(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 108173836 B
(45)授权公告日 2020.12.29

(21)申请号 201711423378.2

(22)申请日 2012.11.27

(65)同一申请的已公布的文献号
申请公布号 CN 108173836 A

(43)申请公布日 2018.06.15

(30)优先权数据
13/307,017 2011.11.30 US

(62)分案原申请数据
201280059144.3 2012.11.27

(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 B.达马拉简 A.钱 A.A.纳萨

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张立达 王英

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04L 29/08(2006.01)

(56)对比文件
US 2006168088 A1,2006.07.27
US 2009029692 A1,2009.01.29
WO 2006112845 A1,2006.10.26
JP 2002358229 A,2002.12.13
US 2011093790 A1,2011.04.21
US 2007055765 A1,2007.03.08
US 2009113532 A1,2009.04.30
CN 101005606 A,2007.07.25
CN 102130935 A,2011.07.20
CN 101471919 A,2009.07.01
US 7114008 B2,2006.09.26
黄涛."基于P2P的CDN流媒体流量本地化技术的研究与实现".《中国优秀硕士学位论文全文数据库-信息科技辑》.2011,

审查员 邓成

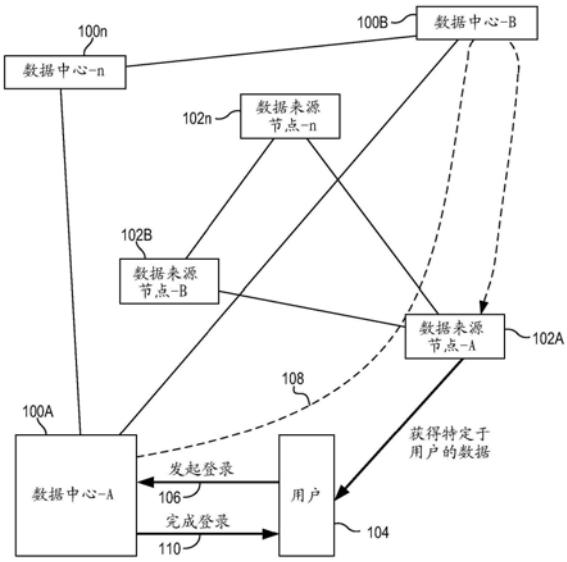
权利要求书2页 说明书13页 附图6页

(54)发明名称

朝向内容消费者迁移经过认证的内容

(57)摘要

技术涉及把网络上的经过认证的内容朝向内容消费者迁移。一种代表性技术包括网络节点接收至少具有存储用户数据的网络服务处的所述用户数据的位置以及用于访问用户数据的密码密钥的已加密种子。所述种子是响应于针对所述网络服务的用户登录尝试而接收到的。至少利用所接收到的密码密钥从所述位置请求用户数据。所述方法还包括在网络节点处接收和存储用户数据,其中与所述网络服务的位置相比,网络节点在物理上更靠近用户的位置。如果用户被成功认证,则向在网络节点处而不是来自网络服务的所存储的用户数据提供用户访问。



CN 108173836 B

1.一种在提供服务的硬件计算设备上执行的方法,其中,提供所述服务的所述硬件计算设备与包括一个或多个计算设备的边缘服务器相比在地理上更远离客户端设备,所述方法包括:

由所述服务从所述客户端设备接收第一信息,所述第一信息向所述服务唯一地标识用户以及指示在所述服务内的所述用户的数据;

由所述服务基于所接收的第一信息,生成第二信息;

由所述服务响应于所述接收,将所述客户端设备重定向到与所述服务相关联的认证模块,其中,所述定向包括向所述客户端设备提供所述第二信息;

由所述服务在所述定向之后从所述边缘服务器接收针对所述用户的所述数据的请求,其中,所述请求包括所提供的第二信息;以及

由所述服务响应于所接收的请求以及基于所接收的提供的第二信息,将所述用户的所述数据高速缓存在所述边缘服务器处,直到所述用户通过所述认证模块成功登录为止。

2.根据权利要求1所述的方法,其中,所生成的第二信息包括足以访问所述服务内的所述用户的所述数据的预授权束。

3.根据权利要求2所述的方法,其中,所述预授权束包括所述用户的唯一标识符。

4.根据权利要求2所述的方法,其中,所述预授权束是基于在所述服务与所述边缘服务器之间共享的密钥来加密的。

5.根据权利要求2所述的方法,其中,所述预授权束还包括:

在密码学上唯一的随机数,其被配置用作访问由所述预授权束包括的所述用户的所述唯一标识符所标识的所述用户的所述数据的密钥。

6.根据权利要求2所述的方法,其中,所述第一信息还包括所述用户的所述数据在所述服务内的位置。

7.根据权利要求6所述的方法,其中,所述预授权束还包括:由从所述客户端设备接收的所述第一信息所包括的所述位置。

8.一种包括硬件计算设备以及至少一个软件模块的系统,所述硬件计算设备以及所述至少一个软件模块一起被配置为执行包括提供服务的动作,其中,所述硬件计算设备与包括一个或多个计算设备的边缘服务器相比在地理上更远离客户端设备,所述动作包括:

由所述服务从所述客户端设备接收第一信息,所述第一信息向所述服务唯一标识用户以及指示在所述服务内的所述用户的数据;

由所述服务基于所接收的第一信息,生成第二信息;

由所述服务响应于所述接收,将所述客户端设备重定向到与所述服务相关联的认证模块,其中,所述定向包括向所述客户端设备提供所述第二信息;

由所述服务在所述定向之后从所述边缘服务器接收针对所述用户的所述数据的请求,其中,所述请求包括所提供的第二信息;以及

由所述服务响应于所接收的请求以及基于所接收的提供的第二信息,将所述用户的所述数据高速缓存在所述边缘服务器处,直到所述用户通过所述认证模块成功登录为止。

9.根据权利要求8所述的系统,其中,所生成的第二信息包括足以访问所述服务内的所述用户的所述数据的预授权束。

10.根据权利要求9所述的系统,其中,所述预授权束包括所述用户的唯一标识符。

11.根据权利要求9所述的系统，其中，所述预授权束是基于在所述服务与所述边缘服务器之间共享的密钥来加密的。

12.根据权利要求9所述的系统，其中，所述预授权束还包括：

在密码学上唯一的随机数，其被配置用作访问由所述预授权束包括的所述用户的所述唯一标识符所标识的所述用户的所述数据的密钥。

13.根据权利要求9所述的系统，其中，所述第一信息还包括所述用户的所述数据在所述服务内的位置。

14.根据权利要求13所述的系统，其中，所述预授权束还包括：由从所述客户端设备接收的所述第一信息所包括的所述位置。

15.至少一个硬件计算机可读介质，其包括基于由硬件计算设备的执行将所述硬件计算设备配置为执行包括提供服务的动作的指令，其中，所述硬件计算设备与包括一个或多个计算设备的边缘服务器相比在地理上更远离客户端设备，所述动作包括：

由所述服务从所述客户端设备接收第一信息，所述第一信息向所述服务唯一标识用户以及指示在所述服务内的所述用户的数据；

由所述服务基于所接收的第一信息，生成第二信息；

由所述服务响应于所述接收，将所述客户端设备重定向到与所述服务相关联的认证模块，其中，所述定向包括向所述客户端设备提供所述第二信息；

由所述服务在所述定向之后从所述边缘服务器接收针对所述用户的所述数据的请求，其中，所述请求包括所提供的第二信息；以及

由所述服务响应于所接收的请求以及基于所接收的提供的第二信息，将所述用户的所述数据高速缓存在所述边缘服务器处，直到所述用户通过所述认证模块成功登录为止。

16.根据权利要求15所述的至少一个硬件计算机可读介质，其中，所生成的第二信息包括足以访问所述服务内的所述用户的所述数据的预授权束。

17.根据权利要求16所述的至少一个硬件计算机可读介质，其中，所述预授权束包括所述用户的唯一标识符。

18.根据权利要求16所述的至少一个硬件计算机可读介质，其中，所述预授权束是基于在所述服务与所述边缘服务器之间共享的密钥来加密的。

19.根据权利要求16所述的至少一个硬件计算机可读介质，其中，所述预授权束还包括：

在密码学上唯一的随机数，其被配置用作访问由所述预授权束包括的所述用户的所述唯一标识符所标识的所述用户的所述数据的密钥。

20.根据权利要求16所述的至少一个硬件计算机可读介质，其中，所述第一信息还包括所述用户的所述数据在所述服务内的位置，并且其中，所述预授权束还包括由从所述客户端设备接收的所述第一信息所包括的所述位置。

朝向内容消费者迁移经过认证的内容

[0001] 本申请是申请日为2012/11/27、申请号为201280059144.3、发明名称为“朝向内容消费者迁移经过认证的内容”的中国专利申请的分案申请。

背景技术

[0002] 可以通过网络获得的数字数据的数量巨大。可以通过其范围从对等网络和局域网到例如因特网之类的全球网络的网络获得信息。可以获得各种类型的信息，其中包括意图可用于任何用户的数据以及例如电子邮件、备份数据等更加个人化的数据。在许多情况下，用户需要提交凭证以证明其被授权观看和/或访问特定内容。举例来说，用户可能被要求登录网站以便观看或下载信息，登录邮件服务器以便接收电子邮件等等。

[0003] 随着可访问数字信息的无所不在，人们已经开始预期无中断的服务以及近乎瞬时的访问速度。除了对于提高通信速度有贡献的技术进步之外，预见性技术在增进网络通信速度方面也可以起到重要作用。举例来说，预先获取和其他预见性技术可以就用户接下来可能请求的内容做出合理的假设。这样的判定可以根据各种因素做出，比如用户当前正在消费的内容、已知的用户优选项、过去的用户行为和/或任何数目的其他因素。

[0004] 这些和其他技术常常是可能的，因为在信息通信中所涉及的特定用户是已知的。举例来说，如果请求他/她的电子邮件的特定用户对于邮件服务器或其他邮件传送代理是已知的，则可以预先获取电子邮件消息和消息列表页面。特定用户的典型过去行为可以促使向保持存储装置发送特定信息以供快速用户访问，这是基于用户将确实很快请求该信息的概率而进行的。这样的技术可以使得数据和其他信息请求显得是接近瞬时的，尽管实际上发生了不为用户所知的后端和/或传输延迟。

