



(12)发明专利申请

(10)申请公布号 CN 107204843 A

(43)申请公布日 2017.09.26

(21)申请号 201710233046.1

(22)申请日 2017.04.11

(71)申请人 北京奇艺世纪科技有限公司

地址 100080 北京市海淀区北一街2号爱奇艺创新大厦10、11层

(72)发明人 吴岩 翁迟迟 丁浩

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319

代理人 苏培华

(51) Int. Cl.

H04L 9/08(2006.01)

G06Q 10/06(2012.01)

G06Q 10/10(2012.01)

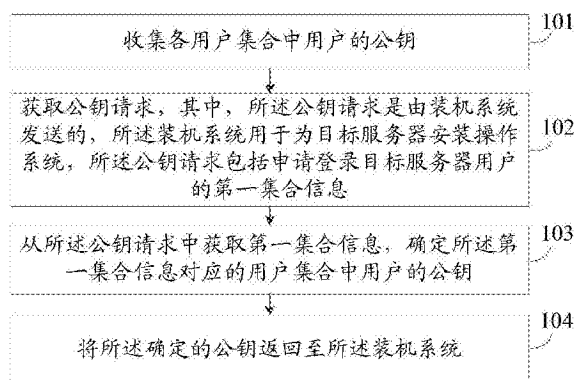
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种公钥处理方法和装置

(57)摘要

本发明实施例提供了一种公钥处理方法和装置,其中,所述的方法包括:收集各用户集合中用户的公钥,其中,每个用户集合至少包括一个用户,每个用户对应一个公钥;获取公钥请求,其中,所述公钥请求是由装机系统发送的,所述装机系统用于为目标服务器安装操作系统,所述公钥请求包括申请登录目标服务器用户的第一集合信息;从所述公钥请求中获取第一集合信息,确定所述第一集合信息对应的用户集合中用户的公钥;将所述确定的公钥返回至所述装机系统,以使所述装机系统将所述确定的公钥存储在所述目标服务器中;从而提高了收集需要登录目标服务器用户的公钥的效率。



1. 一种公钥处理方法,其特征在于,包括:

收集各用户集合中用户的公钥,其中,每个用户集合至少包括一个用户,每个用户对应一个公钥;

获取公钥请求,其中,所述公钥请求是由装机系统发送的,所述装机系统用于为目标服务器安装操作系统,所述公钥请求包括申请登录目标服务器用户的第一集合信息;

从所述公钥请求中获取第一集合信息,确定所述第一集合信息对应的用户集合中用户的公钥;

将所述确定的公钥返回至所述装机系统,以使所述装机系统将所述确定的公钥存储在所述目标服务器中。

2. 根据权利要求1所述的方法,其特征在于,在确定所述第一集合信息对应的用户集合中用户的公钥的步骤之前,还包括:

获取所述第一集合信息对应用户集合的权限信息;

依据所述权限信息确定所述用户集合是否具有登录目标服务器的权限;

如果所述用户集合具有登录目标服务器的权限,执行确定所述第一集合信息对应的用户集合中用户的公钥的步骤。

3. 根据权利要求1所述的方法,其特征在于,收集各用户集合中用户的公钥的步骤,包括:

获取用户的公钥;

从轻量目录访问协议系统中,查询所述获取的公钥对应的管理信息,所述管理信息包括第二集合信息和权限信息;

依据所述管理信息将所述获取的公钥添加至对应的用户集合中。

4. 根据权利要求3所述的方法,其特征在于,依据所述管理信息将所述获取的公钥添加至对应的用户集合中的步骤,包括:

从所述管理信息中获取第二集合信息,确定所述获取的公钥对应的用户集合;

判断是否已经创建所述获取的公钥对应的用户集合;

若已创建所述获取的公钥对应的用户集合,则将所述获取的公钥添加至对应的用户集合中;

若未创建所述获取的公钥对应的用户集合,则在公钥管理系统中建立所述获取的公钥对应的用户集合,并为所述获取的公钥对应的用户集合配置对应的权限信息;以及将所述获取的公钥添加至对应的用户集合中。

5. 根据权利要求1所述的方法,其特征在于,还包括:

