



(12)发明专利

(10)授权公告号 CN 102938043 B

(45)授权公告日 2016.12.21

(21)申请号 201210507142.8

(22)申请日 2012.11.30

(65)同一申请的已公布的文献号

申请公布号 CN 102938043 A

(43)申请公布日 2013.02.20

(30)优先权数据

13/308,572 2011.12.01 US

(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 R·M·霍华德 T·C·米龙

W·D·泰勒 朱韶峰 E·艾登

V·维拉拉哈万

(74)专利代理机构 永新专利商标代理有限公司

72002

代理人 王英

(51)Int.Cl.

G06F 21/62(2013.01)

(56)对比文件

US 2003/0233544 A1,2003.12.18,

CN 101794366 A,2010.08.04,

CN 102238007 A,2011.11.09,

US 2010/0242097 A1,2010.09.23,

Adrienne Porter Felt et al.The

Effectiveness of Application Permissions.

《Proceedings of the 2ND USENIX conference

on Web application development》.2011,第

75-86页.

审查员 吴琼

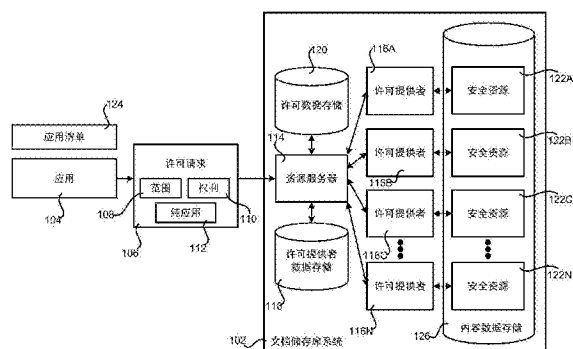
权利要求书2页 说明书10页 附图10页

(54)发明名称

授权应用对安全资源的访问

(57)摘要

本发明涉及授权应用对安全资源的访问。应用将许可请求提交给资源服务器。响应于接收到该请求,资源服务器生成要求用户授予或拒绝所请求的许可的用户界面。如果许可被授予,则存储指示应用具有所请求的许可的数据。在接收到对资源的运行时请求时,资源服务器确定该请求由用户作出、由应用作出还是由应用代表用户作出。如果该请求仅由应用作出,则仅在应用具有以不代表用户的直接调用方式访问资源的许可的情况下准许该请求。如果该请求由应用代表用户作出,则仅在用户和应用两者都具有足够的许可的情况下才准许该请求。



1. 一种用于授权对文档储存库系统中的安全资源的访问的计算机实现的方法,该方法包括执行以下计算机实现的操作:

接收在文档储存库系统中的安全资源上执行动作的请求;

响应于接收到所述请求,确定所述请求仅由用户作出、仅由应用作出、还是由应用代表用户作出;

响应于确定所述请求已由应用代表用户作出,则在所述应用和所述用户两者都具有访问所述安全资源的许可的情况下准许所述请求,其中如果所述应用具有与所述用户不同的访问特权级别,则所述请求被授予到由向所述用户授予的访问特权级别所准许的程度;以及

响应于确定所述请求仅由应用作出,在所述应用已被授予以不代表用户的直接调用的方式访问所述安全资源的许可的情况下才准许所述请求。

2. 如权利要求1所述的计算机实现的方法,其特征在于,还包括响应于确定所述请求已由应用代表用户作出,存储将所请求的动作的执行归因于所述应用和所述用户两者的数据。

3. 一种用于授权对文档储存库系统中的安全资源的访问的方法,所述方法包括:

从应用接收请求访问由文档储存库系统代表用户维护的一个或多个安全资源的许可的许可请求;

响应于接收到所述许可请求,标识与所述一个或多个安全资源相关联的一个或多个许可提供者,从所标识的每一个许可提供者中请求描述对相关的安全资源的所请求的许可的数据,将从许可提供者处接收到的数据聚集在用户界面中,以及向所述文档储存库系统的当前用户显示所述用户界面;

通过所述用户界面从所述当前用户处接收指示所述应用被授予访问所述一个或多个安全资源的所请求的许可的指示;以及

响应于接收到所述应用被授予所请求的许可的指示,存储指示所述应用具有访问所述一个或多个安全资源的所请求的许可的数据,以供在处理所述应用对所述安全资源的运行时请求时使用;

接收在所述文档储存库系统中的安全资源上执行动作的运行时请求;

响应于接收到所述运行时请求,确定所述运行时请求仅由用户作出、由应用作出、还是由应用代表用户作出;以及

响应于确定所述运行时请求已由应用代表用户作出,仅在所述应用和所述用户两者都具有访问所述安全资源的许可的情况下才准许所述运行时请求,其中如果所述应用具有与所述用户不同的访问特权级别,则所述运行时请求被授予到由向所述用户授予的访问特权级别所准许的程度,以及

响应于确定所述运行时请求仅由应用作出,在所述应用已被授予以不代表用户的直接调用的方式访问所述安全资源的许可的情况下才准许所述运行时请求。

4. 如权利要求3所述的方法,其特征在于,还包括:

确定所述当前用户是否具有足够的许可来授予所述应用访问所述一个或多个安全资源的许可,以及

响应于确定所述当前用户不具有足够的许可来授予所述应用访问所述一个或多个安

全资源的许可,拒绝所述许可请求。

5.如权利要求3所述的方法,其特征在于,所述许可请求进一步包括所述应用请求以不代表用户的直接调用的方式来利用所述一个或多个安全资源的请求。

6.如权利要求5所述的方法,其特征在于,还包括:

通过所述用户界面从所述当前用户处接收指示所述应用被授予以直接调用的方式利用所述一个或多个安全资源的许可的指示;以及

存储指示所述应用具有以不代表用户的直接调用的方式使用所述一个或多个安全资源的许可的数据,以供在处理来自应用的对所述一个或多个安全资源的运行时请求时使用。

7.如权利要求3所述的方法,其特征在于,以应用清单的方式将所述许可请求提供给所述文档储存库系统。

8.如权利要求3所述的方法,其特征在于,还包括:

在从所述应用接收所述许可请求之前,将所述许可提供者中的每一个注册为与安全资源的范围相关联。

9.一种用于授权对文档储存库系统中的安全资源的访问的计算机实现的方法,所述方法包括:

从应用接收请求访问文档储存库系统所维护的一个或多个安全资源的许可的许可请求;

响应于接收到所述许可请求,向所述文档储存库系统的用户显示请求该用户准许或拒绝所述许可请求的用户界面;

通过所述用户界面从所述用户处接收指示所述应用被授予访问所述一个或多个安全资源的所请求的许可的指示;

响应于接收到所述应用被授予所请求的许可的指示,存储指示所述应用具有访问所述一个或多个安全资源的所请求的许可的数据,以供在处理所述应用对所述安全资源的运行时请求时使用;

接收在所述文档储存库系统中的安全资源上执行动作的运行时请求;

响应于接收到所述运行时请求,确定所述运行时请求仅由用户作出、由应用作出、还是由应用代表用户作出;以及

响应于确定所述运行时请求已由应用代表用户作出,仅在所述应用和所述用户两者都具有访问所述安全资源的许可的情况下才准许所述运行时请求,其中如果所述应用具有与所述用户不同的访问特权级别,则所述运行时请求被授予到由向所述用户授予的访问特权级别所准许的程度,以及

响应于确定所述运行时请求仅由应用作出,在所述应用已被授予以不代表用户的直接调用的方式访问所述安全资源的许可的情况下才准许所述运行时请求。

授权应用对安全资源的访问

技术领域

[0001] 本发明涉及如何授权对安全资源的访问的技术。

背景技术

[0002] 许多万维网(“Web”)应用允许安装并使用扩展web应用的能力的自定义第三方应用。这些第三方应用从许可角度来说一般作为web应用的当前用户来执行。结果,这样的第三方应用一般可以执行当前用户能够执行的任何动作,这些动作通常在与web应用结合在一起执行的应用的某一受限边界集内。这要求安装该第三方应用的系统管理员给予该应用显著的信任,因为该应用可以读取、修改或删除Web应用中该应用的任何用户都具有访问权的任何信息。

[0003] 以上描述的问题的一个解决方案是将第三方应用的访问权限限制于web应用所提供的仅某一功能。例如,可通过限制向第三方应用展示的应用编程接口(API)来仅给予该应用对web应用的某些能力的访问权。对以上描述的问题的另一方案是限制安全该应用的系统管理员所作出的信任决定的范围。例如,可以使web应用内的各环境彼此隔离,使得各第三方应用可被安装在分开的环境中,而没有破坏其他环境的风险。例如,可利用该解决方案来限制应用对展示了敏感数据的环境的访问。然而,在给定利用第三方应用的最普通理由之一是跨不同的环境聚集数据的事实的情况下,该解决方案严重地受限。结果,跨web应用部署应用于所有公司的环境的应用在这种场景下难以或无法安装。