[0005] 但是这些和其他技术可能是基于与用户相关联或者在某些情况下是用户所独有的信息。如果尚不知道用户的身份、尚未建立会话等等，则这样的技术可能不可用。举例来说，在用户登录到基于web的服务时，尚未建立会话，并且所述服务尚不知道与该用户相关联的身份和/或属性。在发生认证或其他初始活动时，用户只能忍受延迟并且等待直到所述过程完成为止。认证请求和其他初始通信可能涉及多次信息交换。对应于这样的交换的跳跃次数和往返时间可能对于用户导致不合期望的“反应时间(time to glass)”(TTG)体验。

发明内容

[0006] 技术涉及把网络上的经过认证的内容朝向内容消费者迁移。一种代表性技术包括网络节点接收至少具有存储用户数据的网络服务处的所述用户数据的位置以及用于访问用户数据的密码密钥的已加密种子。所述种子是响应于针对所述网络服务的用户登录尝试而接收到的。至少利用所接收到的密码密钥从所述位置请求用户数据。所述方法还包括在网络节点处接收和存储用户数据，其中与所述网络服务的位置相比，网络节点在物理上更靠近用户的位置。如果用户被成功认证，则向在网络节点处而不是来自网络服务的所存储的用户数据提供用户访问。

[0007] 在这种技术的另一种具体实现方式中，提供一种系统，其包括被配置成存储基于

认证的内容的第一位置处的第一存储装置。提供第二位置处的第二存储装置，其中第二位置与第一位置相比在物理上更加紧密邻近所述基于认证的内容的请求者。第二位置处的处理器被配置成在请求者尝试登录到被接纳于第一位置处的服务时从第一存储装置安全地请求所述基于认证的内容的至少一部分以便存储在第二存储装置中。所述处理器还被配置成促进例如由所述请求者从第二存储装置安全地访问所述基于认证的内容。

[0008] 另一种代表性实现方式涉及一种方法或者存储了可由处理器执行以施行各项功能的指令的计算机可读介质。所述方法涉及在基于web的电子邮件服务处接收用户访问请求，并且作为响应生成包括用户标识符、在所述电子邮件服务处的该用户的电子邮件数据的存储位置以及用于访问该用户的电子邮件数据的密码密钥的已加密种子。用户被重定向到认证模块，所述认证模块呈现登录页面以及所述登录页面内的图像标签，其中所述图像标签包括所述已加密种子以及内容分发网络的边缘服务器的地址。从边缘服务器接收针对至少通过所述加密密钥标识的用户电子邮件数据的第一部分的请求。所请求的用户电子邮件数据的第一部分被导向边缘服务器，并且允许从边缘服务器而不是从电子邮件服务向用户提供所述用户电子邮件数据的第一部分。

[0009] 提供本发明内容是为了以简化形式介绍以下将在具体实施方式中进一步描述的概念的选择。本发明内容不意图标识出所要求保护的主题的关键特征或必要特征，也不意图被用来限制所要求保护的主题的范围。

附图说明

[0010] 图1A是示出了可以据以实施这里所描述的技术的一种代表性方式的代表性联网环境；

[0011] 图1B描绘出可以被用来使得特定于用户的信息在更靠近用户的地方可用以便减少延迟并且改进反应时间的更加具体的交互实例；

[0012] 图2示出了用于减少与获得特定于用户的信息相关联的延迟的代表性系统层级实例；图3示出了用于减少与基于web的电子邮件程序的登录处理相关联的延迟的代表性实例；

[0013] 图4是示出了其中网络节点可以充当高速缓存元件以便减少用户在对于网络服务的初始访问期间所经历的等待时间的一种代表性方法的流程图；

[0014] 图5是用于在用户登录到提供用户数据的服务时取回用户数据并且用于把用户数据高速缓存在用户可以从该处更加快速地获得所述用户数据的位置处的系统的方块图；

[0015] 图6是把用户的电子邮件数据的至少一部分移动到与电子邮件系统相比在地理上更靠近用户的CDN的边缘服务器的方式的一个代表性实例的流程图；以及

[0016] 图7描绘出可以在其中实施这里所描述的原理的代表性计算系统。

具体实施方式

[0017] 在后面的描述中将参照描绘出代表性实现方式实例的附图。应当理解的是，可以利用其他实施例和实现方式，这是因为在不背离本公开内容的范围的情况下可以做出结构和/或操作方面的改变。

[0018] 如前所述，通过使用预先获取或其他预见性技术常常可以减少网络访问延迟。这

样的技术涉及到关于用户可能请求的内容的合理假设，并且可以发起动作以获得很可能将由用户请求的信息。但是如果尚不知道用户的身份、会话尚未建立或者结合某种其他初始活动，则这样的技术是无效的。举例来说，在用户已“登录”或者结合应用或服务以其他方式得到认证之前，不能向用户呈现经过认证的内容，这是因为用户尚未被授权观看所述内容。因此，在这样的认证或其他初始处理发生时，在相关内容被呈现之前，用户可能会经历不合期望的延迟。

[0019] 本公开内容总体上涉及使得基于认证的内容至少暂时地在与所述内容通常被存储的位置相比在物理上更加靠近用户的位置处可用于内容消费者或“用户”。网络应用/服务可以响应于针对访问所述服务的用户请求生成已加密令牌。可以直接地，经由重定向的认证模块等等向用户提供所述令牌。利用所述令牌，用户可以向与网络服务相比更加邻近的网络节点发出请求，其中所述请求使得更加邻近的网络节点从更远距离的网络服务获得所述基于认证的内容的至少第一可呈现部分。请求并且向更近的网络节点提供基于认证的内容的这一事务可以在用户正登录到网络服务的同时进行，从而允许传输延迟在用户原本将不会预期为其呈现内容的时间发生。当用户最终被认证时，可以向用户快速提供已被高速缓存在更近的网络节点处的所述基于认证的内容的第一可呈现部分。至少由于用户数据的并行获取以及当用户最终被认证时数据更加邻近，TTG得以改进。

[0020] 现在参照图1A，所描述的代表性联网环境示出了可以据以实施这里所描述的技术的一种代表性方式。在所示出的实例中，基于网络的应用、服务或其他网络实体可以具有分布在网络上的各点处的数据，正如数据中心100A、100B、100n等所描绘的那样。作为举例的目的，这些数据中心100A、100B、100n可以包括与基于网络的服务相关联的数据存储实体。例如数据来源节点-A 102A、数据来源节点-B 102B、数据来源节点-n102n之类的其他网络实体可以和与数据中心100A、100B、100n相同或不同的网络相关联。在一个实例中，数据来源节点102A、102B、102n代表例如通过内容分发网络(CDN)提供数字内容的内容存储实体。在另一个实例中，至少数据来源节点-A 102A是相对于数据中心100A、100B、100n的第三方网络节点，其中在数据中心100A-100n处采取的数据安全性措施通常不会被延续到数据来源节点102A-102n。

[0021] 用户104可以与所示出的网络实体中的任何一个或更多进行交互。这里所描述的一种代表性技术减少了用户104在与一个或更多网络实体进行初始交互时所遇到的延迟。举例来说，所述初始交互可以是登录处理，其中用户输入特定于用户的凭证以便获得对于网络服务、数据等等的访问。

[0022] 在一个更加具体的实例中，假设用户104发起了登录处理，正如交互线106所描绘的那样。这里所描述的实施例阐述了这样的方式，其中通过把与用户有关的信息高速缓存或者以其他方式存储在与其原始存储位置相比更靠近用户的网络实体处来减少从用户的登录发起开始算起的反应时间(TTG)。举例来说，当用户104如线106上所描绘的那样发起登录时，用户104可能会输入电子邮件地址和/或用户标识符(用户ID)、口令等等。一旦由用户104提交，用户通常等待直到所述凭证已被认证为止，并且最终向用户104呈现应用/服务。根据这里所描述技术，通过把正被访问的应用/服务的第一页面存储在物理上更靠近用户104的节点中来减少用户的等待时间，从而在登录处理完成时更快地向用户104呈现。

[0023] 因此，可以在用户登录时或者以其他方式忙于初始交互时从存储区域取回通常对

于用户来说是私有的内容或数据。在这些并行动作期间，通过预见到登录处理最终导致用户的成功认证，可以将所述内容移动到在地理上更靠近用户的位置。应当提到的是，除非另行表明，否则提到事件是“并行”、“同时”发生等等并不意味着这样的事件在时间上精确地重叠，而是意味着它们至少在某种程度上重叠。

[0024] 在图1A的实例中，当用户104如交互线106所描绘的那样发起了登录处理时，发起用户数据高速缓存操作。用户数据高速缓存操作由虚线108描绘，其中在该例中将用户标识信息安全地提供到数据中心-B 100B。用户标识信息被用来标识存储在数据中心-B 100B处的特定于用户的信息，比如可以在登录过程完成时向用户104呈现的初始web内容。这样的特定于用户的信息可以被从距离更远的数据中心-B 100B提供到数据来源节点-A 102A或者数据中心-B 100B可访问的其他节点。当用户104如交互线110所描绘的那样完成了登录时，特定于用户的信息可以被更加快速地提供到用户104，至少部分地被提供到与其更加邻近的数据来源节点-A 102A处。

[0025] 图1B描绘出可能被用来使得特定于用户的信息在更接近用户的地方可用以便减少延迟并且改进TTG的交互的一个更加具体的实例。该实例涉及在图1A中所提到的项目，因此在适当情况下使用相同的附图标记。在该例中假设用户104访问网站或其他网络节点以便与数据中心-A 100A进行交互，正如线A所示出的那样。通过在下面的更加具体的实施例中所描述的方式，与特定于用户的信息被存储在其中的数据中心-B 100B相比，与用户104相关联的浏览器(未示出)最终向更靠近用户104的节点提供安全的信息。数据来源节点-A 102A代表相对于用户104的这样的“更近的节点”，并且虚线B代表安全信息的传送。

[0026] 利用通过虚线B描绘的该安全信息，节点-A 102A向存储在数据中心-B 100B处的特定于用户的信息发出请求，正如虚线C所描绘的那样。从数据中心-B 100B向数据来源节点-A 102A提供特定于用户的信息以供至少暂时存储。如果用户的登录最终成功，数据中心-A 100A(其可以包括认证节点或者与之相关联)可以如线E所描绘的那样生成用于用户104的页面，从而使得用户104的浏览器访问暂时存储在数据来源节点-A102A处的信息，正如线F和G所描绘的那样。