接收轻量目录访问协议系统发送的更新信息,并依据所述更新信息更新对应的用户集合。

6. 一种公钥处理装置,其特征在于,包括:

收集模块,用于收集各用户集合中用户的公钥,其中,每个用户集合至少包括一个用户,每个用户对应一个公钥;

请求获取模块,用于获取公钥请求,其中,所述公钥请求是由装机系统发送的,所述装机系统用于为目标服务器安装操作系统,所述公钥请求包括申请登录目标服务器用户的第一集合信息;

确定模块,用于从所述公钥请求中获取第一集合信息,确定所述第一集合信息对应的用户集合中用户的公钥;

返回模块,用于将所述确定的公钥返回至所述装机系统,以使所述装机系统将所述确定的公钥存储在所述目标服务器中。

7. 根据权利要求6所述的装置,其特征在于,

所述确定模块,还用于在确定所述第一集合信息对应的用户集合中用户的公钥之前,获取所述第一集合信息对应用户集合的权限信息;依据所述权限信息确定所述用户集合是否具有登录目标服务器的权限;如果所述用户集合具有登录目标服务器的权限,确定所述第一集合信息对应的用户集合中用户的公钥。

8. 根据权利要求6所述的装置,其特征在于,所述收集模块包括:

公钥获取子模块,用于获取用户的公钥;

查询子模块,用于从轻量目录访问协议LDAP系统中,查询所述获取的公钥对应的管理信息,所述管理信息包括第二集合信息和权限信息;

添加子模块,用于依据所述管理信息将所述获取的公钥添加至对应的用户集合中。

9. 根据权利要求8所述的装置,其特征在于,

所述添加子模块,具体用于从所述管理信息中获取第二集合信息,确定所述获取的公钥对应的用户集合;判断是否已经创建所述获取的公钥对应的用户集合;若已创建所述获取的公钥对应的用户集合,则将所述获取的公钥添加至对应的用户集合中;若未创建所述获取的公钥对应的用户集合,则在公钥管理系统中建立所述获取的公钥对应的用户集合,并为所述获取的公钥对应的用户集合配置对应的权限信息;以及将所述获取的公钥添加至对应的用户集合中。

10. 根据权利要求6所述的装置,其特征在于,还包括:

更新模块,用于接收轻量目录访问协议系统发送的更新信息,并依据所述更新信息更新对应的用户集合。

一种公钥处理方法和装置

技术领域

[0001] 本发明涉及数据处理技术领域,特别是涉及一种公钥处理方法和装置。

背景技术

[0002] 随着互联网技术的不断发展,互联网公司也在不断增加和扩大。大多数大型的互联网公司为了提高用户的体验,会高频率的购买服务器并投入使用。

[0003] 在为服务器安装系统之前,装机人员需要人工收集需要登录此服务器的员工的公钥,然后将收集的公钥上传至服务器中。从而在服务器投入使用后,公钥保存在此服务器中的员工可以通过安全外壳协议(Secure Shell,ssh)的方式登录此服务器。但人工收集需要登录此服务器员工的公钥的方法效率低。

发明内容

[0004] 本发明实施例所要解决的技术问题是提供一种公钥处理方法,以解决现有技术中人工收集需要登录服务器用户的公钥效率低的问题。

[0005] 相应的,本发明实施例还提供了一种公钥处理装置,用以保证上述方法的实现及应用。

[0006] 为了解决上述问题,本发明公开了一种公钥处理方法,具体包括:收集各用户集合中用户的公钥,其中,每个用户集合至少包括一个用户,每个用户对应一个公钥;获取公钥请求,其中,所述公钥请求是由装机系统发送的,所述装机系统用于为目标服务器安装操作系统,所述公钥请求包括申请登录目标服务器用户的第一集合信息;从所述公钥请求中获取第一集合信息,确定所述第一集合信息对应的用户集合中用户的公钥;将所述确定的公钥返回至所述装机系统,以使所述装机系统将所述确定的公钥存储在所述目标服务器中。

