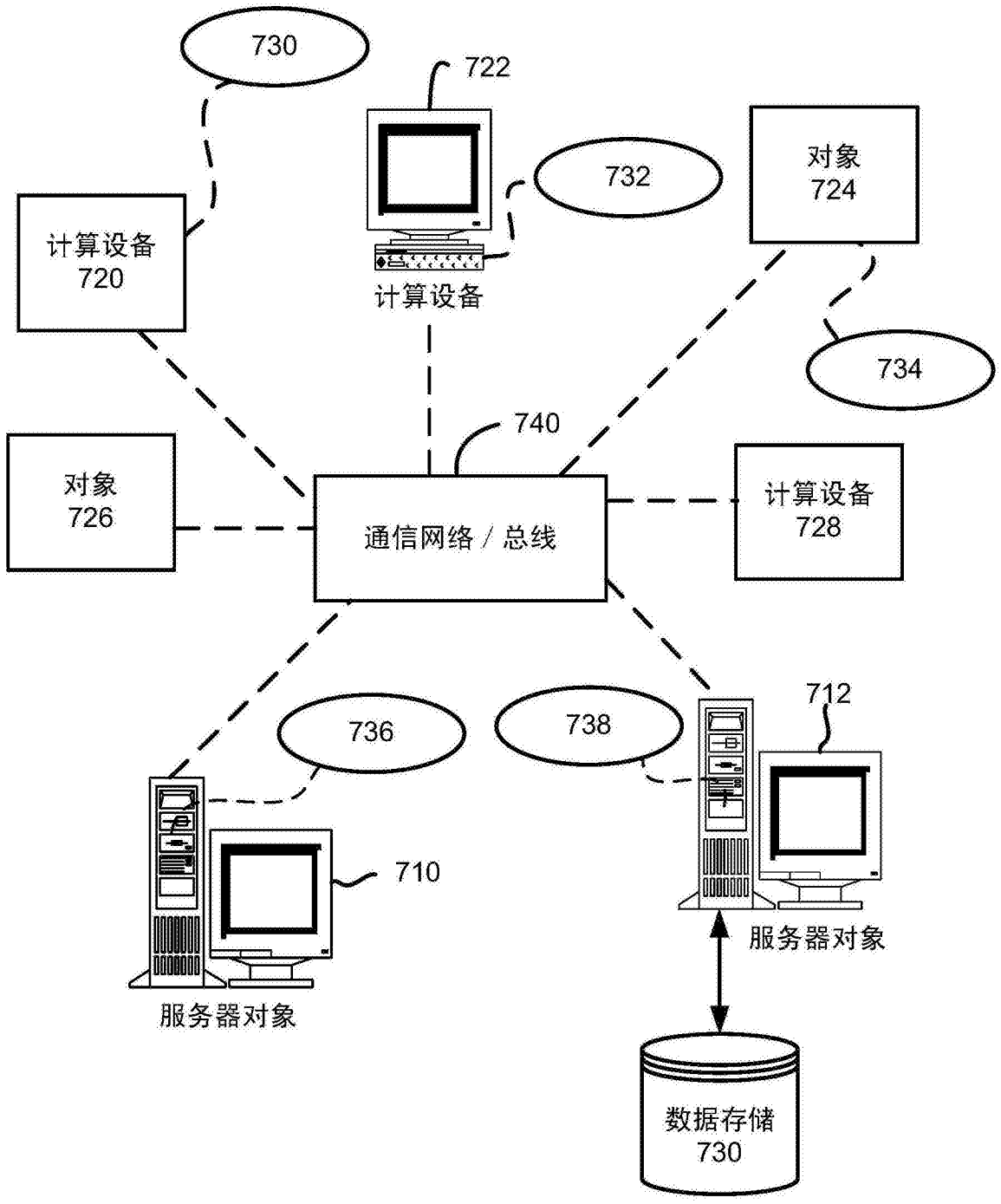

730
722
732
对象
724
计算设备
720
计算设备
734
740
对象
726
通信网络 / 总线
计算设备
728
712
736
738
710
服务器对象
服务器对象
数据存储
730