[0027] 因此，除了别的之外，这里所描述的技术允许从距离更远的数据中心向网络的边缘推送特定于至少一个用户的经过认证的内容。举例来说，可以通过把经过认证的数据推送来更靠近用户以加速认证或“登录”过程。在一个实施例中，将数据推送到通常不存储涉及认证来获得的数据的服务器。举例来说，所述经过认证的内容可以代表原本将不会被分发到任何一般的请求者的内容，比如将在用户的凭证已被认证时呈现给用户的web内容的第一页面。在一个更加具体的实例中，所述经过认证的内容可以是用户的主页的第一页面、基于web的电子邮件收件箱等等。在一个实施例中，获取经过认证的内容并且至少暂时存储在与其原本将被存储的位置相比更靠近客户端设备的次级服务器处，比如边缘服务器或其他中间服务器。可以在为用户给出输入认证凭证的方式的同时获得经过认证的内容以便高速缓存/存储在更近的服务器处。按照这种方式，高速缓存经过认证的内容与输入用户凭证之间的时间重叠就是在总体登录处理中所节省的时间。更具体来说，当用户完成输入他/她的凭证时，不需要从远距离节点获得经过认证的内容，而是经过认证的内容将在更靠近用户的节点处轻松获得，比如在CDN边缘服务器处。

[0028] 图2示出了用于减少与获得特定于用户的信息相关联的延迟的另一个代表性实

例。在图2的实例中，假设经由网络提供的服务是基于因特网的电子邮件(email)服务，其中当用户登录以访问他/她的电子邮件时，TTG得以减少。

[0029] 在图2的实例中描绘出可能由用户使用来访问电子邮件和/或其他网络服务的若干代表性装置或设备202。设备202是出于示例性目的而示出的，而不代表穷举列表。这里所描述的技术适用于可以经由一个或更多网络与服务和/或数据通信或者以其他方式访问服务和/或数据的任何设备。设备202可以是独立的计算设备、便携式计算和/或通信设备、嵌入到例如电器或汽车之类的其他产品中的设备等等。代表性设备202包括台式计算机202-1、便携式计算机(例如膝上型计算机)202-2、移动电话202-3、个人数字助理202-4或者能够经由网络进行通信的其他202-5设备。如果由设备202所利用的至少一项网络服务是电子邮件，则设备202可以包括例如用以访问基于web的邮件的浏览器204、本地电子邮件客户端206等软件。

[0030] 图2的代表性实施例包括通过网络214可用的一个或更多数据中心208、210、212。数据中心208、210、212可以在地理上分布于全球的受到服务的部分的周围。在一个实施例中，数据中心包括集群，比如在数据中心208处示出的集群216。用于设备202的用户的电子邮件和/或其他数据可以被存储在特定的集群216和数据中心208处。因此，当用户访问统一资源定位符(URL)或其他地址以到达基于web的电子邮件应用215时，该用户可以与该特定数据中心208进行交互。

[0031] 当用户被导向电子邮件应用215时，用户的浏览器204在一个实施例中被重定向到认证模块217，认证模块217可以与数据中心208相关联或者与之分开。认证模块217便于用户输入例如电子邮件地址和/或用户名、口令等用户凭证。当该信息由认证模块217验证时，可以把浏览器204重定向回到电子邮件应用215。根据这里所描述技术，与从其服务web内容/数据的数据中心208相比，所述web内容(比如将被呈现给设备202的示出用户的电子邮件收件箱的屏幕)被高速缓存在地理上更靠近设备202的网络实体处。当正在输入和/或验证用户的凭证时，可以获得所述内容并且将其移动到更近的网络实体，比如边缘服务器218。

[0032] 举例来说，网络214可以包括内容分发网络(CDN)，内容分发网络包括一个或更多边缘服务器218、220，并且在某些情况下包括可以与所述电子邮件系统、CDN和/或其他系统的任何部分相关联的一个或更多附加的中间服务器222、224、226。设备202的用户可以把浏览器204指向由电子邮件应用215提供的服务，并且开始登录处理。在这一时间期间，可以把特定于用户的数据从数据中心208处的适当集群216移动到更靠近设备202的网络节点，比如CDN边缘服务器218。虽然CDN边缘服务器218通常可以被用来存储不需要认证的内容，比如一般的图像、javascript代码、级联样式表(CSS)等等，这里所描述的技术利用边缘服务器218的邻近性来安全地高速缓存基于认证的特定于用户的数据。通过利用适当的安全性措施，可以利用针对未经授权的访问的保护将特定于用户的数据高速缓存在边缘服务器218处。

[0033] 在一个实施例中，特定于用户的数据包括将被呈现给用户的电子邮件服务的第一页面，比如用户的个人电子邮件收件箱。将被呈现在用户的设备202上的第一页面对于各个用户将是不同的，这是因为电子邮件收件箱或其他内容通常将是每一个用户所独有的。当用户的凭证已被验证时，浏览器204可以获得或者被指示来获得来自物理上邻近的边缘服

务器218的所高速缓存的特定于用户的内容。电子邮件内容可以通过浏览器204来呈现、由邮件服务器230管理以及通过本地电子邮件客户端206来呈现等等。通过在物理上更靠近设备202地高速缓存特定于用户的内容，可以减少花费在呈现所请求的内容的第一页面上的时间。下面将描述在保持用户隐私的同时得到特定于用户的数据以允许更快的TTG的方式。

[0034] 图3示出了用于减少与基于web的电子邮件程序的登录处理相关联的延迟的一个代表性实例。在所示出的实施例中，假设电子邮件系统300分布在一个或更多数据中心302当中。虽然结合这里所描述的技术可能有多种实现方式，但是所示出的实施例涉及多个集群304、306到308，其中每一个接纳多个用户，并且在许多情况下是接纳大量用户。每一个集群(比如集群308)可以代表一个自含式服务器集合，其包括一个或更多后端服务器310、312以及一个或更多前端服务器314、316。前端服务器314、316接口到例如客户端设备350之类的外部设备，并且可以施行例如格式化页面、检查病毒等功能。前端服务器314、316可以包括前门(FD)服务器318、320，前门服务器可以从事与利用电子邮件系统300的客户端设备350的第一次接触。FD服务器318、320可以代表客户端设备350向后端服务器310、312发出请求。

[0035] 除别的之外，后端服务器310、312可以提供用于存储用户数据的数据库和/或其他存储装置322，所述用户数据包括用户的电子邮件324以及其他特定于用户的内容。在一个实施例中，存储在所述一个或更多数据中心302中的任何一个处的存储装置322中的特定于用户的内容包括将在成功登录时呈现给用户的一个或更多web页面，比如电子邮件服务的主页、电子邮件服务的收件箱等等。应当提到的是，代表性前端服务器318、320与后端服务器310、312之间的具体职责分配仅仅是出于说明的目的来描述的，这是因为不管多台服务器之间的职责分配如何或者到底是否有多台服务器，这里所描述的技术都适用。

[0036] 如前所述，图3的实例是在电子邮件系统300的情境中来描述的。在该实施例中，假设客户端设备350先前与电子邮件系统300进行了通信，并且至少一个小型文件(cookie)352被存储在客户端设备350处。小型文件352例如可以是标识出用户并且指出用户数据驻留在何处的数据。举例来说，位置小型文件352可以被存储在客户端设备350处，其包括标识出用户的电子邮件数据驻留在哪一个集群304、306、308等等之中并且可能还标识出驻留在哪一个数据中心302中的数据。

[0037] 正如后面更加详细地描述的那样，这样的位置小型文件352可以提供充分地标识出用户的信息，从而可以为该用户生成已加密令牌或“种子”。结合这里所描述的技术并不要求位置小型文件352，这是因为可以使用其他标识信息。举例来说，电子邮件地址可以充分地标识出用户以便发起对于特定于用户的内容的取回和更近的高速缓存。但是与用户第一次提交电子邮件地址或其他标识信息的情况相比，使用小型文件352或其他所存储的信息可以允许更快地创建种子并且最终高速缓存特定于用户的内容。还应当提到的是，在一个实施例中，对于至少存储用户的电子邮件数据的位置(例如集群304、306、308等等)的位置小型文件352的使用假设用户的数据保持在相同的集群中，或者至少自从上一次电子邮件访问之后尚未改变。按照这种方式，位置小型文件352可以快速提供已知存储了用户的电子邮件数据的位置。

[0038] 在其他实施例中，于是可以使用标识出用户的其他信息来标识用户的数据的位置，这在某些情况下可能涉及找到用户的个人电子邮件数据的额外步骤。各个实施例涉及

用户标识信息和/或用户数据位置信息的不同层级的细节，其中任一项结合这里的描述都是可行的，但是在某些情况下，可以借助于其他标识信息而不是通过直接位置信息(例如集群地址)来找到用户数据的确切位置。因此，虽然图3的实施例是结合标识出用户以及用户的所存储的电子邮件数据的位置和其他特定于用户的内容的位置小型文件352来描述的，但是在不背离这里所描述的技术的情况下可以替换地使用其他标识信息。

[0039] 在一个实施例中，响应于位置小型文件352或者其他用户标识信息在数据中心302处生成的种子358A代表按照已加密令牌的形式的预授权束(preauthorization bundle)。该已加密令牌或“种子”可以包括例如向电子邮件系统300和认证模块356唯一地标识对应的用户的数值(其在这里可以被称作客户端标识符(CID))之类的信息。正如前面所提到的那样，所述种子还可以包括用户的电子邮件的位置和有关的数据，比如用户的电子邮件集群名称、地址或者其他集群标识符。在一个实施例中，还提供作为所述种子的一部分的密码安全的随机数，其在这里可以被称作预授权密钥或者种子-GUID(全球唯一的标识符)。所述种子-GUID可以被用作访问由CID在所标识出的集群处标识出的用户的适当数据的密钥，所述适当数据比如是用户的电子邮件收件箱。

[0040] 更具体来说，客户端设备350可以向电子邮件系统300提供位置小型文件352或其他用户标识信息。在一个实施例中，位置小型文件352按照用户标识小型文件(UIC)的形式，其至少包括用户的标识和用户的数据集群的位置。可以对位置小型文件352进行加密。前门服务器320接收位置小型文件352，并且在一个实施例中利用针对认证模块356的重定向消息354以及从位置小型文件352中的用户信息生成的种子358A作出响应。在该例中，种子358A代表至少包括所述集群、种子-GUID和CID的已加密结构，该结构在这里被称作三元组。