[0007] 本发明还公开了一种公钥处理装置,具体包括:收集模块,用于收集各用户集合中用户的公钥,其中,每个用户集合至少包括一个用户,每个用户对应一个公钥;请求获取模块,用于获取公钥请求,其中,所述公钥请求是由装机系统发送的,所述装机系统用于为目标服务器安装操作系统,所述公钥请求包括申请登录目标服务器用户的第一集合信息;确定模块,用于从所述公钥请求中获取第一集合信息,确定所述第一集合信息对应的用户集合中用户的公钥;返回模块,用于将所述确定的公钥返回至所述装机系统,以使所述装机系统将所述确定的公钥存储在所述目标服务器中。

[0008] 与现有技术相比,本发明实施例包括以下优点:

[0009] 本发明实施例由公钥管理系统收集各用户集合中用户的公钥,在收集各用户集合公钥后,接收装机系统发送的公钥请求,所述公钥请求是由装机系统发送的,所述装机系统用于为目标服务器安装操作系统,所述公钥请求包括申请登录目标服务器用户的第一集合信息;进而,公钥管理系统可以将所述第一集合信息对应的用户集合中用户的公钥返回至所述装机系统,使得装机系统将所述确定的公钥存储在所述目标服务器中;从而提高了收集需要登录目标服务器用户的公钥的效率。

附图说明

- [0010] 图1是本发明的一种公钥处理方法实施例的步骤流程图；
- [0011] 图2是本发明的一种公钥管理系统、LDAP系统和装机系统关系示意图；
- [0012] 图3是本发明的另一种公钥处理方法实施例的步骤流程图；
- [0013] 图4是本发明的一种公钥处理装置实施例的结构框图；
- [0014] 图5是本发明的另一种公钥处理装置实施例的结构框图。

具体实施方式

[0015] 为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0016] 本发明实施例的构思之一是，公钥管理系统首先按照用户集合收集用户的公钥；在接收到装机系统在为目标服务器安装系统操作系统过程中，发送的公钥请求时，将对应用户的公钥发送至装机系统，从而装机系统可以在安装操作系统的过程中存储对应的公钥，提高了收集用户的公钥的效率。

[0017] 实施例一

[0018] 参照图1，示出了本发明的一种公钥处理方法实施例的步骤流程图，具体可以包括如下步骤：

[0019] 步骤101、收集各用户集合中用户的公钥。

[0020] 本发明实施例提供一种公钥处理方法，应用在公钥管理系统中，为装机系统在为目标服务器安装操作系统的过程中，提供申请登录目标服务器用户对应的公钥，其中，所述公钥管理系统用于存储和管理各用户集合用户的公钥，所述目标服务器是需要安装操作系统的服务器，所述装机系统用于为目标服务器安装操作系统。每个公司包括多个部门，如流程部、开发部等等，每个部门包括至少一个员工，每个员工对应一个公钥；因此，可以按照部门进行分组，一个组即对应一个用户集合，各部门包含的员工即为对应用户集合中的用户。公司在为每个员工分配公钥后，公钥管理系统可以收集各员工的公钥，然后按照公钥的特征信息，将公钥存储在对应的用户集合中，其中，各用户集合中至少包括一个用户的公钥，公钥管理系统中每个用户一个公钥，每个用户的公钥均不同。例如，公司包括流程部、开发部、测试部、运维部四个部门，每个部门分别包括的员工有20、40、50、10个；则公钥管理系统中的用户集合包括流程部集合、开发部集合、测试部集合和运维部集合，每个用户集合分别包括20、40、50、10个用户的公钥。

[0021] 步骤102、获取公钥请求，其中，所述公钥请求是由装机系统发送的，所述装机系统用于为目标服务器安装操作系统，所述公钥请求包括申请登录目标服务器用户的第一集合信息。

[0022] 本发明实施例中，在装机系统为目标服务器按照操作系统之前，登录目标服务器的用户如运维人员，可向装机系统提交登录目标服务器的申请，用户在提交申请中可以只填写用户所在用户集合对应的第一集合信息，而无需填写用户的公钥，操作便捷。装机系统为目标服务器安装操作系统的过程中，可以提取用户提交申请中的第一集合信息，然后生成对应的公钥请求并发送至公钥管理系统，其中，所述公钥请求中包括申请登录目标服务