[0004] 如上所述,第三方应用从许可角度来说一般作为web应用的当前用户来执行。这意味着这些应用仅可执行它们的用户具有执行许可的那些动作。然而,在许多情况下,需要允许用户或用户组通过使用应用来执行他们的许可不准许他们直接执行的动作。例如,费用报告应用可能在符合某些条件(例如,较小的值)时批准费用报表,但用户不应具有直接批准费用报表而无需通过该应用来执行该操作的许可。当该应用作为当前用户来执行时,这种类型的操作并不可能。一些系统通过允许应用提高给系统账户的许可来阐明这种限制,该系统账户在系统内不具有许可限制。然而,这种解决方案使得系统管理员甚至更不愿意将程序安装在展示了敏感信息的环境中。

[0005] 本文中所做出的公开正是针对这些以及其他考虑事项而呈现的。

发明内容

[0006] 在此描述了用于授权应用对安全资源的访问权的概念和技术。在此处公开的技术的整个实现中,安全资源的所有者可向应用授予利用安全资源的特权。利用所授予的特权,应用可以在运行时以与安全资料的所有者相同的程度直接(即,没有用户)利用该资料。然而,如果用户利用应用来访问安全资料,则将对资源的使用限制于用户的特权的程度。通过这种方式,可以在应用直接访问安全资源时,将该应用的特权提高到安全资源的所用者的级别。但是,在用户利用该应用来访问资源时,对安全资源的访问被限制为用户许可的程度。

[0007] 根据在此呈现的一个方面,诸如文档储存库应用之类的web应用被配置成允许使用自定义第三方应用,该第三方应用扩展web应用的能力。为了获得用于访问和利用web应用所管理的安全资源(诸如,内容数据库中的项目)的许可,应用首先向作为web应用的一部分来执行的资源服务器提交许可请求。该许可请求标识该应用所请求的范围和权限。许可请求还可请求授予应用以不代表用户的直接调用方式来利用一个或多个安全资源的许可。可经由超文本传输协议(HTTP)请求、应用清单、web应用所提供的用户界面(UI)的方式通过web应用所提供的API或以另一方式来提交许可请求。

[0008] 响应于接收到许可请求,资源服务器被配置成标识与针对其请求了许可的安全资源相关联的一个或多个许可提供者。资源服务器随后从所标识的每一许可提供者处请求描述了所请求的对相关联的安全资源的许可的数据。随后将该数据聚集在向web应用的当前用户显示的UI中。UI要求用户向该应用授予或拒绝所请求的许可。如果用户授予该应用所请求的许可,则存储指示应用具有所请求的许可的数据。在运行时,该数据被利用来处理该应用对由web应用来管理安全资源的运行时请求。

[0009] 当对安全资源执行动作的运行时请求被资源服务器接收到时,该资源服务器确定该请求是已由用户作出的、仅由应用作出的、还是由应用代表用户作出的。如果该请求仅由应用作出,则资源服务器仅在以前述方式授予了该应用以不代表用户的直接调用方式访问安全资源的许可的情况下才准许该请求。如果该请求是由应用代表用户作出的,则资源服务器仅在用户和应用都具有执行所请求的动作的许可的情况下准许该请求。资源服务器还存储将该动作在安全资源上的执行归结于用户、应用或用户和应用两者的历史数据。

[0010] 本发明内容并不旨在标识所要求保护的的主题的关键特征或必要特征,也不旨在使用本发明内容来限制所要求保护的的主题的范围。此外,所要求保护的的主题不限于解决在本公开的任一部分中所提及的任何或所有缺点的实现。

附图说明

[0011] 图1是示出在此处公开的一个实施例中应用和文档储存库系统的操作的各方面的软件架构图;

[0012] 图2是示出在此处公开的一个实施例中用于注册许可提供者的一个例程的各方面的流程图;

[0013] 图3A—3B是示出在此处公开的一个实施例中用于向资源服务器注册应用的一个例程的各方面的流程图;

[0014] 图4A是示出在此处公开的一个实施例中利用的示例许可请求的格式和结构的数据结构图;

[0015] 图4B是示出在此处公开的一个实施例中用于向应用授予许可的一个说明性用户界面的用户界面图;

[0016] 图5是示出在此处公开的一个实施例中利用的、用于处理资源请求的机制的各方面的网络图;

[0017] 图6A—6B是根据一个实施例的用于处理对安全资源的请求的一个例程的各方面的流程图;以及

[0018] 图7是示出用于能够实现本文所提出的各种实施例的计算系统的说明性计算机硬

件和软件体系结构的计算机体系结构图。

具体实施方式

[0019] 以下具体实施方式涉及用于授权应用对安全资源的访问权的概念和技术。如之前简要讨论的,通过使用在此公开的技术,结合web应用来执行的应用可以以与资源的所有者相同的程度在运行时直接利用安全资源。当用户使用该应用来利用安全资源时,用户和应用两者都必须具有利用该安全资源的合适许可。关于这些特征和其他特征的更多细节将在以下参考图1-7来提供。

[0020] 尽管在结合一个或多个计算机系统上的操作系统和各个程序的执行而执行的程序模块的一般上下文中呈现了本文中所描述的主题,但本领域技术人员将认识到,其他实现可结合其他类型的程序模块来执行。一般地,程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、组件、数据结构、以及其他类型的结构。此外,本领域技术人员应当理解,可用其他计算机系统配置来实施本文中所描述的主题,这些计算机系统配置包括手持式设备、多处理器系统、基于微处理器或可编程的消费电子产品、小型计算机、大型计算机等。

[0021] 在以下详细描述中,参考形成详细描述的一部分并为例示具体实施例或示例而示出的附图。现在参考附图(全部若干附图中相同的标号表示相同的元素),将描述用于授权应用对安全资源的访问权的计算系统和方法的各方面。

[0022] 图1是示出在此处公开的一个实施例中应用104和文档储存库系统102的操作的各方面的软件架构图。文档储存库系统102是被配置为执行基于web的文档储存库应用(未示出)的一个或多个计算系统。文档储存库系统102提供用于存储、访问及在该文档储存库系统102的各授权用户之间共享文档和可能其他类型的项目的功能。在这个方面,文档储存库系统102可提供允许用户创建、修改、删除和以其他方式利用存储在内容数据存储126中的文档和其他类型的电子项目的功能。

[0023] 文档储存库系统102可以基于许可来限制对内容数据存储126中的项目的访问。例如,可以对文档储存库系统102的用户设置许可,使得仅某些用户被准许访问或修改内容数据存储126中的某些项目。通过以前面描述的方式使用许可,存储在内容数据存储126中的项目是受保护的,因此这些项目在此被称为安全资源122A—122N(合起来为安全资源122)。

[0024] 应该理解,尽管在此主要将安全资源122描述为内容数据存储126中的项目,但安全资源122可以是可基于许可来控制访问权的任何自他类型的计算资源。还应该理解,尽管在此公开的实施例主要是在文档储存库系统102的上下文中描述的,但在此公开的各实施例不限于这样的实现。而且,在此公开的各实施例可以与准许应用访问安全资源的任何类型的计算系统一起使用。

[0025] 在一个实施例中,文档储存库系统102包括用于控制对安全资源122的访问的资源服务器114。资源服务器114是被配置成接收安全资源122和对访问安全资源的请求作出响应的一个或多个软件和/或硬件组件。资源服务器114还提供注册将利用安全资源122的应用(诸如,应用104)的功能。

[0026] 应用104是被配置成与文档储存库系统102一起使用的应用。例如,应用104可以扩展文档储存库系统102所提供的功能。应用104可以是基于web的应用或者可以直接在文档

储存库系统102上执行。为了提供所需的功能,应用104一般利用一个或多个安全资源122。应该理解,尽管应用104在此主要被描述成用于扩展文档储存库系统102所提供的功能的应用,但在此利用的各实施例可以用其他类型的应用来实施。

[0027] 为了获得利用安全资源122的授权,在一个实施例中,应用104向资源服务器114提供许可请求106。许可请求106是定义应用104所请求的访问的范围108的数据以及为指定范围定义所请求的许可的权利110。许可请求106还可包括“纯应用”请求112,该请求112通过直接调用而非代表用户的方式请求向应用104授予利用安全资源122中的一个或多个的许可。应用104可经由超文本传输协议(HTTP)请求、应用清单124、文档储存库系统102所提供的用户界面(UI)的方式通过文档储存库系统102所提供的API或以另一方式来提交许可请求。以下将参考图4A描述一示例许可请求106。

[0028] 响应于从应用104接收到许可请求106,资源服务器114标识一个或多个许可提供者116A—116N(统称为许可提供者116),所述一个或多个许可提供者116A—116N已分别注册为对安全资源122A—122N的许可的提供者。在图1所示的示例中,例如,许可提供者116A已注册为对安全资源122A的许可的提供者。如果许可请求106中的范围108包括安全资源122A,则资源服务器114会将许可提供者116A标识为许可请求106的相关许可提供者。

[0029] 为了向资源服务器114进行注册,每一许可提供者116向资源服务器114指示与该许可提供者相关联的资源范围。每一许可提供者116还可向资源服务器114注册回调函数。例如,每一许可提供者116可以向资源服务器114注册资源服务器114可通过其来获得描述与安全资源122相关联的许可的数据的回调函数。如以下将详细描述的,资源服务器114可利用该数据来构建向用户指示由应用104在许可请求106中请求的许可的UI。