[0041] 客户端设备350的浏览器遵循重定向消息354链接去到认证模块356，所述认证模块356作为响应提供登录页面360。可以将种子358B提供给认证模块356以供后续使用。根据一个实施例，除别的之外，登录页面360包括例如图像标签之类的内容标签。所述内容标签作为由认证模块356在登录页面360上为电子邮件系统300再现的定制内容的一部分。下面示出这样的图像标签的一个实例:<img src＝https://CDN.emailname.com/clear.gif?s＝<encrypted>”/>

[0042] 实例1。

[0043] 其中，“CDN”在该例中代表内容分发网络边缘服务器390，因此CDN.emailname.com代表与邮件系统(emailname.com)300协作的CDN边缘服务器390。

[0044] 结果是，在客户端设备350的用户可能正在输入他/她的凭证的时间期间，客户端设备350的浏览器可以并行地向边缘服务器390的该URL发出内容请求362。内容请求362指向边缘服务器390，该边缘服务器390触发该调用以开始高速缓存特定于用户的数据。应当提到的是，边缘服务器390可以是能够与电子邮件系统300协作的在物理上更靠近客户端设备350的任何网络节点。在所示出的实施例中，该网络节点由CDN边缘服务器390表示，但是它不需要是。但是在一个实施例中，特定于用户的内容被高速缓存到的网络节点是原本可能不会涉及认证要求以便接收内容的网络节点。

[0045] 利用前面的实例1的URL，客户端设备350的浏览器将利用已加密种子发出针对CDN.emailname.com处的图像标签的内容请求362。正如后面更加详细地描述的那样，内容请求362充当向边缘服务器390提供已加密种子使得该边缘服务器390可以进而获得并且高

速缓存特定于用户的内容(即电子邮件服务的第一web页面)的一种方式。

[0046] 应当提到的是,登录页面360可以包括脚本化语言或其他编程(而不是图像或其他内容标签)以便触发针对边缘服务器390的请求。对于图像标签和其他内容标签的使用代表帮助在边缘服务器390或其他中间节点上存储内容的一种方式。但是利用其他标签或脚本等等可以获得类似的结果。举例来说,可以利用AJAX调用(异步JAVASCRIPT™和XML)来替代内容标签的使用。在一个实施例中,这样的调用还可以允许在期望的情况下发布更大数量的认证信息,这是因为一些图像URL可能是利用受到字符限制的请求方法来实施的。因此可以把用户内容368B预先高速缓存或者以其他方式存储在边缘服务器390上,这是通过例如使用IMG、IFRAME、SCRIPT或者其他类似的HTML标签或其他编程标签传递已加密种子和其他有关的信息而实现的,或者是通过利用设备使用例如XML HTTP请求等脚本而实现的。可以使用这些以及其他类似的传递信息的方式,并且这里所描述的那些方式是出于说明的目的而提供的。

[0047] 应当提到的是,由内容请求所宣称请求的实际的图像、内容或其他数据是无关的。在一个实施例中,针对内容的请求是促进由边缘服务器390向适当的集群308发起的用以获得特定于用户的信息的客户端发起的请求的伪装,所述特定于用户的信息比如是由电子邮件系统300给出的该用户的第一web页面。在采用图像请求的一个更加具体的实例中,可以响应于所述请求获得察觉不到的图像,比如透明的和/或太小从而无法看到的一像素接着一像素的图像。可替换地,所述图像或其他内容请求可以返回可察觉的图像、声音等等。但是在一个实施例中,所述图像请求并不实际寻求结果图像,而是利用图像标签作为向边缘服务器390提供已加密种子的载体,所述边缘服务器390将与电子邮件系统300协作以便高速缓存用户的经过认证的信息的至少一部分。该信息高速缓存在用户输入登录凭证的同时发生,从而允许更快地呈现电子邮件服务的第一页面,这是因为该第一页面被高速缓存在物理上更靠近客户端设备350的地方。

[0048] 为了促进对于所述种子和/或涉及已加密信息的其他信息的解密,与边缘服务器390和/或关联于该边缘服务器390的CDN共享为边缘服务器390创建的域(比如CDN.emailname.com)的数字证书。此外,电子邮件系统300、认证模块356和CDN边缘服务器390共享在这里被称作种子密钥的密钥,该密钥被用来至少对所述种子进行加密。所述种子密钥例如可以是对称密钥。可替换地,所述种子密钥可以是对应于数字证书的私有密钥。可以利用对种子进行加密的其他方式。

[0049] 当边缘服务器390接收到内容请求362时,边缘服务器390可以在解密模块392处利用先前与之共享的种子密钥对已加密种子进行解密。因此边缘服务器390将可以访问所述集群、种子-GUID和CID,并且可以向在已解密种子中提供的集群(例如https://clustername.emailname.com/)发布种子-GUID 366。电子邮件系统300的前端服务器316向后端服务器312提供该种子-GUID 366,以便从存储装置322获得特定于用户的内容。举例来说,所存储的信息可以是用户的电子邮件的收件箱页面或者根据用户优选项的其他“主页”内容。电子邮件系统300将该特定于用户的内容368A发放或者以其他方式提供给边缘服务器390,在该边缘服务器390处,该特定于用户的内容368A被至少暂时地存储,直到用户通过认证模块356成功登录到电子邮件系统300上为止。

[0050] 在一个实施例中,存储在边缘服务器390处的用户内容368B具有期满时间。响应于

接收到内容请求362或者响应于接收到用户内容368B，或者其间的任何时间，边缘服务器390可以提供针对原始内容请求362的响应370。正如前面所提到的那样，所述响应可以是小的、基本上察觉不到的图像，或者是其本身在客户端设备350处不被使用的其他内容。在一个实施例中，响应370可以是在解密模块392处对种子进行解密的时间期间以及在用户内容368B的接收期间并行地异步发送的小图像。此时，用户内容368B被高速缓存在边缘服务器390处，等待用户的成功登录，在用户成功登录时，可以将用户内容368B提供给客户端设备350。

[0051] 在某一时间，用户完成经由呈现在客户端设备350上的登录页面360输入他/她的凭证。认证模块356提供认证比较模块372以便把用户的登录凭证与所存储的登录信息进行比较。在成功认证后，解密模块374对所述种子进行解密以便得到用户的集群、种子-GUID和CID。用户比较模块376把已解密CID与被授予凭证的用户进行比较。如果存在匹配，则认证模块356生成页面378。页面378可以包括脚本化语言(例如JAVASCRIPT™)或使得客户端设备350处的浏览器将种子-GUID 372发布到高速缓存在更近的边缘服务器390处的用户内容368B的位置的其他代码。

[0052] 响应于来自与提供种子-GUID 372相关联的用户设备350的请求，边缘服务器390提供其早前高速缓存的用户内容368B，正如通过用户内容368C被提供到客户端设备350所描绘的那样。如果所述内容没有被找到或者已期满，则边缘服务器390可以简单地将所述发布传递到电子邮件系统300以进行默认处理。

[0053] 按照这种方式，用户可以在成功登录到电子邮件系统300(或者其他基于网络的服务)时更加快速地接收到用户内容368C。在一个实施例中，所述用户内容代表仅仅响应于所述预授权束或“种子”的传送而使得各个实体能够管理用户内容的高速缓存才被分发的特定于用户的内容。

[0054] 通过使得所述种子成为三元组列表而不是单一项目，可以将这里所描述的技术扩展到客户端设备350的多个用户。举例来说，对于两个用户，所述种子可以是包括两个三元组的一个列表，每一个三元组包括客户端设备350的对应用户的集群、种子-GUID和CID。在这种情况下，特定于用户的信息被高速缓存在其中的逻辑(例如边缘服务器390)可以对于种子内的每一个三元组施行内容请求362的解密和用户内容368B的高速缓存。此外，认证模块356可以从已解密种子当中选择与当前正在认证的用户的CID数值相匹配的三元组。

[0055] 图3的具体实施例是出于说明的目的给出的，这是因为可以在多种其他情境中利用这里所描述的技术。举例来说，可以结合任何网络应用/服务以及可以充当用户设备与网络服务之间的中间节点的任何协作性网络节点提供所述技术。图4是示出了一种代表性方法的流程图，其中网络节点可以充当高速缓存元件以便减少用户在对于网络服务的初始访问期间所经历的等待时间。在方块400处，网络节点接收包括在存储用户数据的网络服务处的用户数据的位置以及用于允许访问用户数据的密码密钥的已加密种子。在一个实施例中，网络节点响应于用户针对网络服务的登录尝试而至少接收所述已加密种子。

[0056] 如方块402处所示，网络节点可以至少利用所接收到的密码密钥来请求提供在已加密种子中的用户数据位置。作为响应，方块404示出了网络节点可以接收并存储通常被存储在网络服务处的用户数据，其中与网络服务的位置相比，该网络节点在物理上的位置更靠近用户。在方块406处，响应于从用户登录尝试所导致的成功的用户认证，允许针对在网

络节点处而不是来自网络服务的所存储的用户数据的用户访问。

[0057] 类似地，图5是用于在用户正登录提供用户数据的服务时取回用户数据以及用于把用户数据高速缓存在用户可以从其中更加快速地获得该用户数据的位置处的系统的方块图。该实施例示出了第一位置500处的第一存储装置502。第一位置500例如可以接纳电子邮件服务或者其他基于web的服务504。第一存储装置502被配置成存储基于认证的内容510A，比如用户电子邮件收件箱或其他用户敏感数据。第一位置500可以包括用来施行对于服务504的处理、认证508和/或从第一位置500实施的其他处理的处理器和/或其他电路。

[0058] 提供第二位置520处的第二存储装置522，与第一位置500相比，第二位置520在物理上更加邻近基于认证的内容510A的请求者530。第二位置520可以代表能够与第一位置500和请求者530二者通信的网络540上的可访问的节点。在一个实施例中，第二位置520处的处理器524被配置成在请求者530尝试登录在第一位置500处被接纳的服务504的同时，从第一存储装置502安全地请求基于认证的内容510A的至少一部分以便存储在第二存储装置522中。所述登录处理可以由可能或者可能不位于第一位置500处的处理器506和/或认证模块508施行。处理器524还被配置成促进对于来自第二存储装置522的基于认证的内容510B的安全访问。