器用户的第一集合信息;公钥管理系统获取装机系统发送的公钥请求。

[0023] 步骤103、从所述公钥请求中获取第一集合信息,确定所述第一集合信息对应的用户集合中用户的公钥。

[0024] 步骤104、将所述确定的公钥返回至所述装机系统。

[0025] 公钥管理系统在获取公钥请求后,可以将公钥请求中第一集合信息对应的公钥返回至装机系统;具体的,公钥管理系统从公钥请求中获取对应的第一集合信息,然后确定公钥管理系统中与该第一集合信息对应的用户集合;再确定该用户集合中对应所有用户的公钥,从而将确定的公钥返回至装机系统。装机系统接收公钥后,在为目标服务器安装操作系统的过程中,将接收的公钥存储在目标服务器中,从而在目标服务器安装操作系统后,申请登录目标服务器的用户,可以在对应的终端上通过ssh方式登录目标服务器。例如,运维部门的员工张三,向装机系统提交申请,张三在提交的申请中只需填写第一集合信息如运维部门;公钥管理系统从公钥请求中获取运维部门后,确定对应的用户集合为运维部集合,其中,运维部集合包括12个用户的公钥,公钥管理系统将运维部集合中12个用户公钥全部返回至装机系统。装机系统在安装系统的过程中,将这12个用户的公钥存储在目标服务器上,张三可以通过对应的终端登录目标服务器,对目标服务器进行运维。当然其他11个用户的公钥对应的用户,也可以通过对应的终端登录目标服务器。

[0026] 本发明实施例由公钥管理系统收集各用户集合中用户的公钥,在收集各用户集合公钥后,接收装机系统发送的公钥请求,所述公钥请求是由装机系统发送的,所述装机系统用于为目标服务器安装操作系统,所述公钥请求包括申请登录目标服务器用户的第一集合信息;进而,公钥管理系统可以将所述第一集合信息对应的用户集合中用户的公钥返回至所述装机系统,使得装机系统将所述确定的公钥存储在所述目标服务器中;从而提高了收集需要登录目标服务器用户的公钥的效率。

[0027] 实施例二

[0028] 本发明实施例中,公钥管理系统可从轻量目录访问协议(Lightweight Directory Access Protocol,LDAP)系统中获取管理信息,然后依据管理信息存储各用户集合中用户的公钥;在获取公钥请求后,将具有权限的用户集合中用户的公钥返回至装机系统;其中,公钥管理系统、LDAP系统和装机系统的关系如图2所示。公钥管理系统具体收集公钥和返回公钥的方法可参照图3。图3示出了本发明的一种公钥管理方法实施例的步骤流程图,具体可以包括如下步骤:

[0029] 步骤301、获取用户的公钥。

[0030] 步骤302、从轻量目录访问协议LDAP系统中,查询所述获取的公钥对应的管理信息,所述管理信息包括第二集合信息和权限信息。

[0031] 公钥管理系统收集各用户集合中用户的公钥的过程,是将获取的各用户的公钥保存在各用户集合的过程,其中,公钥管理系统根据LDAP系统中各用户的公钥对应的管理信息,存储用户的公钥。本发明实施例中LDAP系统用于存储用户管理信息,所述管理信息包括第二集合信息和权限信息,所述权限信息对应的权限包括登录目标服务器的权限。任一用户分配一个公钥后,可以在公钥管理系统中直接录入对应的公钥,也可以是由LDAP系统向公钥管理系统发送添加公钥的指令;从而公钥管理系统可以根据录入操作,或LDAP系统发送的指令中获取需要存储的公钥。公钥管理系统在将获取的公钥存储在对应用户集合时,

可以向LDAP系统发送查询请求,以查询该需要存储的公钥对应的管理信息。LDAP系统接收到公钥管理系统的查询请求后,将查询请求中公钥对应的管理信息返回至公钥管理系统,进而,公钥管理系统根据查询的管理信息将需要存储的公钥,添加至对应的用户集合中,具体步骤如下:

[0032] 步骤303、判断是否已经创建所述获取的公钥对应的用户集合;若是,则执行步骤304;若否,则执行步骤305。

[0033] 公钥管理系统可以从管理系统中获取第二集合信息,确定获取的公钥所属的用户集合;再判断公钥管理系统中是否已创建对应的用户集合,若已创建所述获取的公钥对应的用户集合,则执行步骤304;若未创建所述获取的公钥对应的用户集合,则执行步骤305。