[0030] 每一许可提供者116还可注册资源服务器114可通过其来提供已经准许许可请求106的通知的回调函数。资源服务器114将包括标识回调函数的数据的注册数据存储在许可提供者数据存储118中。与一种用于注册许可提供者116的过程有关的附加细节将在以下参考图2来提供。

[0031] 一旦资源服务器114已经将许可提供者116标识为与许可请求106相关,资源服务器114调用所标识的每一个提供者116的用于获取描述所请求的许可的数据的回调函数。资源服务器114可将许可请求106中的范围108和权利110与标识当前用户的当前上下文一起传递给所标识的许可提供者116。进而,所调用的每一许可提供者116确定当前用户是否具有足够的特权来向应用104授予许可请求106中所请求的许可。

[0032] 如果用户不具有足够的特权来向应用104授予所请求的许可,则许可请求106将被拒绝。如果用户不具有足够的特权来准许许可请求106,则每一许可提供者116将向资源服务器114返回可用于构建向用户指示应用104所请求的许可的UI的数据。该数据可以用超文本标记语言(HTML)的格式、空白文本的格式、或者用适合于直接包括在UI元素(例如,对话框)中的另一格式。

[0033] 一旦资源服务器114已经从所标识的许可提供者116处接收到了响应,则许可服务器114将所接收的数据聚集在向当前用户显示的UI中。UI阐明了对所请求的许可的描述,并要求用户授予或拒绝由应用104在许可请求106中请求的许可。将在以下参考图4B描述一个这样的说明性UI。如果用户通过UI向应用104授予所请求的许可,则资源服务器114将指示应用104具有所请求的许可的数据存储在许可数据存储120中。在运行时,资源服务器114利

用该数据来处理应用104请求对安全资源122执行动作的请求。以下将参考图5和图6A—6B来提供与资源服务器114所执行的运行时处理有关的附加细节。

[0034] 图2是示出在此处公开的一个实施例中用于注册许可提供者116的一个例程200的各方面的流程图。应该了解,这里参考图2和其他附图所描述的逻辑操作是(1)作为计算机实现的动作或在计算系统上运行的程序模块的序列和/或(2)计算系统内的互连机器逻辑电路或电路模块来实现的。该实现是取决于计算系统的性能及其他要求的选择问题。因此,此处所描述的逻辑操作被不同地称为操作、结构设备、动作或模块。这些操作、结构设备、动作和模块可以用软件、固件、专用数字逻辑,以及其任何组合来实现。还应该理解,可以执行比附图中示出并在此处描述的操作更多或更少的操作。这些操作还可以按与此处所描述的那些操作不同的次序来执行。

[0035] 例程200始于操作202,在操作202,许可提供者116向资源服务器114提供对许可提供者116应该为其注册的安全资源的范围的指示。例程200随后前进到操作204,在操作204,许可提供者116向资源服务器114提供可通过其来获得描述所请求的许可的数据的回调函数。如上简要讨论的,资源服务器114可利用该信息来生成请求用户批准或拒绝许可请求106的UI。

[0036] 从操作204,例程200前进到操作206,在操作206许可提供者116向资源服务器114提供可由资源服务器114来向许可提供者116通知许可请求106已被准许的回调函数。应该理解,可以用一个或多个数据结构来提供操作202、204和206处提供的信息。还可以使用可扩展标记语言(XML)、使用另一结构化语言格式、或以另一种方式来一起格式化这些信息。

[0037] 从操作206,例程200前进到操作208,在操作208,资源服务器114将许可提供者116所提供的范围和回调函数存储在许可提供者数据存储118中。一旦已经存储了该数据,例程200从操作208前进到操作210,在操作210例程200结束。

[0038] 图3A—3B是示出在此处公开的一个实施例中用于向资源服务器114注册应用104的一个例程300的各方面的流程图。例程300在资源服务器114接收许可请求106的操作处开始。例程300随后继续至操作304,在操作304,资源服务器114标识与许可请求106中阐明的各许可的范围108相关联的许可提供者116。例如,资源服务器114可通过许可提供者数据存储118中存储的信息来进行迭代,以便标识与范围108相关联的许可提供者116。一旦标识了许可提供者116,例程300就从操作304前进至操作306。

[0039] 在操作306,资源服务器114将所请求的范围108、权利110、纯应用请求112(如果存在的话)以及当前上下文传递给从其请求许可的所注册的各许可提供者116中的每一个。响应于接收到该信息,每一许可提供者116确定当前用户是否具有足够的权威来授予所请求的许可。这可例如通过引用存储在许可数据存储120中的、指示当前用户所持有的特权的的数据来完成。如果用户不能向应用104授予所请求的许可,则例程300从操作310前进到操作312,在操作312,许可请求106被拒绝。另外,可向用户呈现指示许可不可被授予的UI。例程300然后从操作312前进到操作314,在操作314例程300结束。

[0040] 如果用户不拥有足够的特权来准许许可请求106,则例程300从操作310前进到操作316(如图3B所示)。在操作316,资源服务器114调用所标识的每一许可提供者116的、用于获得描述向每一许可提供者116请求的许可的数据的回调函数。进而,所调用的每一许可提供者116将所请求的信息提供给资源服务器114。例程300随后从操作316前进至操作318。

[0041] 在操作318,资源服务器114将从许可提供者116处接收到的数据聚集在UI中,并向当前用户呈现该UI。如上所述,UI还要求用户批准或决绝向许可请求106中阐明的应用104授予特权。以下将参考图4B描述一个这样的UI。

[0042] 如果用户决绝向应用104授予特权,则例程300从操作320前进到操作322。在操作322,许可请求106被决绝。另外,可向用户呈现指示不可授予所请求的许可的UI。例程300然后从操作322前进至操作328,在操作328例程300结束。

[0043] 如果用户批准许可请求106,则例程300从操作320前进到操作324。在操作324,资源服务器调用由所标识的每一许可提供者116展示的、用于指示许可请求106被准许的回调函数。例程300随后前进至操作326,在操作326,将指示向应用104授予所请求的许可的数据存储在许可数据存储120中。如上所述,在运行时利用该数据来确定应该批准还是决绝从应用104接收到的对安全资源122的请求。从操作326,例程300前进至操作328,在操作328例程300结束。

[0044] 图4A是示出在此处公开的一个实施例中利用的示例许可请求106的格式和结构的数据结构图。具体地,在图4A所示的示例许可请求106中,应用104正在请求对四个不同的安全资源的许可。因此,许可请求106包括与每一个资源相对应的XML元素。具体地,一个元素对应于对文档库的特权的请求,一个元素对应于对用户简档存储的特权的请求,一个元素对应于对日历的特权的请求,且另一元素对应于对联系人的特权的请求。

[0045] 对于请求对其的特权的每一安全资源,许可请求106还指定所请求的权利。例如,图4A中示出的许可请求106请求读取联系人、读取日历以及对文档库进行写入的权利。应该理解,还可请求其他类型的权利。还应该理解,尽管图4A中示出的许可请求是利用XML来表达的,但也可以利用其他结构化或非结构化语言。也可利用数据的其他元素、配置和安排来表达范围108、权利110、纯应用请求112和许可请求106的任何其他元素。

[0046] 图4B是示出在此处公开的一个实施例中用于向应用104授予许可的一个说明性用户界面400的用户界面图。如上所述,资源服务器114在接收到许可请求106之后生成用户界面400。图4B中示出的UI 400是基于图4A中示出的许可请求106而生成的。

[0047] 用户界面400包括向用户解释应用已经请求了对安全资源122的访问权的文本。用户界面400还包括描述了由应用104在许可请求106中请求的各个许可的文本。如上所述,可以以回调函数的方式从与许可请求106中阐明的范围108相关联的许可提供者116处获得该信息。在一个实施例中,从许可提供者116处接收到的信息被显示在域402A—402D中。

[0048] 在图4B所示的示例中,例如,从许可提供者116处接收到的、针对描述所请求的许可的文档库的数据可被示出在域402A中。从许可提供者116处接收到的、针对用户简档的数据可被显示在域402B中。从许可提供者116处接收到的、针对描述所请求的许可的日历的数据可被示出在域402C中。从许可提供者116处接收到的、针对联系人的数据可被显示在域402D中。当前用户可以选择UI控件404B来授予所请求的特权。另选地,用户可以选择UI控件404A来决绝许可请求106。

[0049] 应该理解,图4B中示出的用户界面仅仅是说明性的,可以呈现更多或更少的数据。例如,可以呈现附加的域402,包括指示已作出了纯应用请求112的域。另外,所呈现的数据可以以不同的方式来呈现,或者可利用与图4B中所示的不同的UI控件。其他变型对于本领域的技术人员而言将是明显的。

[0050] 图5是示出在此处公开的一个实施例中利用的、用于处理运行时资源请求的机制的各方面的网络图。在图5所示的示例中,用户502和应用104可以向资源服务器114发起对安全资源的请求(资源请求504)。具体地,用户502可以在不使用应用104的情况下直接通过文档储存库系统102来生成对安全资源122A的资源请求504A。类似地,应用104可以直接地而非代表用户502生成对安全资源122A的资源请求504C。另外,用户502可以利用应用104来生成由应用104和用户502作出的资源请求504B。