[0059] 图6是把用户电子邮件数据的至少一部分移动到与电子邮件系统相比在地理上更加靠近用户的CDN的边缘服务器的方式的一个代表性实例的流程图。在所示出的实例中，用户输入电子邮件系统600的URL或其他地址。举例来说，用户可以把“emailname.com”输入到他/她的浏览器的地址栏中。在一个实施例中，如方块602处所示，电子邮件系统前门读取小型文件，该小型文件在这里被称作用户标识小型文件(UIC)。该UIC至少包括用户的标识以及用户数据被存储的地方。此外，同样在方块602处所示，电子邮件系统发出去到登录服务器的重定向。在下面的实例2中描绘出这样的重定向的一个实例：loginserver.com?wreply＝https://CDN.emailname.com/...&s＝<encrypted>

[0060] 实例2。

[0061] 在实例2中，“s”代表“seed(种子)”，并且是至少包含数据集群名称、种子-GUID和CID的已加密结构。如方块604处所示，用户的浏览器遵循所述重定向去到登录页面。通过该登录页面，用户可以输入他/她的凭证，正如方块606处所示出的那样。这样的凭证例如可以包括电子邮件地址和/或用户名、口令等等。在用户输入这样的凭证的同时，采取其他动作以便获得用户数据的一部分，并且将该数据高速缓存在更靠近用户的CDN边缘服务器处。在一个实施例中，如方块608处所示，这是从包括图像标签的登录页面发起的。在一个实例中，所述图像标签可以具有作为当前正由认证模块在登录页面上为电子邮件系统所再现的定制内容的一部分的一个来源。在前面的实例1中示出了这样一个实例。结果是，当在方块606处用户正输入他/她的凭证时，浏览器并行地向实例1的URL发出请求。

[0062] 如方块610处所示，CDN接收图像请求，并且利用种子密钥来解密种子。方块612示出了CDN将种子-GUID发布到在该种子中标识出的特定集群，比如在下面的实例3中所示出的集群：https://cluster.emailname.com/

[0063] 实例3。

[0064] 在方块614处，电子邮件系统利用用户的收件箱的第一页面、主页内容或者默认的、根据用户优选项等等的其他第一页面来对CDN作出响应。此外，方块614示出了CDN将这

一内容存储在与电子邮件系统相比更靠近用户的CDN边缘服务器或其他服务器处。该CDN尚未把所述内容转发给用户,这是因为用户仍在进行认证。在一个实施例中,所述内容可以具有期满时间,比如一分钟、五分钟等等,但是其他实施例不包括这样的期满时间。

[0065] 如方块610处所提到的那样,CDN接收充当用户到达CDN并且提供种子的载体的图像请求。在方块616处,CDN可以返回图像以作为针对该图像请求的响应。在一个实施例中,并不实际寻求所述图像,因此所请求的图像是在所述图像被返回到浏览器时不被该浏览器使用的“虚设(dummy)”图像。这一点在方块616处示出。举例来说,所请求的图像可以是非常小的和/或透明的图像,该图像对于用户的浏览器显示将只有很小的影响或者没有影响。

[0066] 在某一时间,如方块618处所描绘的,用户完成输入他/她的凭证并且提交。如方块620处所示,登录模块对用户进行认证,并且对所述种子进行解密以便得到用户的集群、种子-GUID和CID。如果在方块622处确定该CID与被授予凭证的用户不匹配,则如方块624处所示,用户不被授权。另一方面,如果在方块622处确定该CID与被授予凭证的用户匹配,则方块626示出登录模块可以例如利用脚本语言生成页面,该脚本语言使得浏览器将种子-GUID发布到CDN边缘服务器(例如https://CDN.emailname.com)。该CDN接收来自用户的该发布以便提供CDN早前所高速缓存的内容(例如收件箱、主页等等),正如方块628处所示出的那样。如果所述内容已到期或者未被找到,则CDN可以把所述发布传递到电子邮件系统以进行正常处理。

[0067] 在一个实施例中,所述方案的安全性涉及通过安全套接字层(SSL)提供电子邮件数据,从而使得种子-GUID绝不会以明文传播。此外,通过使得所述种子成为一个三元组(集群、种子-GUID、CID)列表而不是单一三元组,可以将所述方案扩展到多个用户。

[0068] 图7描绘出可以在其中实施这里所描述的原理的代表性计算设备/系统700。代表性计算系统700可以代表这里所描述的任何计算/通信设备,比如例如电子邮件服务器、认证服务器、边缘服务器或者其他中间网络节点、用户设备等等,下面将提到它们的代表性差异。结合图7描述的计算环境是出于示例性目的而描述的,这是因为用于把特定于用户的内容朝向内容消费者迁移的结构和操作公开内容可适用于可以在其中传送用户内容的任何环境。还应当提到的是,图7的计算布置在一些实施例中可以跨多个设备分布。

[0069] 对于客户端设备和服务器二者而言,代表性计算系统700可以包括通过系统总线704耦合到许多模块的处理器702。所描绘的系统总线704代表可以直接或间接地耦合到所述计算环境的各个组件和模块的任何类型的总线结构。可以提供只读存储器(ROM)706以便存储由处理器702使用的固件。ROM 706代表任何类型的只读存储器,比如可编程ROM(PROM)、可擦除PROM(EPROM)等等。

[0070] 主机或系统总线704可以耦合到存储器控制器714,所述存储器控制器714进而通过存储器总线716耦合到存储器712。与这里所描述的原理相关联的操作模块可以被存储在任何存储装置中和/或利用任何存储装置,这些存储装置包括例如存储器712之类的易失性存储装置以及非易失性存储设备。图7示出了可以在其中暂时或永久性地存储应用、模块、数据和其他信息的各种其他代表性存储设备。举例来说,系统总线可以耦合到内部存储装置接口730,所述内部存储装置接口730可以耦合到例如硬盘驱动器之类的驱动器732。存储装置734与所述驱动器相关联或者是以其他方式利用所述驱动器可操作的。这样的存储装置的实例包括硬盘驱动器和其他磁性或光学介质、闪存和其他固态设备等等。内部存储装

置接口730可以利用任何类型的易失性或非易失性存储装置。

[0071] 类似地，用于可移除介质的接口736也可以耦合到总线704。驱动器738可以耦合到可移除存储装置接口736以便容纳可移除存储装置740并且对其采取动作，所述可移除存储装置740比如例如是软盘、光盘、存储器卡、闪存、外部硬盘等等。在某些情况下，可以提供主机适配器742以访问外部存储装置744。举例来说，主机适配器742可以通过小型计算机系统接口(SCSI)、光纤通道、串行高级技术附件(SATA)或eSATA以及/或者能够连接到外部存储装置744的其他类似接口与外部存储设备接口。通过网络接口746，还有其他的远程存储装置可能是计算系统700可以访问的。举例来说，与网络接口746相关联的有线和无线收发器允许通过一个或更多网络750与存储设备748通信。存储设备748可以代表分离的存储设备，或者与另一个计算系统、服务器等等相关联的存储装置。可以通过有线局域网(LAN)、无线LAN和/或包括例如因特网之类的全球区域网(GAN)在内的更大的网络实现与远程存储设备和系统的通信。

[0072] 用户设备、网络服务、认证服务器、边缘服务器和其他中间网络节点可以像这里所描述的那样传送信息。用户设备与服务器设备之间的通信可以通过直接连线、对等网络、基于本地基础设施的网络(例如有线和/或无线局域网)、例如城域网之类的非现场网络以及其他广域网、全球区域网等等来实施。在图7中示出了发送器752和接收器754以描绘所述代表性计算系统的按照这些或其他通信方法中的任何一种发送和/或接收数据的结构能力。发送器752和/或接收器754设备可以是独立组件，可以被集成为收发器，可以被集成到例如网络接口746等等之类的其他通信设备的现有部件中或者就是该现有部件。

[0073] 由于计算系统700可以被实施在用户设备、电子邮件服务器、认证服务器、边缘服务器等处，因此当其代表设备/服务器之一时，方块756代表与通信系统700通信的其他设备/服务器。除了可以被实施在用户设备、电子邮件服务器、认证服务器、边缘服务器等等中的每一个中的操作系统和其他软件/固件之外，每一个还可以包括可由执行指令的处理器702操作的软件模块。下面将描述用于若干代表性设备/服务器当中的每一个的一些代表性模块。

[0074] 当计算系统700代表用户或客户端设备时，客户端设备存储装置/存储器760代表可以被存储在例如计算机、智能电话、膝上型计算机等等之类的客户端设备的存储器712、存储装置734、740、744、748和/或其他数据保持设备中的内容。代表性的客户端设备存储装置/存储器760可以包括操作系统(未示出)以及由功能模块所表示的处理器实施的功能。举例来说，可以提供浏览器762和/或电子邮件客户端764。还可以存储数据766，比如UIC 768、种子密钥770等等。

[0075] 如果代表性计算系统700代表这里所描述的边缘服务器或其他中间服务器，则存储器712和/或存储装置734、740、744、748可以被用来存储结合前面所描述的服务器的功能操作使用的程序和数据。服务器存储装置/存储器772代表可以被存储在存储器712、存储装置734、740、744、748、数据库和/或其他数据保持设备中的内容。代表性的服务器存储装置/存储器772可以包括操作系统(未示出)、解密模块774、例如被高速缓存的用户内容778和种子密钥780之类的数据776等等。

[0076] 如果代表性计算系统700代表这里所描述的电子邮件服务器或其他网络服务，则存储器712和/或存储装置734、740、744、748可以被用来存储结合前面所描述的服务器的功

能操作所使用的程序和数据。服务器存储装置/存储器782代表可以被存储在存储器712、存储装置734、740、744、748、数据库和/或其他数据保持设备中的内容。代表性的服务器存储装置/存储器782例如可以包括操作系统(未示出)、电子邮件应用784、种子生成模块786以及例如所存储的用户内容788、种子密钥789之类的数据787等等。

[0077] 如果代表性计算系统700代表这里所描述的认证服务器，则存储器712和/或存储装置734、740、744、748可以被用来存储结合前面所描述的服务器的功能操作所使用的程序和数据。服务器存储装置/存储器782代表可以被存储在存储器712、存储装置734、740、744、748、数据库和/或其他数据保持设备中的内容。代表性的服务器存储装置/存储器790例如可以包括操作系统(未示出)以及结合图3所描述的模块，比如认证比较模块792、用户比较模块794、解密模块796、数据798等等。