[0034] 步骤304、将所述获取的公钥添加至对应的用户集合中。

[0035] 若公钥管理系统中已存在所述获取的公钥对应的用户集合,直接将获取的公钥存储在对应的用户集合中即可。

[0036] 步骤305、在公钥管理系统中建立所述获取的公钥对应的用户集合,并为所述获取的公钥对应的用户集合配置对应的权限信息;以及将所述获取的公钥添加至对应的用户集合中。

[0037] 若公钥管理系统中不存在所述获取的公钥对应的用户集合,则可以根据从管理信息中获取的第二集合信息建立对应的用户集合。本发明实施例中不同的部门具有不同的权限,可能某些部门不具有登录目标服务器的权限如流程部门、测试部门等,而某些部门具有登录目标服务器的权限如运维部门、开发部门等;只有具有登录目标服务器权限的用户集合中各用户,才能够登录目标服务器。因此,公钥管理系统在建立用户集合时,可以从管理信息中获取权限信息,并为各用户集合配置对应的权限信息,以向装机系统返回具有权限的公钥。然后再将获取的公钥存储在建立的用户集合中。

[0038] 例如,LDAP系统中包括四个用户集合:A、B、C、D,其中,A包括的成员A1-A12,B包括的成员B1-B10,C包括的成员C1-C18,D包括的成员D1-A30;A和B具有登录目标服务器的权限,C和D不具有登录目标服务器的权限。公钥管理系统中已建立用户集合A和D,当公钥管理系统获取A10的公钥时,直接将A10对应的公钥存储在A用户集合中;当获取B1时,在公钥管理系统中建立B集合,再配置B集合的权限信息为登录目标服务器的权限,然后将B1对应的公钥存储在B集合中。

[0039] 步骤306、获取公钥请求。

[0040] 装机系统为目标服务器安装操作系统的过程中,在接收到用户提交的申请后,可以向公钥管理系统发送公钥请求,以获取用户提交的申请对应的公钥;其中,所述公钥请求可以是HTTPS请求,即装机系统向公钥管理系统的HTTPS接口发送公钥请求。公钥管理系统通过HTTPS接口获取所述公钥请求。

[0041] 步骤307、从所述公钥请求中获取第一集合信息,获取所述第一集合信息对应用户集合的权限信息。

[0042] 本发明实施例中申请登录目标服务器的用户所属的用户集合,可能是具有登录目标服务器权限的用户集合,也可能是不具有登录目标服务器权限的用户集合;为了保证目标服务器的安全,公钥管理系统在获取装机系统发送的公钥请求后,可以从所述公钥请求中获取对应的第一集合信息,对申请登录目标服务器的第一集合信息进行权限的验证,以

将具有登录目标服务器权限的用户集合中用户的公钥返回至装机系统。具体的,公钥管理系统可以根据第一集合信息确定对应的用户集合,然后获取所述第一集合信息对应用户集合的权限信息,以确定公钥请求中第一集合信息对应的用户集合是否具有登录目标服务器的权限。

[0043] 步骤308、依据所述权限信息判断所述用户集合是否具有登录目标服务器的权限;若是,则执行步骤309;若否,则执行结束的步骤。

[0044] 公钥管理系统获取用户集合对应的权限信息后,依据所述权限信息判断所述用户集合是否具有登录目标服务器的权限;当确定所述用户集合具有登录目标服务器的权限时,则执行步骤309;当确定所述用户集合不具有登录目标服务器的权限时,则执行结束的步骤。

[0045] 步骤309、确定所述第一集合信息对应的用户集合中用户的公钥。

[0046] 步骤310、将所述确定的公钥返回至所述装机系统。

[0047] 在确定公钥请求中第一集合信息对应的用户集合具有登录目标服务器的权限时,确定该用户集合中所有用户对应的公钥,再将确定的公钥返回至装机系统。装机系统在获取公钥后,在为目标服务器安装操作系统的过程中,将获取的公钥存储在目标服务器中;从而申请登录目标服务器的用户,可以登录目标服务器。