[0051] 为了确定资源请求504仅由用户502、仅由应用104、还是由应用104代表用户502作出的,可以利用合适的认证机制。通过这样的机制,在资源请求504A仅由用户502作出时,将用户身份506A呈现给资源服务器114。当资源请求504C仅由应用104作出时,将应用身份506C呈现给资源服务器114。类似地,在资源请求504B由应用104代表用户502作出时,将应用和用户身份506B呈现给资源服务器114。可以利用合适的协议来在资源请求504被作出时将身份506呈现给资源服务器114。也可以利用其他机制来认证用户502和应用104,并在资源请求504仅由用户502作出、仅由应用102作出或由104代表用户502作出时向资源服务器114进行指示。

[0052] 响应于接收到资源请求504,资源服务器114确定资源请求504由用户502作出、仅由应用104作出、还是由应用104代表用户502作出。资源服务器114随后从许可数据存储120中检索数据以确定可准许资源请求504还是应拒绝资源请求504。如果资源请求504仅由应用104作出,则资源服务器114仅在以上述方式授予了应用104以不代表用户的直接调用方式访问安全资源122的许可的情况下才准许该请求504。如果资源请求504由应用104代表用户502作出,则资源服务器114仅在用户502和应用104两者都具有执行所请求的动作的许可的情况下才准许该请求504。资源服务器114还可在合适时将动作在安全资源122上的执行归因于用户502、应用104、或用户502和应用104两者的数据存储于历史数据存储508中。关于这些过程的其他细节将在以下参考图6A-6B来提供。

[0053] 图6A-6B是根据一个实施例的用于处理对安全资源122的运行时请求504的一个例程600的各方面的流程图。例程600始于操作602,在操作602资源服务器114接收资源请求504。响应于接收到资源请求504,例程600前进到操作604,在操作604资源服务器114确定所接收的请求504是否是仅代表用户502作出的。如果请求504是仅代表用户502作出的,则例程600从操作604前进到操作610。

[0054] 在操作610,资源服务器114利用许可数据存储120来确定作出该请求的用户502是否具有足够的特权来执行在所接收的资源请求504中请求的动作。如果用户502不具有足够的特权,则例程600从操作612前进到操作614,在操作614拒绝所接收的资源请求504。例程600然后从操作614前进至操作620,在操作620例程600结束。

[0055] 如果用户502具有足够的特权,则例程600从操作612前进到操作616,在操作616执行在所接收的资源请求504中请求的动作。例如,可以在安全资源122上执行读操作、写操作或另一种类型的操作。一旦完成了该动作,例程600前进到操作618,在操作618,资源服务器114将把所执行的动作归因于用户502的数据存储于历史数据存储508中。例如,可以存储指示用户502在安全资源122上执行了写操作的数据。从操作618,例程600前进至操作620,在操作602例程600结束。

[0056] 如果在操作604资源服务器114确定所接收的资源请求504不是仅由用户502作出

的,则例程600前进到操作606。在操作606,资源服务器114确定所接收的资源请求504是否是由应用140代表用户502作出的。如果所接收的资源请求504是由应用140代表用户502作出的,则例程600从操作606前进到操作622。

[0057] 在操作622,资源服务器114利用许可数据存储120来确定是否应用104和用户502两者都具有足够的特权来执行在所接收的资源请求504中请求的动作。如果应用104或用户502任一不具有足够的特权,则例程600从操作624前进到操作614,在操作614拒绝所接收的资源请求504。例程600然后从操作614继续至操作620,在操作620例程500结束。

[0058] 如果应用104和用户502两者都具有足够的特权,则例程600从操作624前进到操作626,在操作626执行在所接收的资源请求504中请求的动作。一旦完成了该动作,例程600前进到操作628,在操作628,资源服务器114将把所执行的动作归因于应用104和用户502两者的数据存储,在历史数据存储508中。例如,可以存储指示应用104代表用户502在安全资源122上执行了删除操作的数据。从操作628,例程600前进到操作620,在操作620例程600结束。

[0059] 如果在操作606资源服务器114确定所接收的资源请求不是代表用户502和应用104两者作出的,则例程600从操作606前进到操作608。在操作608,资源服务器114确定所接收的资源请求504是否是仅代表应用104作出的。如果所接收的资源请求504不是仅代表应用104作出的,则例程600从操作608前进到操作614,在操作614拒绝所接收的资源请求504。例程600然后从操作614继续至操作620,在操作620例程600结束。

[0060] 如果资源服务器114确定所接收的资源请求504是仅代表应用104作出的,则例程600从操作608前进到操作630(如图6B所示)。在操作630,资源服务器114利用许可数据存储120来确定应用104是否具有足够的特权来执行在所接收的资源请求504中请求的动作。如果应用104不具有足够的特权,则例程600从操作632前进到操作634,在操作634拒绝所接收的资源请求504。例程600然后从操作634前进到操作640,在操作640例程600结束。

[0061] 如果应用104具有足够的特权,则例程600从操作632前进到操作636,在操作636执行在所接收的资源请求504中请求的动作。一旦完成了该动作,例程600前进到操作638,在操作638,资源服务器114将把所执行的动作仅归因于应用104的数据存储在历史数据存储508中。从操作638,例程600前进至操作640,在操作640例程600结束。

[0062] 图7是示出用于能够实现本文所提出的各种实施例的计算系统的说明性计算机硬件和软件体系结构的计算机体系结构图。图7示出的计算机体系结构示出了传统台式计算机、膝上计算机,或服务器计算机,并可被用来执行以上描述的用于提供此处公开的功能的各种软件组件。

[0063] 图7所示的计算机体系结构包括中央处理单元702(“CPU”)、包括随机存取存储器714(“RAM”)和只读存储器(“ROM”)716的系统存储器708、以及将存储器耦合至CPU 702的系统总线704。包含诸如在启动期间有助于在计算机700内的元件之间传输信息的基本例程的基本输入/输出系统(“BIOS”)被存储在ROM 716中。计算机700还包括用于存储操作系统718、应用程序和其他程序模块的大容量存储设备710,这将在以下更为详细地描述。

[0064] 大容量存储设备710通过连接到总线704的大容量存储控制器(未示出)连接到CPU 702。大容量存储设备710及其相关联的计算机可读存储介质为计算机700提供非易失性的存储。虽然对此处包含的计算机可读介质的描述引用了诸如硬盘或CD-ROM驱动器等大容量

存储设备,但本领域的技术人员应当理解,计算机可读介质可以是可由计算机700访问的任何可用计算机存储介质。

[0065] 作为示例而非限制,计算机可读存储介质可包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据的信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。例如,计算机可读存储介质包括,但并不限于,RAM、ROM、EPROM、EEPROM、闪存或其他固态存储器技术,CD-ROM、数字多功能盘(“DVD”)、HD-DVD、蓝光或其他光学存储,磁带盒、磁带、磁盘存储器或其他磁存储设备,或可以用来存储所需信息并可由计算机700访问的任何其他非易失性介质。

[0066] 可以理解,此处公开的计算机可读介质也包括通信介质。通信介质通常以诸如载波或其他传输机制等已调制数据信号来体现计算机可读指令、数据结构、程序模块或其他数据,并包括任意信息传送介质。术语“已调制数据信号”指其一个或多个特征以这样的方式设置或改变以便在信号中对信息进行编码的信号。作为示例而非限制,通信介质包括有线介质(如有线网络或直接连线连接)以及无线介质(如声学、射频、红外和其它无线介质)。上述中任一组合也应包括在计算机可读介质的范围之内。计算机可读存储介质不包括通信介质。

[0067] 根据各实施例,计算机700可以使用通过诸如网络720之类的网络到远程计算机的逻辑连接来在联网环境中操作。计算机700可以通过连接至总线704的网络接口单元706来连接到网络720。应当理解,网络接口单元706还可以被用来连接到其他类型的网络和远程计算机系统。计算机700还可以包括用于接收和处理来自多个其他设备的输入/输出控制器712,这些设备包括键盘、鼠标或者电子指示笔(未在图7中示出)。类似地,输入/输出控制器可以提供至显示屏、打印机或其他类型的输出设备(也未在图7中示出)的输出。

[0068] 如前简述的那样,多个程序模块和数据文件可以存储在计算机700的大容量存储设备710和RAM 714内,包括适于控制联网的台式计算机、膝上型计算机或服务器计算机的操作的操作系统704。大容量存储设备710和RAM 714还可以存储一个或多个程序模块。具体地,大容量存储设备710和RAM 714可以存储用于提供以上描述的功能的一个或多个软件组件,诸如应用104或资源服务器114、或者另一类型的程序或服务。大容量存储设备710和RAM 714还可存储在此公开的其他程序模块和数据。