[0078] 如前所述，图7中的代表性计算系统700是出于示例性目的而提供的，这是因为任何具有处理和通信能力的计算设备都可以利用这里所描述的教导来实施这里所描述的功能。还应当提到的是，除非另行表明，否则这里所描绘的流程图或其他图示中的各项功能的序列不需要是按照所描绘出的代表性顺序。

[0079] 正如在前面的实例中所表明的那样，描述了可以在计算设备上执行的方法，这例如是通过提供可由处理器(其包括物理处理器和/或逻辑处理器、控制器等等)执行的软件模块而实现的。所述方法还可以被存储在可以由处理器和/或准备信息以通过处理器处理的电路访问和读取的计算机可读介质或其他存储装置上。举例来说，所述计算机可读介质可以包括任何数字存储技术，包括存储器712、存储装置734、740、744、748、任何其他易失性或非易失性数字存储装置等等。让指令存储在这里所描述的计算机可读介质上有别于让指令传播或传输，这是因为所述传播传送指令，而不是例如对于其上存储了指令的计算机可读介质可能发生的存储指令。因此，除非另行表明，否则在以这种形式或类似形式提到其上存储有指令的一种/多种计算机可读介质时，所提到的是可以在其上存储或保持数据的有形介质。

[0080] 虽然用特定于结构特征和/或方法动作的语言描述了主题，但是应当理解的是，在所附权利要求书中限定的主题不一定受限于前面描述的特定特征或动作。相反，前面所描述的特定特征和动作是作为实施权利要求书的代表性形式而公开的。

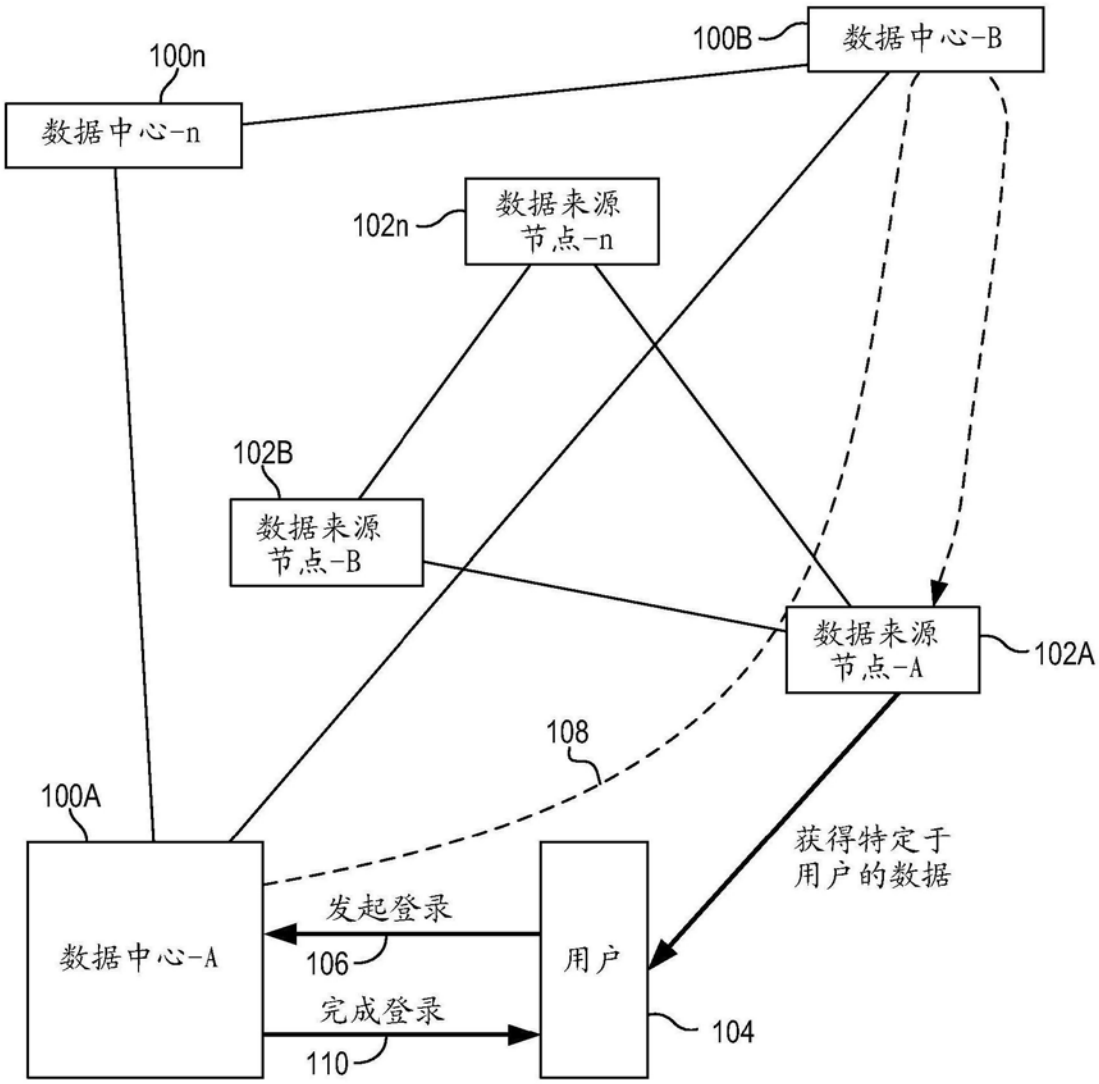

100n
数据中心-n
100B
数据中心-B
102n
数据来源节点-n
102B
数据来源节点-B
数据来源节点-A
102A
108
100A
数据中心-A
发起登录
106
完成登录
110
用户
104
获得特定于用户的数据

图1A

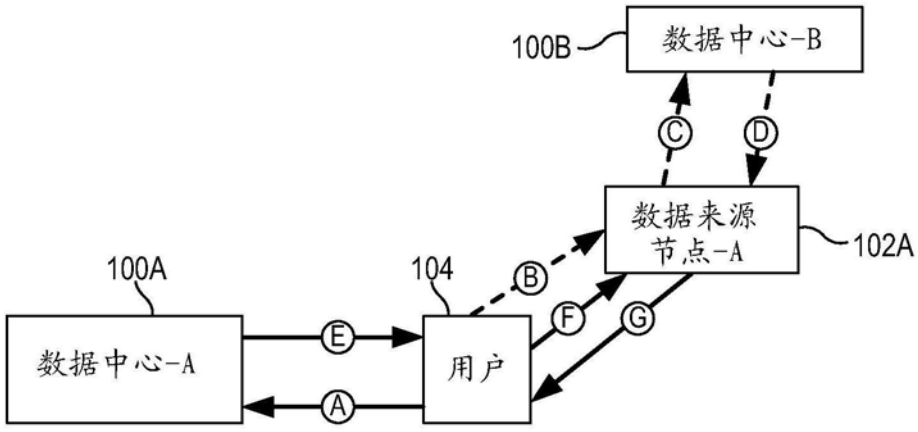

100B
数据中心-B
C
D
数据来源节点-A
102A
100A
数据中心-A
104
用户
E
A
B
F
G

图1B

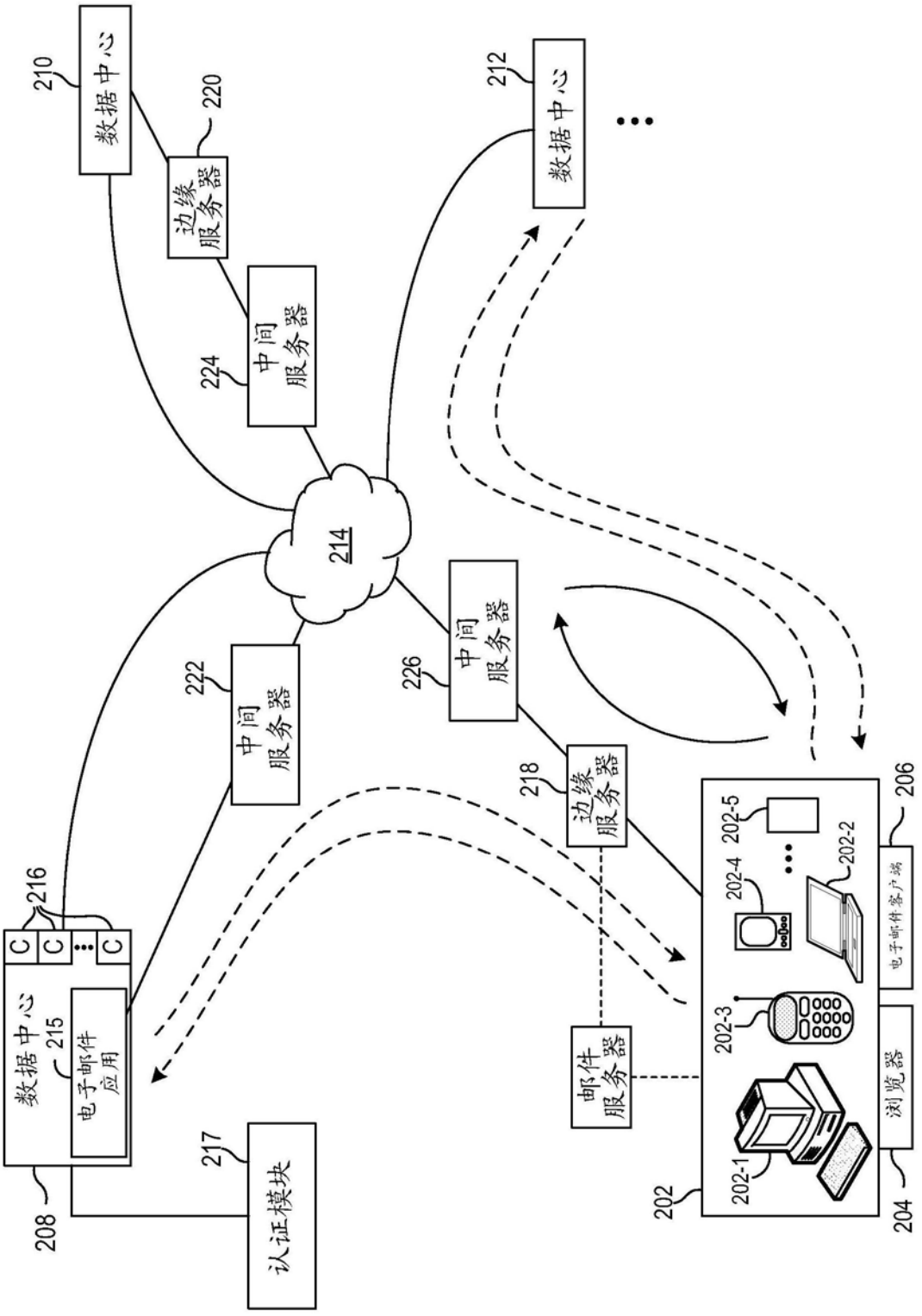

210
数据中心
220
边缘服务器
224
中间服务器
212
数据中心
214
222
中间服务器
226
中间服务器
218
边缘服务器
216
C
C
C
数据中心
215
电子邮件应用
208
217
认证模块
邮件服务器
202
202-1
202-3
202-4
202-5
202-2
206
电子邮件客户端
浏览器
204