[0048] 例如,公钥管理系统中包括四个用户集合:A、B、C、D,其中,A包括A1-A12的公钥,B包括B1-B10的公钥,C包括C1-C18的公钥,D包括D1-D30的公钥;A和B具有登录目标服务器的权限,C和D不具有登录目标服务器的权限。当公钥管理系统确定公钥请求中第一集合信息对应的用户集合为B,则将B1-B10的公钥全部返回至装机系统;当公钥管理系统确定公钥请求中第一集合信息对应的用户集合为C,则不返回任一用户的公钥至装机系统。

[0049] 此外,接收LDAP系统发送的更新信息,并依据所述更新信息更新对应的用户集合。

[0050] 本发明实施例中,公钥管理系统中的用户集合和LDAP系统中的用户集合是对应的,LDAP系统中建立的用户集合更新时,如用户中用户的删除或添加,用户集合的权限的变化以及用户集合的名称的变化等等,公钥管理系统中的用户集合也需要进行对应的更新。公钥管理系统获取更新信息的具体方法包括,公钥管理系统可以按照预设周期向LDAP系统发送更新请求,进而LDAP系统向公钥管理系统发送对应的更新信息;也可以是LDAP系统中的用户集合在更新后,直接向公钥管理系统发送更新信息。公钥管理系统在接收到更新信息后,依据更新信息更加对应的用户集合。

[0051] 本发明实施例的公钥管理系统在收集各用户集合中用户的公钥过程中,在建立各用户集合时,为各用户集合配置对应的权限信息;进而在根据公钥请求的第二集合信息,将具有权限的用户集合中用户的公钥返回至装机服务器,从而保证了服务器的安全。此外,公钥管理系统可以根据接收的LDAP系统发送的更新信息,更新对应的用户集合,以保证公钥管理系统中各用户集合对应权限信息的准确性,和用户的公钥所属的用户集合的准确性。

[0052] 需要说明的是,对于方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明实施例并不受所描述的动作顺序的限制,因为依据本发明实施例,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作并不一定是本发明实施例所必须的。

[0053] 实施例三

[0054] 参照图4,示出了本发明的一种公钥处理装置实施例的结构框图,用以保证上述公钥处理方法的实施,所述装置具体包括:收集模块401、请求获取模块402、确定模块403和返回模块404,其中,

[0055] 收集模块401,用于收集各用户集合中用户的公钥,其中,每个用户集合至少包括一个用户,每个用户对应一个公钥。

[0056] 请求获取模块402,用于获取公钥请求,其中,所述公钥请求是由装机系统发送的,所述装机系统用于为目标服务器安装操作系统,所述公钥请求包括申请登录目标服务器用户的第一集合信息。

[0057] 确定模块403,用于从所述公钥请求中获取第一集合信息,确定所述第一集合信息对应的用户集合中用户的公钥。

[0058] 返回模块404,用于将所述确定的公钥返回至所述装机系统,以使装机系统将所述确定的公钥存储在所述目标服务器中。

[0059] 在本发明的另一个实施例中,针对所述装置还包括模块,以及各模块包括的子模块进行详细的说明,具体的,所述装置还包括:更新模块405,所述更新模块405,用于接收LDAP系统发送的更新信息,并依据所述更新信息更新对应的用户集合。

[0060] 本发明实施例中所述收集模块401包括:公钥获取子模块4011、查询子模块4012和添加子模块4013,其中,

[0061] 公钥获取子模块4011,用于获取用户的公钥;

[0062] 查询子模块4012,用于从轻量目录访问协议LDAP系统中,查询所述获取的公钥对应的管理信息,所述管理信息包括第二集合信息和权限信息;

[0063] 添加子模块4013,用于依据所述管理信息将所述获取的公钥添加至对应的用户集合中。

[0064] 本发明实施例中,所述确定模块403,还用于在确定所述第一集合信息对应的用户集合中用户的公钥之前,获取所述第一集合信息对应用户集合的权限信息;依据所述权限信息确定所述用户集合具有登录目标服务器的权限时,执行确定所述第一集合信息对应的用户集合中用户的公钥的步骤。