[0069] 一般而言,软件应用或模块在被加载到CPU 702中并被执行时,可将CPU702和整个计算机700从通用计算系统变换成被定制成执行此处呈现的功能的专用计算系统。CPU 702可由任意数量的晶体管或其他分立电路元件(它们可单独地或共同地呈现任意数量的状态)构建。更具体地说,CPU 702可以响应软件或模块内包含的可执行指令,作为一个或多个有限状态机来操作。这些计算机可执行指令可以通过指定CPU 702如何在多个状态之间转换来转换CPU702,从而在物理上转换构成CPU 702的晶体管或其他分立的硬件元件。

[0070] 将软件或模块编码在大容量存储设备上还可变换大容量存储设备或相关联的计算机可读存储介质的物理结构。在本说明书的不同实现中,物理结构的具体变换可取决于各种因素。这些因素的示例包括但不限于:用来实现计算机可读存储介质的技术、计算机可读存储介质被表征为主存储还是次级存储等等。例如,如果计算机可读存储介质是按照基于半导体的存储器实现的,则当软件被编码到其中时,软件或模块可以转换半导体存储器的物理状态。例如,软件可以转换构成半导体存储器的晶体管、电容器或其他分立的电路元

件的状态。

[0071] 作为另一个示例,计算机可读存储介质可以使用磁性或光学技术来实现。在这样的实现方式中,当软件被编码到磁性或光学介质中时,软件或模块可以转换磁性或光学介质的物理状态。这些变换可包括更改给定磁性介质内的特定位置的磁性特征。这些变换还可以包括改变给定光学介质内的特定位置的物理特征或特性,以改变这些位置的光学特性。在不背离本说明书的范围和精神的情况下,物理介质的其他变换也是可能的,其中所提供的上述示例只是便于该讨论。

[0072] 基于前述内容,应当理解,在此公开了用于授权应用对安全资源的访问的技术。虽然以计算机结构特征、方法动作、以及计算机可读介质专用的语言描述了本文提出的主题,但是应该理解,在所附权利要求书中所限定的本发明不一定限于本文描述的具体特征、动作、或介质。相反,这些具体特征、动作、以及介质是作为实现权利要求的示例形式而公开的。

[0073] 以上所述的主题仅作为说明提供,并且不应被解释为限制。可对本文中所描述的主题作出各种修改和改变,而不必遵循示出和描述的示例实施例和应用且不背离所附权利要求书中所阐述的本发明的真正精神和范围。