图2

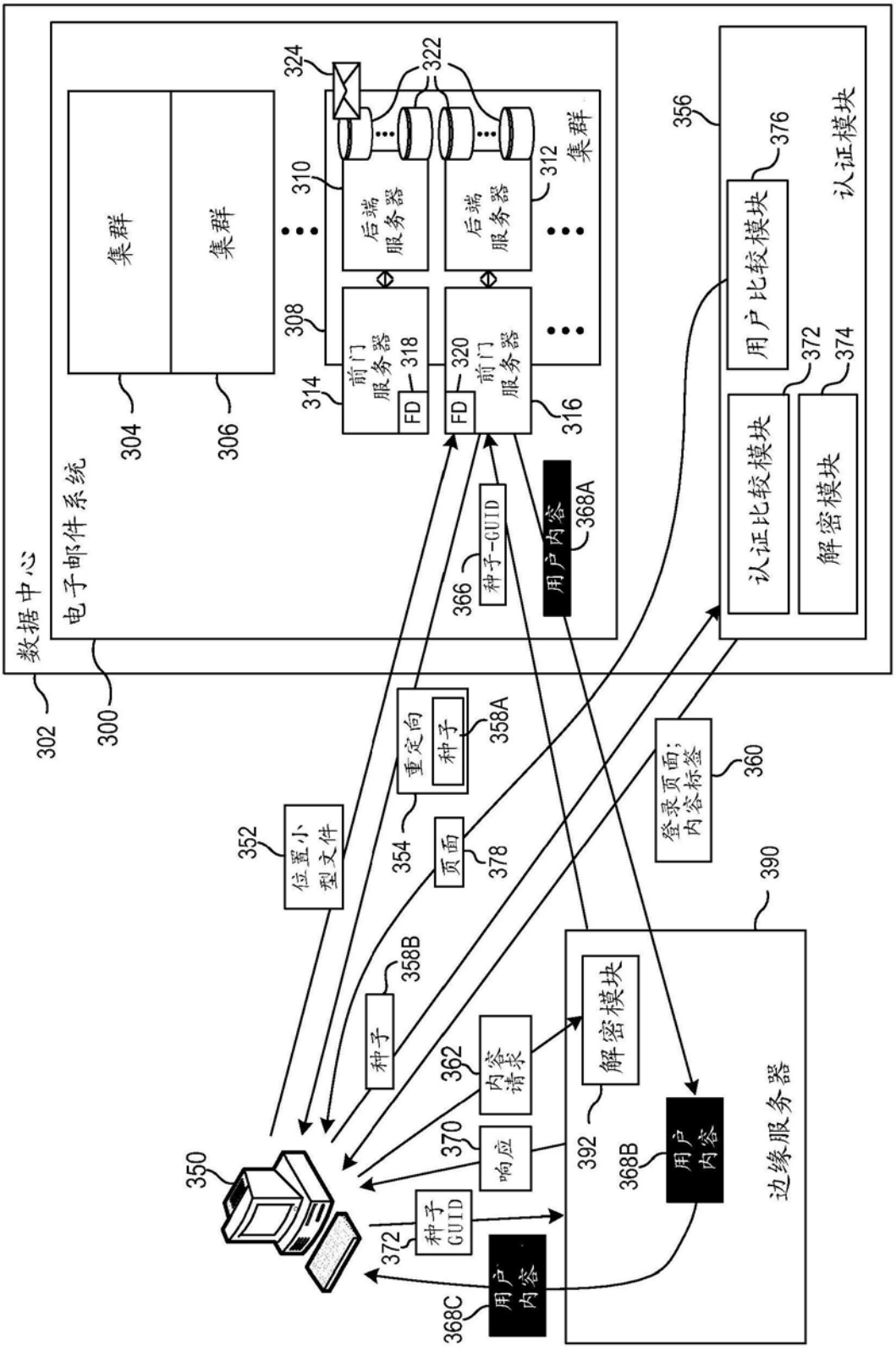

数据中心
302
电子邮件系统
300
集群
304
集群
306
后端服务器
310
后端服务器
312
集群
322
324
前门服务器
308
FD
318
前门服务器
314
FD
320
316
认证模块
356
用户比较模块
376
认证比较模块
372
解密模块
374
种子-GUID
366
用户内容
368A
重定向
种子
358A
354
页面
378
位置小型文件
352
登录页面；内容标签
360
390
种子
358B
内容请求
362
响应
370
解密模块
392
用户内容
368B
边缘服务器
350
种子GUID
372
用户内容
368C

图3

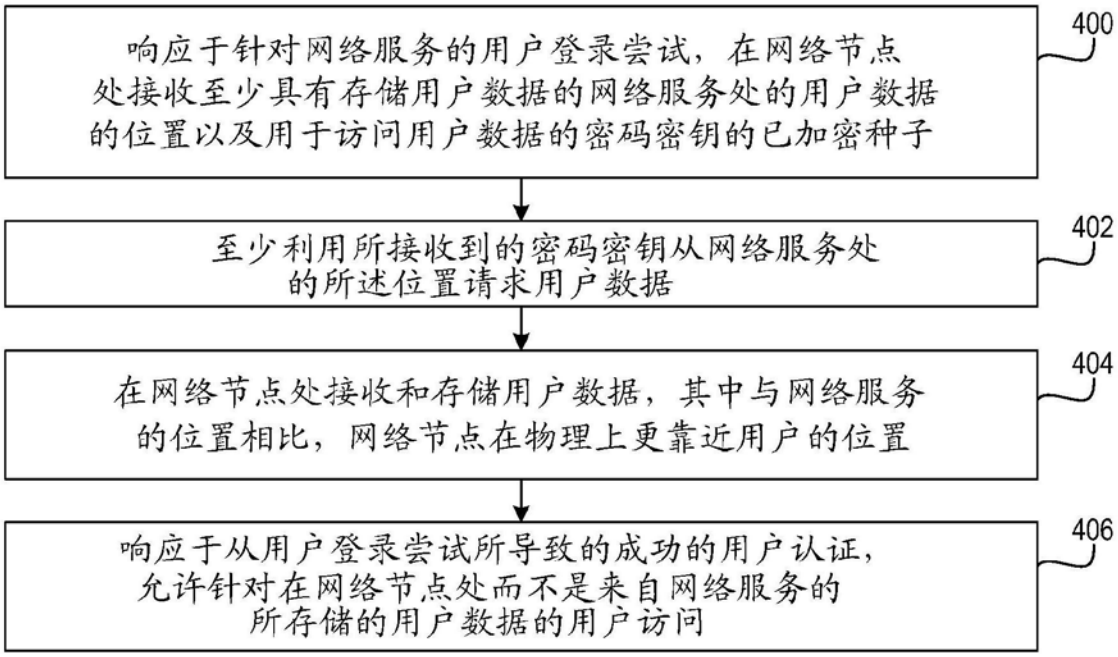

响应于针对网络服务的用户登录尝试，在网络节点处接收至少具有存储用户数据的网络服务处的用户数据的位置以及用于访问用户数据的密码密钥的已加密种子
400
至少利用所接收到的密码密钥从网络服务处的所述位置请求用户数据
402
在网络节点处接收和存储用户数据，其中与网络服务的位置相比，网络节点在物理上更靠近用户的位置
404
响应于从用户登录尝试所导致的成功的用户认证，允许针对在网络节点处而不是来自网络服务的所存储的用户数据的用户访问
406

图4

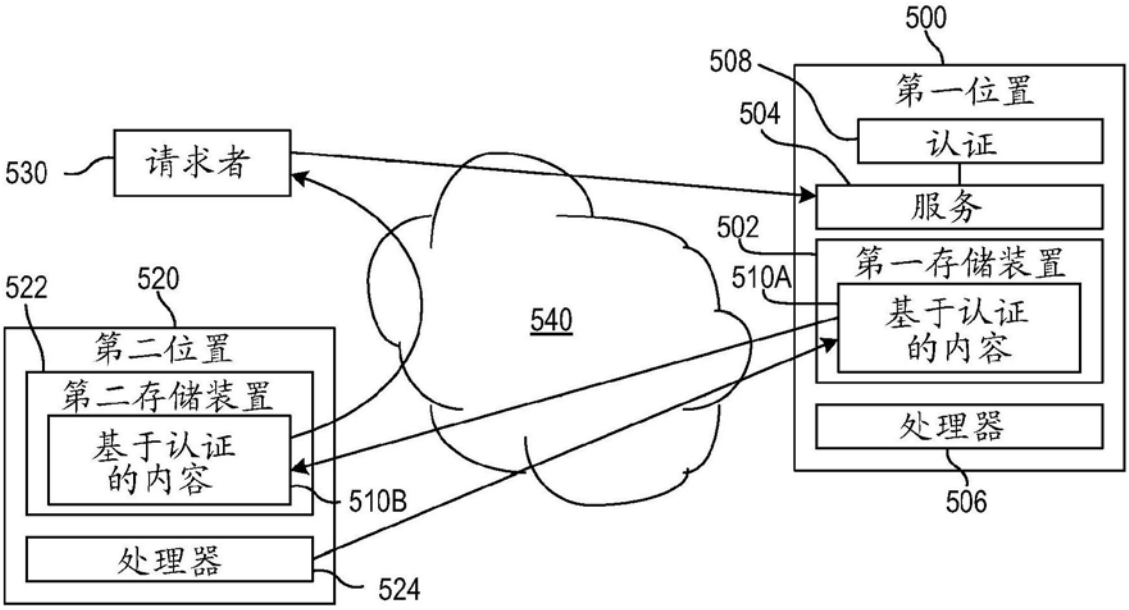

500
508
第一位置
504
认证
530
请求者
服务
502
第一存储装置
510A
基于认证的内容
522
520
540
第二位置
第二存储装置
基于认证的内容
510B
处理器
524
处理器
506