[0065] 本发明实施例由公钥管理系统收集各用户集合中用户的公钥,在收集各用户集合公钥后,接收装机系统发送的公钥请求,所述公钥请求是由装机系统发送的,所述装机系统用于为目标服务器安装操作系统,所述公钥请求包括申请登录目标服务器用户的第一集合信息;进而,公钥管理系统可以将所述第一集合信息对应的用户集合中用户的公钥返回至所述装机系统,使得装机系统将所述确定的公钥存储至所述目标服务器中;从而提高了收集需要登录目标服务器用户的公钥的效率。

[0066] 对于装置实施例而言,由于其与方法实施例基本相似,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0067] 本说明书中的各个实施例均采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似的部分互相参见即可。

[0068] 本领域内的技术人员应明白,本发明实施例的实施例可提供为方法、装置、或计算机程序产品。因此,本发明实施例可采用完全硬件实施例、完全软件实施例、或结合软件和

硬件方面的实施例的形式。而且,本发明实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0069] 本发明实施例是参照根据本发明实施例的方法、终端设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0070] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0071] 这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上,使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0072] 尽管已描述了本发明实施例的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例做出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本发明实施例范围的所有变更和修改。

[0073] 最后,还需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

[0074] 以上对本发明所提供的一种公钥设置方法和一种公钥设置装置,进行了详细介绍,本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