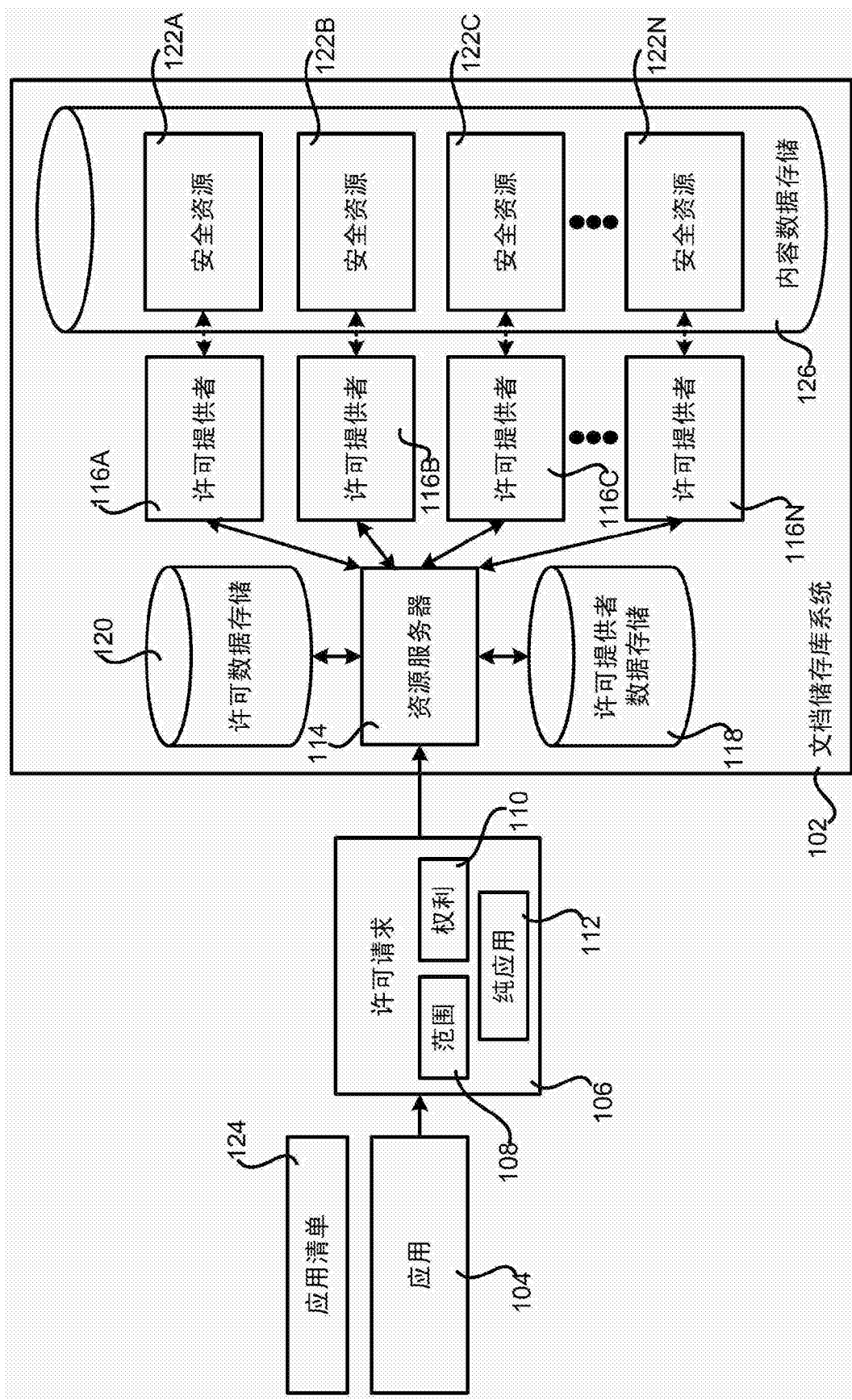


图1

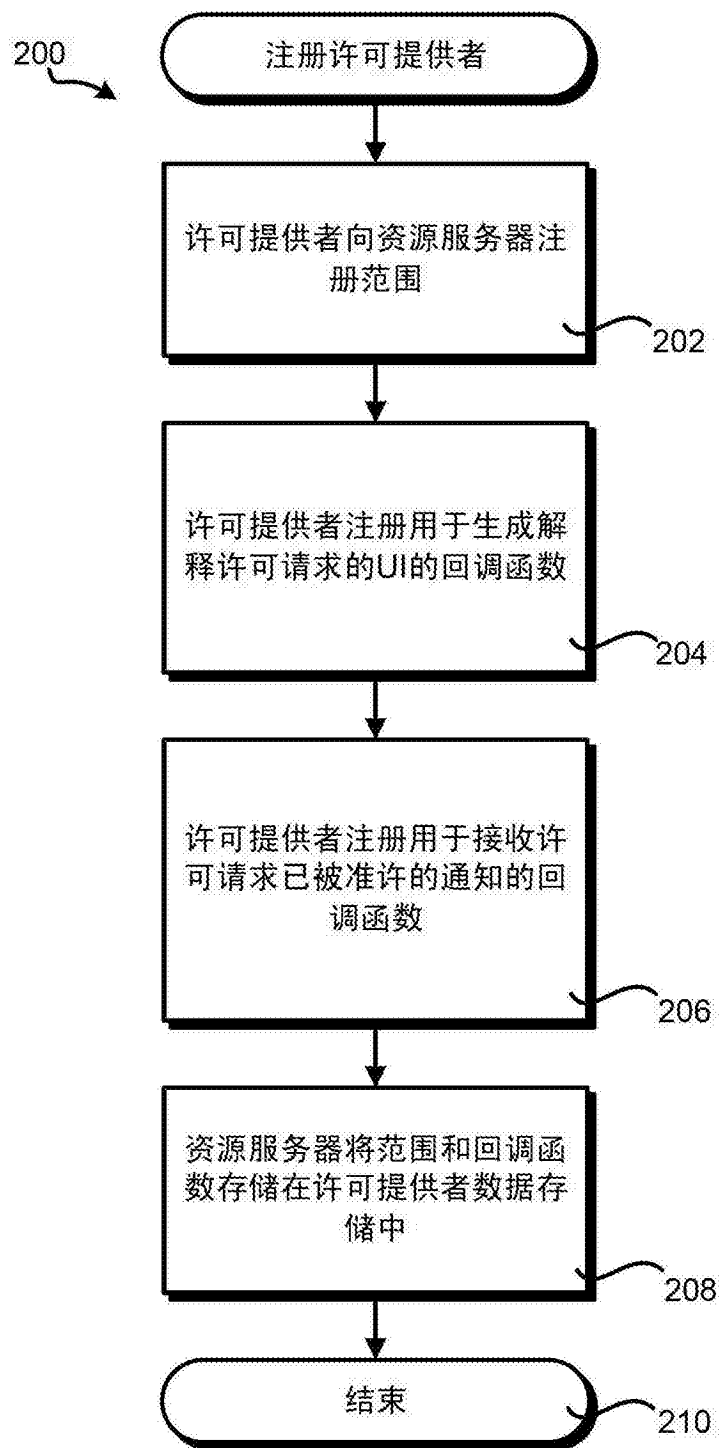


图2

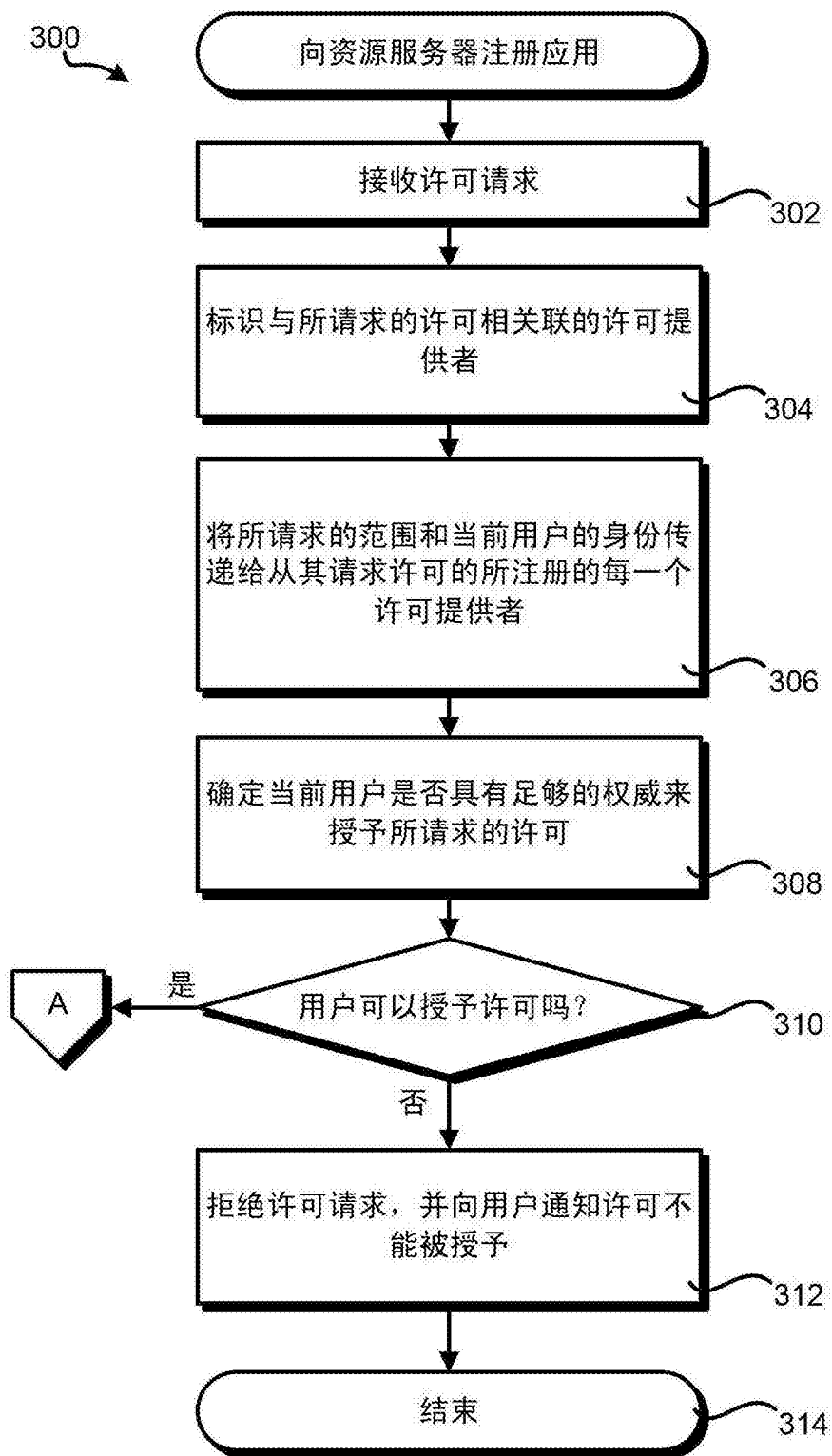


图3A

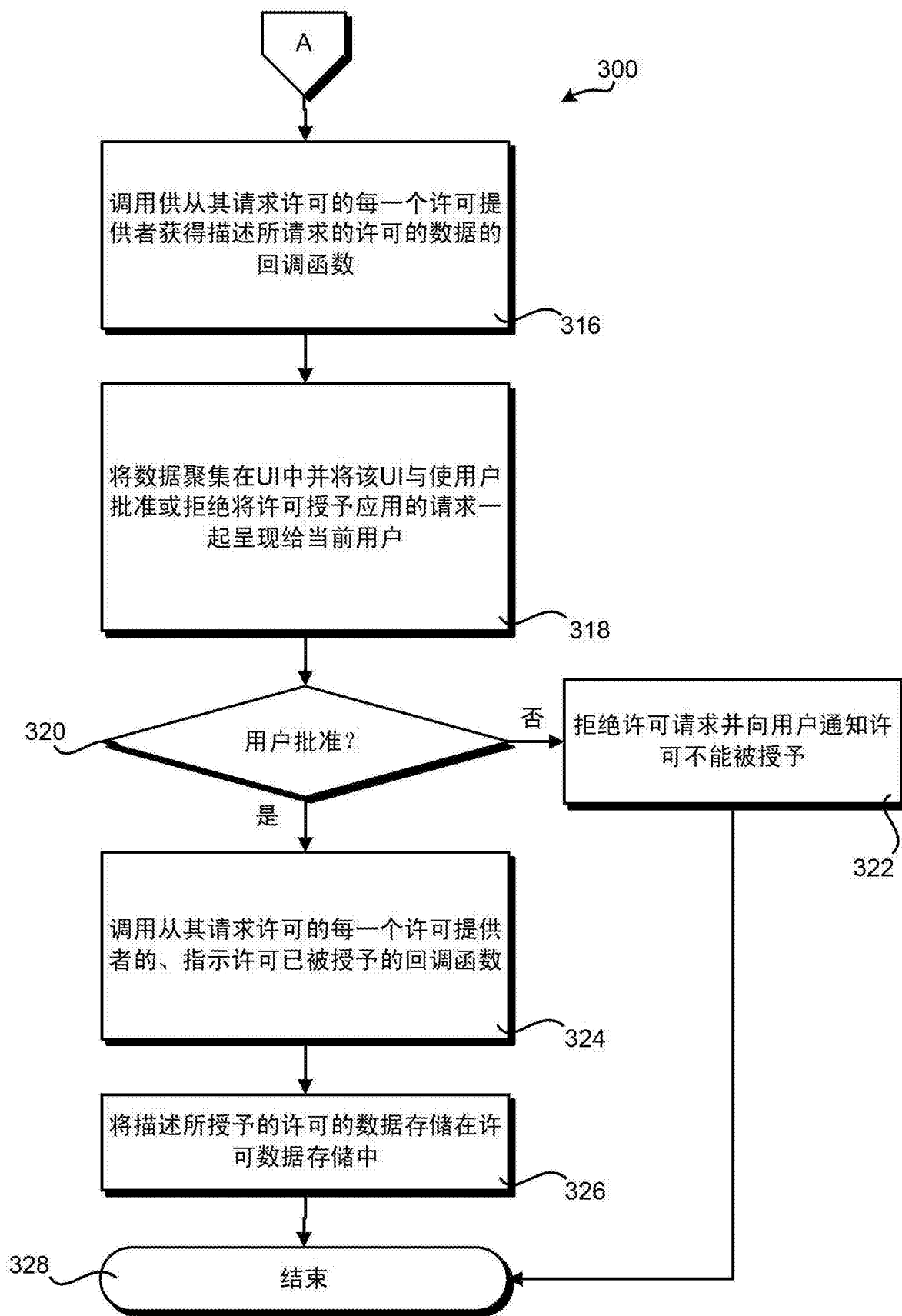


图3B

106

```
<App ...>
...
<AppPermissionRequests>
  <AppPermissionRequest Scope="http://
sharepoint/content/sitecollection/web/list"
Right="Write">
    <Property Name="BaseTemplateId"
Value="101"/>
  </AppPermissionRequest>
  <AppPermissionRequest Scope="http://
sharepoint/userprofilestore"/>
  <AppPermissionRequest Scope="http://
exchange/calendars" Right="Read"/>
  <AppPermissionRequest Scope="http://
lync/contacts" Right="Read"/>
</AppPermissionRequests>
...
</App>
```