图7

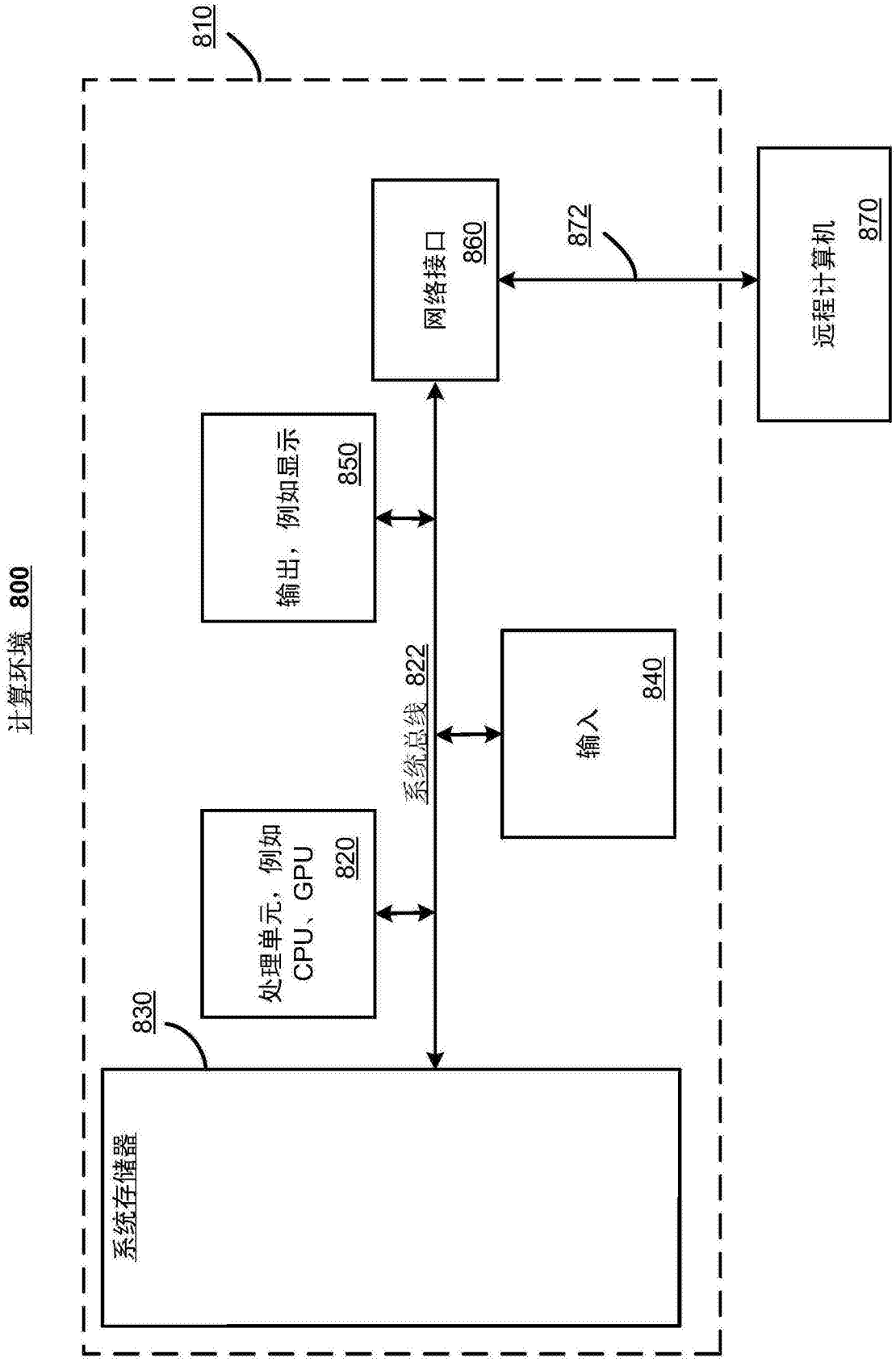

计算环境 800
810
网络接口 860
872
远程计算机 870
输出，例如显示 850
系统总线 822
输入 840
处理单元，例如 CPU、GPU 820
830
系统存储器

图8