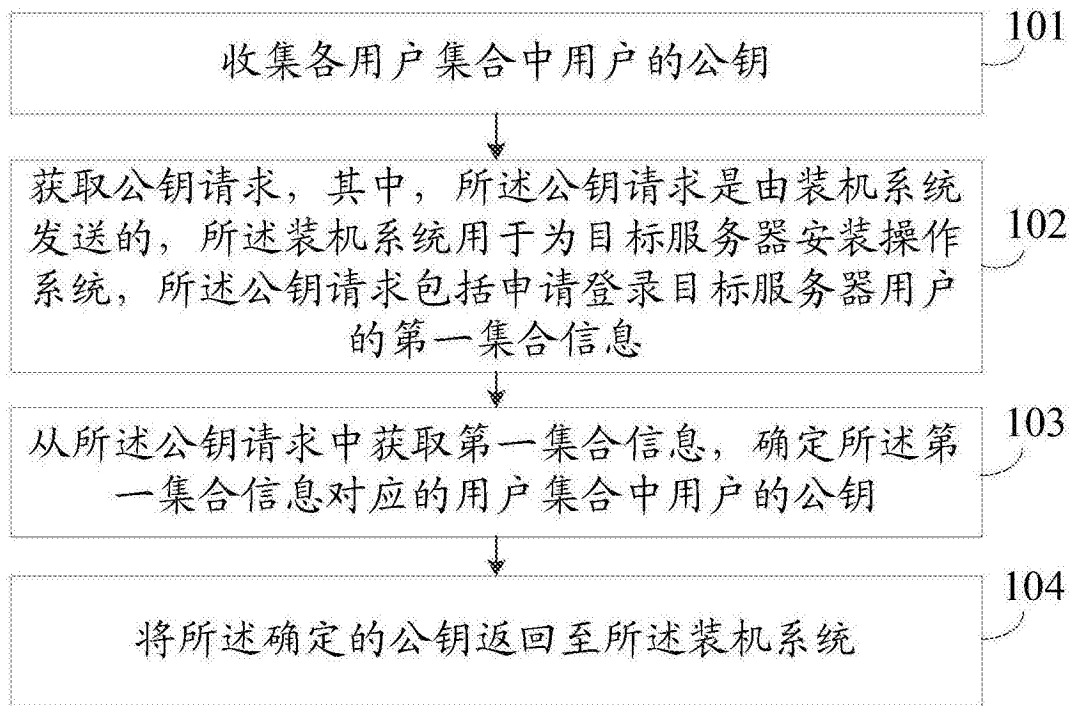


图1

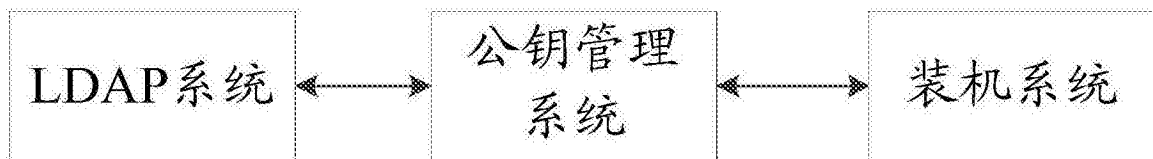


图2

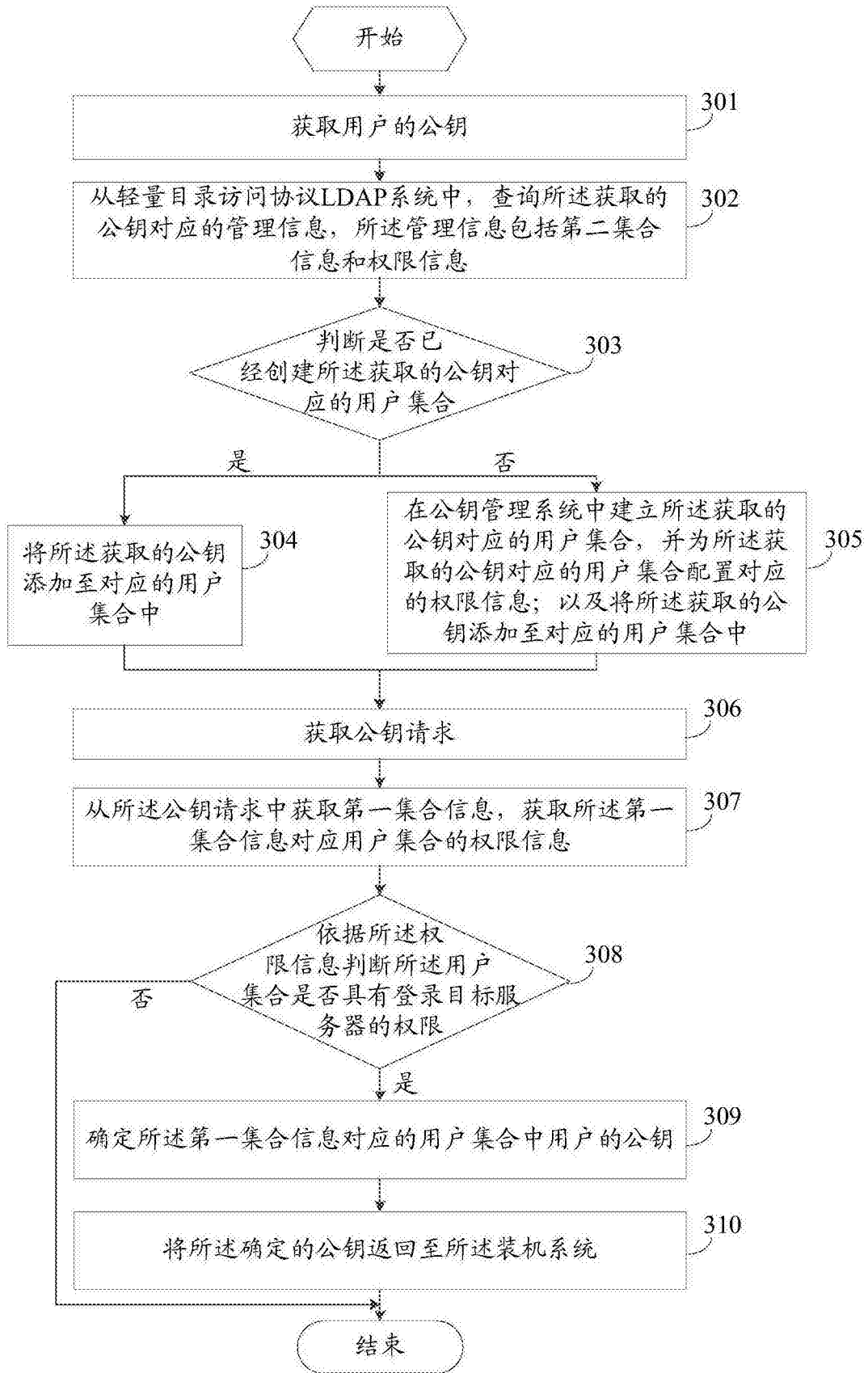


图3



图4



图5