许可请求

图4A

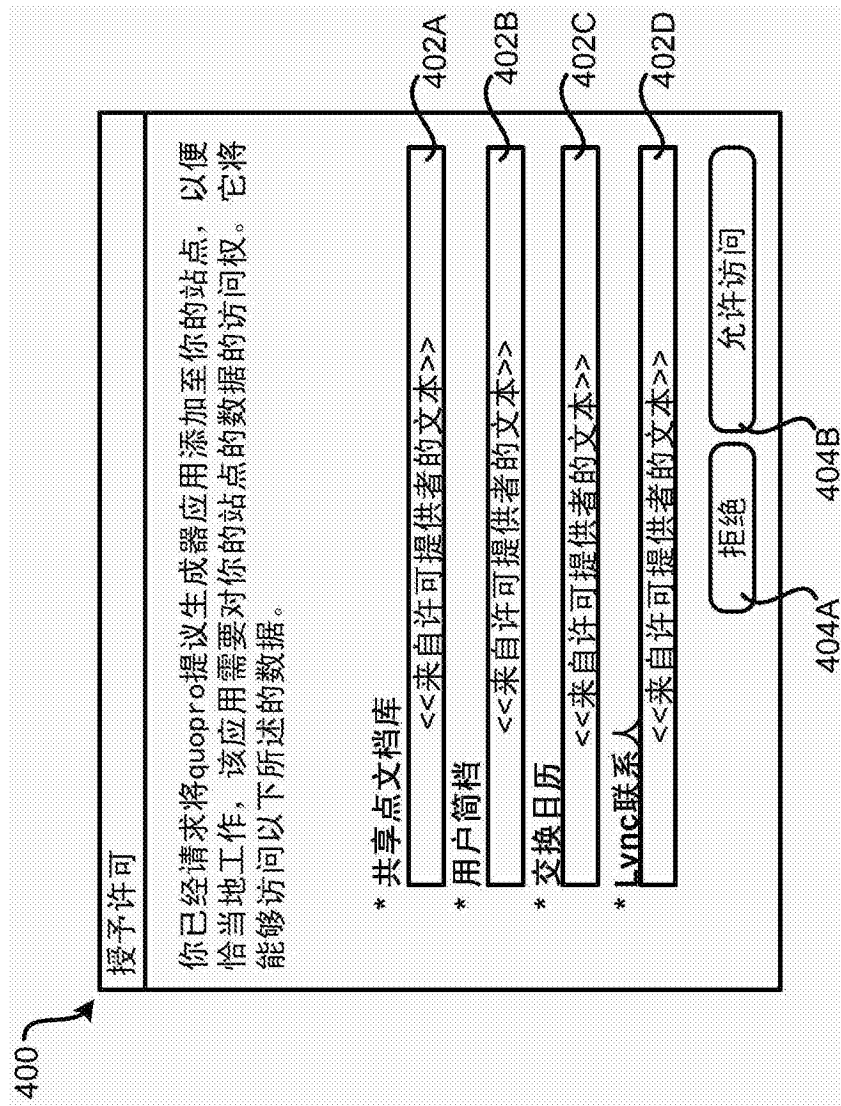


图4B

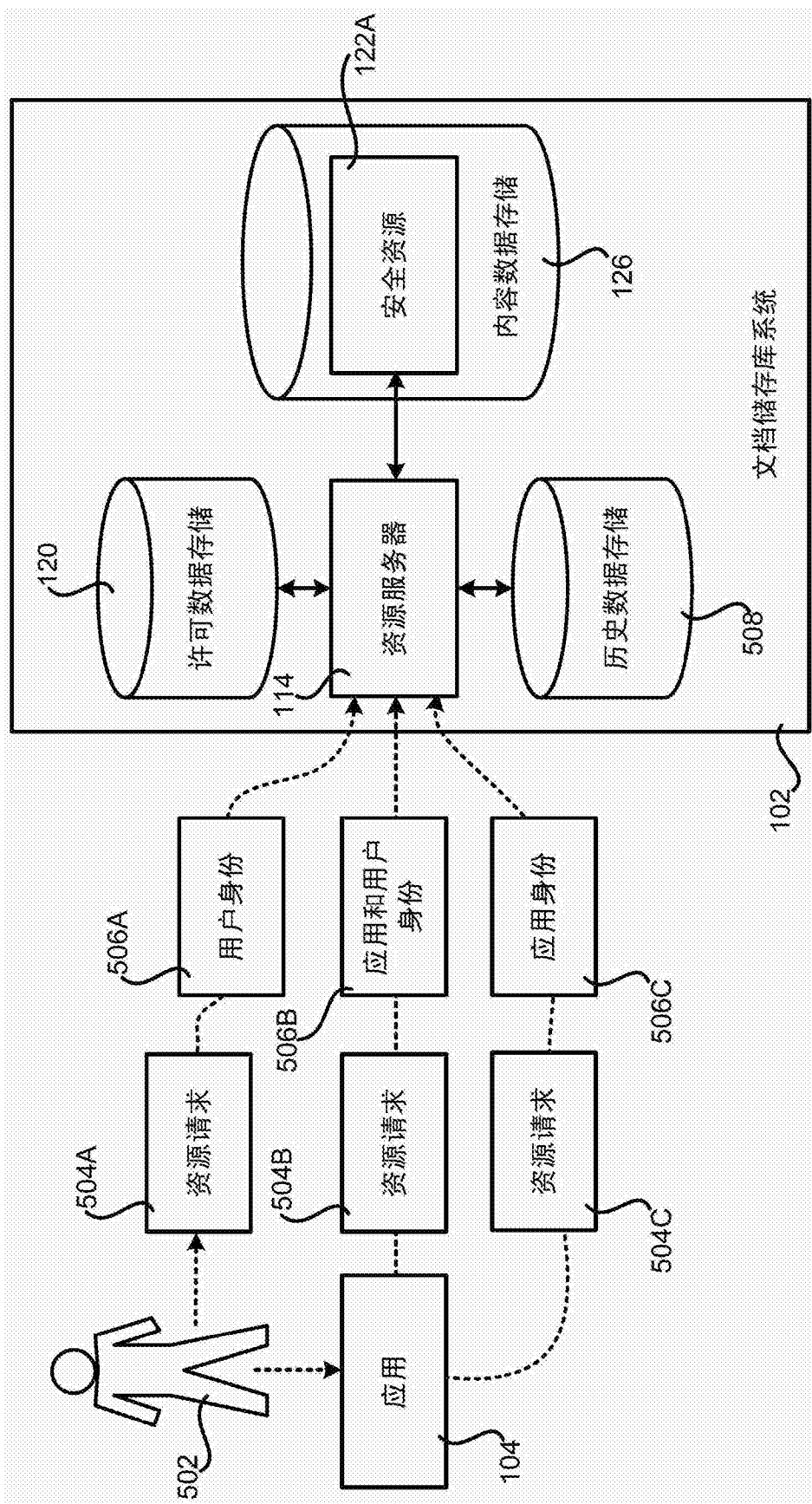


图5