图5

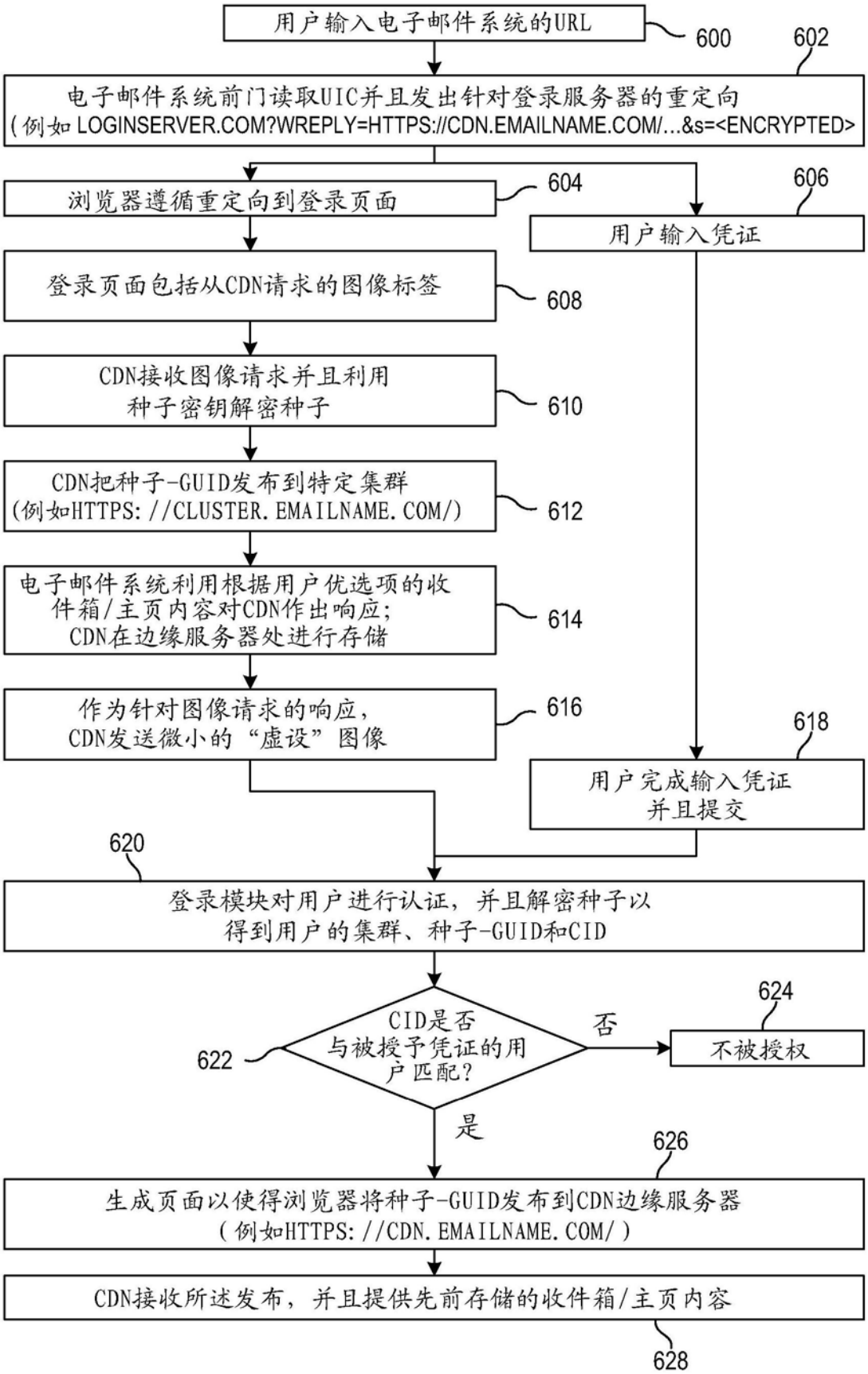

用户输入电子邮件系统的URL
600
602
电子邮件系统前门读取UIC并且发出针对登录服务器的重定向
(例如 LOGINSERVER.COM?WREPLY=HTTPS://CDN.EMAILNAME.COM/...&s=<ENCRYPTED>
浏览器遵循重定向到登录页面
604
606
用户输入凭证
登录页面包括从CDN请求的图像标签
608
CDN接收图像请求并且利用
种子密钥解密种子
610
CDN把种子-GUID发布到特定集群
(例如HTTPS://CLUSTER.EMAILNAME.COM/)
612
电子邮件系统利用根据用户优选项的收
件箱/主页内容对CDN作出响应;
CDN在边缘服务器处进行存储
614
作为针对图像请求的响应,
CDN发送微小的“虚设”图像
616
618
用户完成输入凭证
并且提交
620
登录模块对用户进行认证,并且解密种子以
得到用户的集群、种子-GUID和CID
622
CID是否
与被授予凭证的用
户匹配?
否
624
不被授权
是
626
生成页面以使得浏览器将种子-GUID发布到CDN边缘服务器
(例如HTTPS://CDN.EMAILNAME.COM/)
CDN接收所述发布,并且提供先前存储的收件箱/主页内容
628

图6

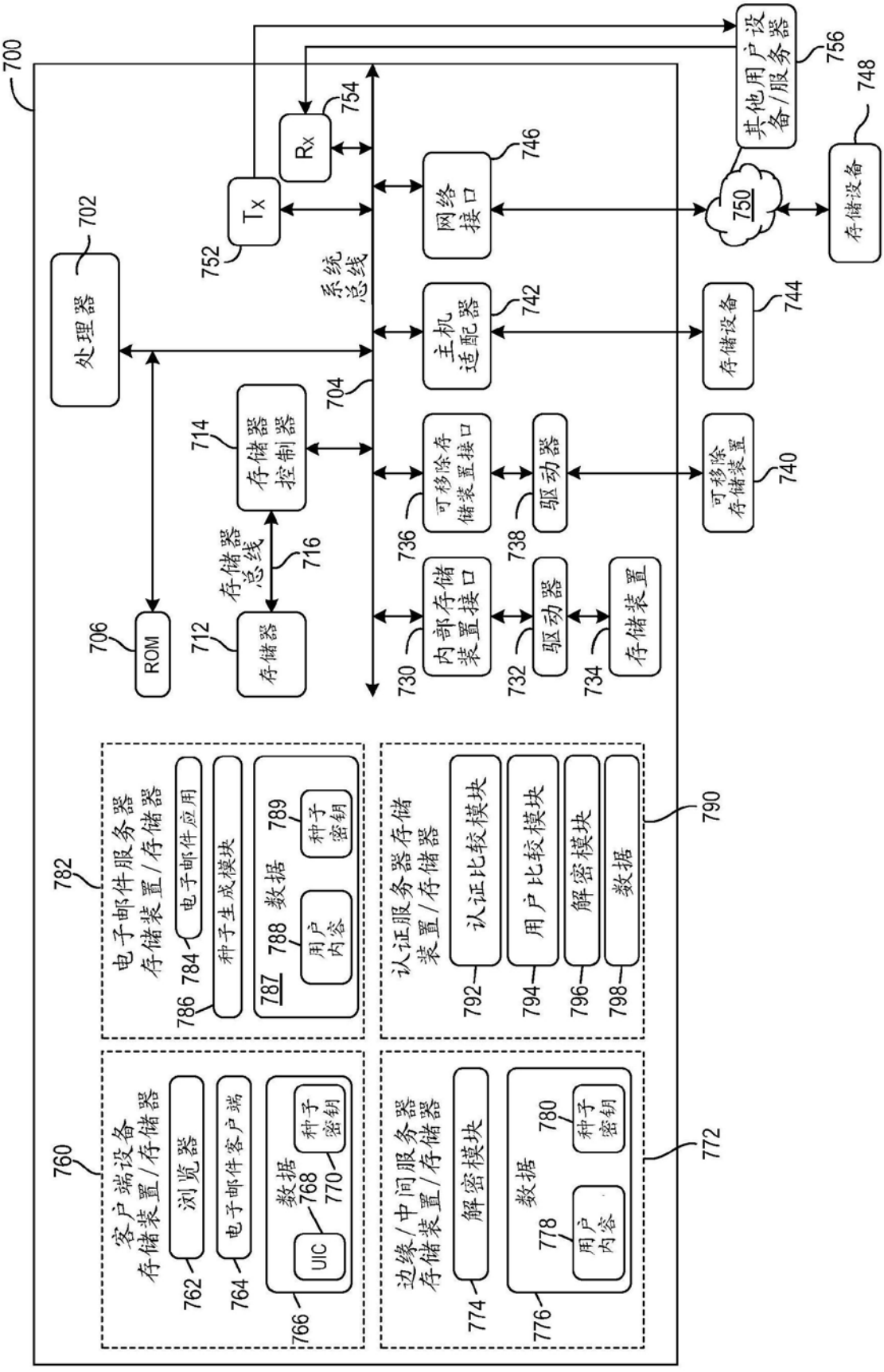

700
处理器
702
ROM
706
存储器
712
存储器控制器
714
存储器总线
716
系统总线
704
Tx
752
Rx
754
网络接口
746
主机适配器
742
可移除存储装置接口
736
驱动器
738
内部存储装置接口
730
驱动器
732
存储装置
734
存储设备
744
可移除存储装置
740
750
其他用户设备/服务器
756
存储设备
748
电子邮件服务器存储装置/存储器
782
电子邮件应用
784
种子生成模块
786
数据
787
用户内容
788
种子密钥
789
认证服务器存储装置/存储器
790
认证比较模块
792
用户比较模块
794
解密模块
796
数据
798
客户端设备存储装置/存储器
760
浏览器
762
电子邮件客户端
764
数据
766
UIC
768
种子密钥
770
边缘/中间服务器存储装置/存储器
772
解密模块
774
数据
776
用户内容
778
种子密钥
780

图7