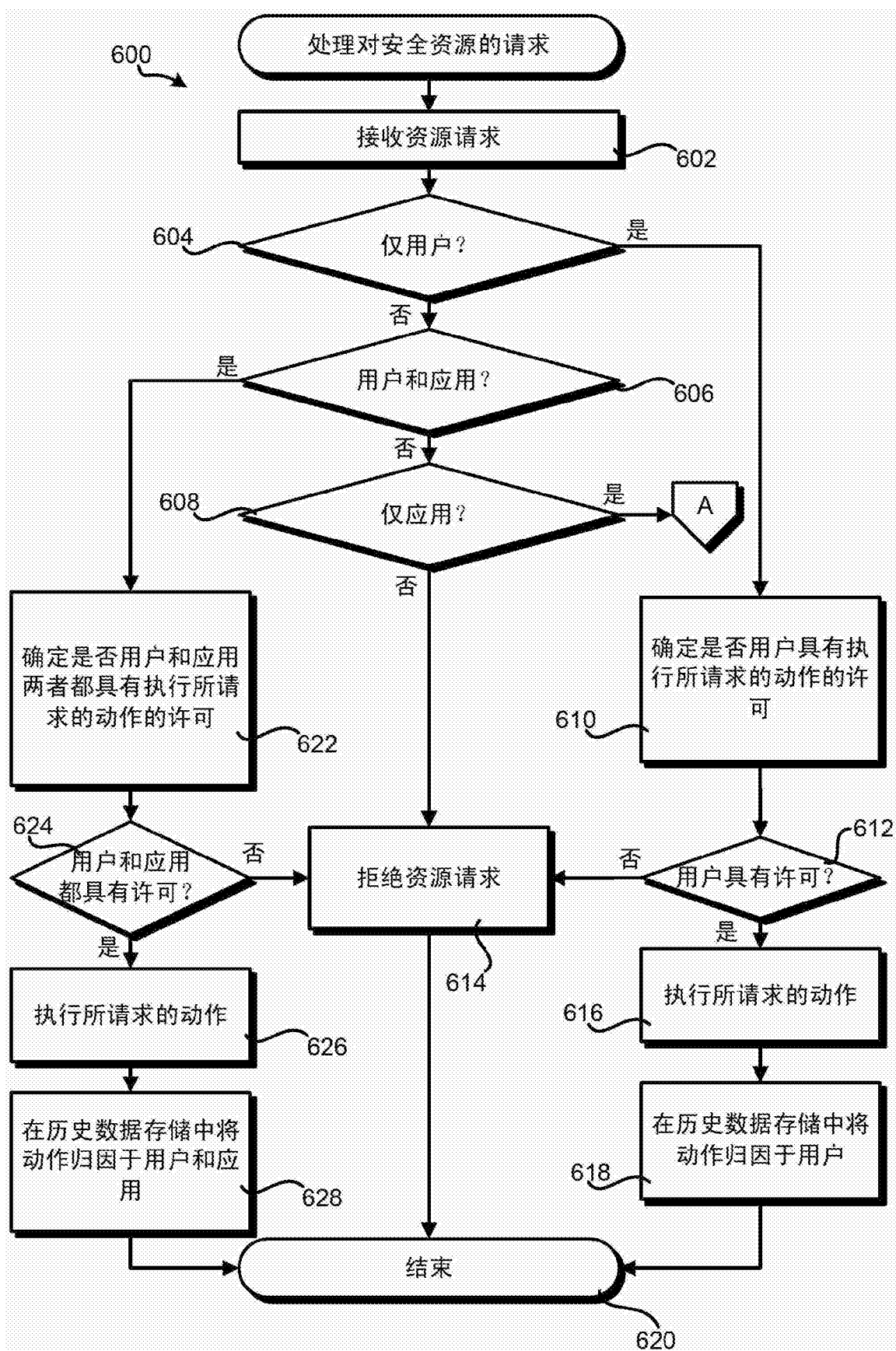


图6A

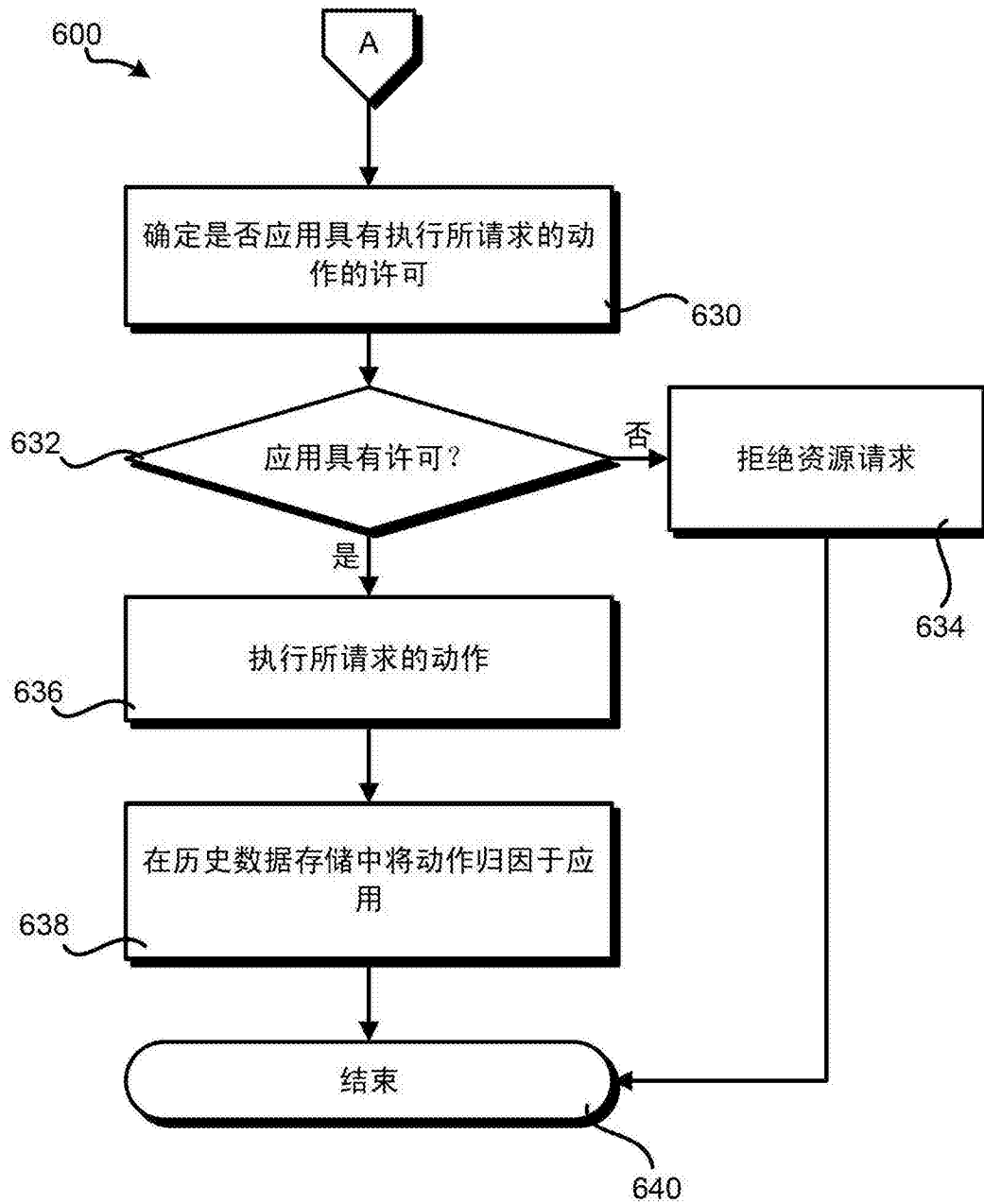


图6B

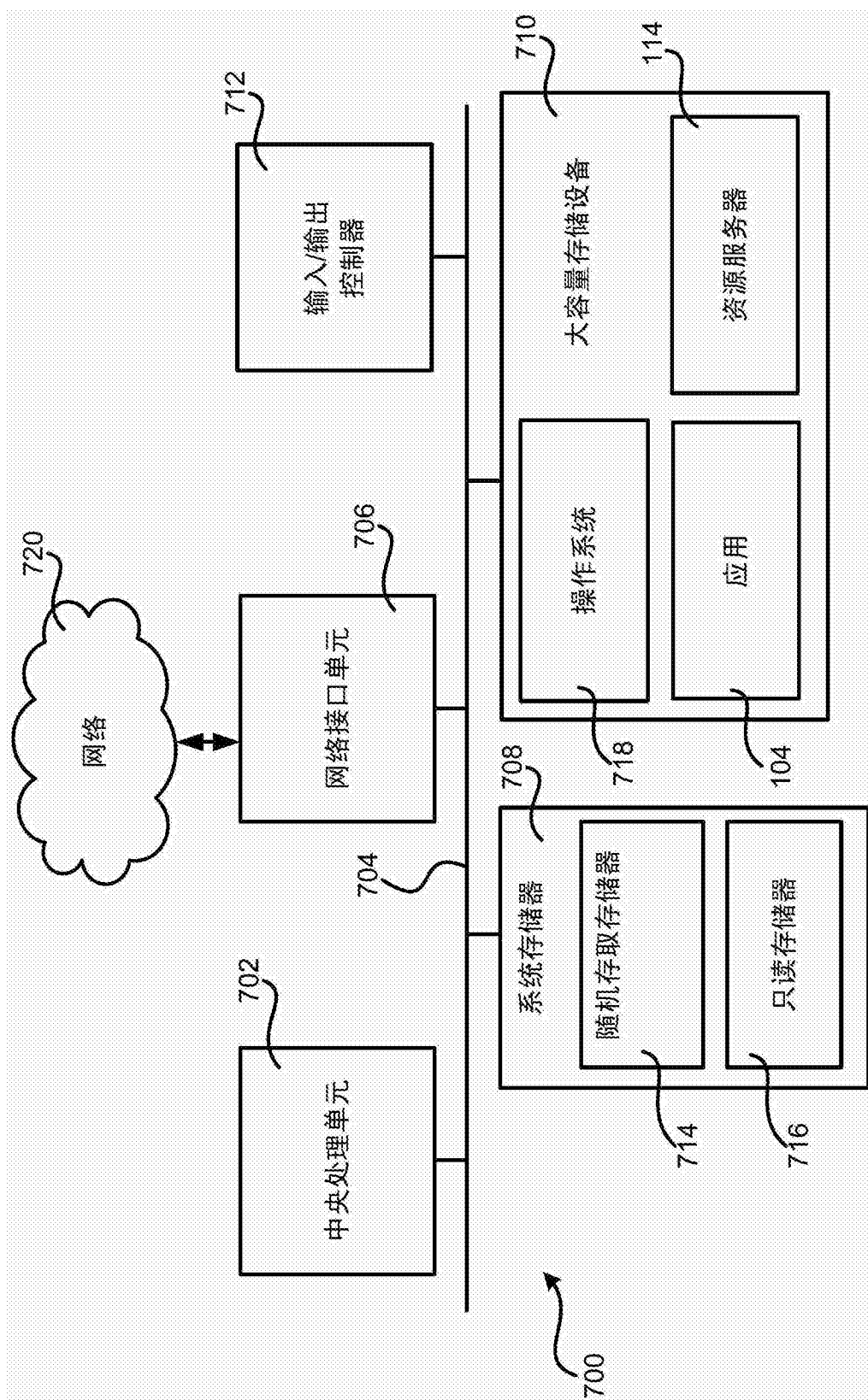


图7