



(12) 发明专利

(10) 授权公告号 CN 102035849 B

(45) 授权公告日 2013. 12. 18

(21) 申请号 201010604779. X

CN 101197026 A, 2008. 06. 11,

(22) 申请日 2010. 12. 23

审查员 颜悦

(73) 专利权人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

(72) 发明人 祁小波

(74) 专利代理机构 北京同立钧成知识产权代理
有限公司 11205

代理人 刘芳

(51) Int. Cl.

H04L 29/06 (2006. 01)

H04L 29/08 (2006. 01)

(56) 对比文件

CN 101197026 A, 2008. 06. 11,

CN 101296230 A, 2008. 10. 29,

CN 101350710 A, 2009. 01. 21,

CN 101425027 A, 2009. 05. 06,

WO 2005/018254 A2, 2005. 02. 24,

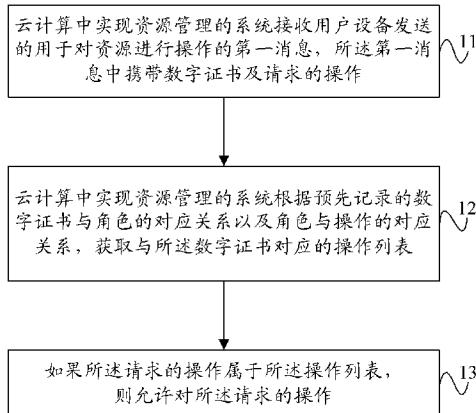
权利要求书2页 说明书8页 附图7页

(54) 发明名称

云计算中实现资源管理的方法、设备及系统

(57) 摘要

本发明提供一种云计算中实现资源管理的方法、设备及系统。该方法包括接收用户设备发送的用于对资源进行操作的第一消息，所述第一消息中携带数字证书及请求的操作；根据预先记录的数字证书与角色的对应关系以及角色与操作的对应关系，获取与所述数字证书对应的操作列表；如果所述请求的操作属于所述操作列表，则允许对所述请求的操作。本发明实施例可以实现分权分域管理。



1. 一种云计算中实现资源管理的方法,其特征在于,包括:

接收用户设备发送的用于注册的第二消息,所述第二消息中携带请求的角色;

根据预先配置的角色与数字证书的对应关系,为所述用户设备分配数字证书,并记录数字证书与角色的对应关系,其中,不同的角色对应不同的数字证书;

将分配的数字证书发送给所述用户设备,以便所述用户设备采用所述数字证书请求操作;

接收用户设备发送的用于对资源进行操作的第一消息,所述第一消息中携带数字证书及请求的操作;

根据预先记录的数字证书与角色的对应关系以及角色与操作的对应关系,获取与所述数字证书对应的操作列表;

如果所述请求的操作属于所述操作列表,则允许对所述请求的操作。

2. 根据权利要求 1 所述的方法,其特征在于,当所述数字证书为具有创建虚拟机权限的数字证书,所述请求的操作为创建虚拟机时,所述允许对所述请求的操作,包括:

创建与所述具有创建权限的数字证书对应的虚拟机,并记录数字证书与虚拟机的对应关系。

3. 根据权利要求 1 所述的方法,其特征在于,当所述数字证书为具有分配权限的数字证书,所述请求的操作为将所述具有分配权限的数字证书对应的虚拟机分配给被授权的数字证书时,所述允许对所述请求的操作,包括:

将所述具有分配权限的数字证书对应的虚拟机分配给所述被授权的数字证书;

更新已记录的数字证书与资源的对应关系,使得与所述有分配权限的数字证书对应的资源,与所述被授权的数字证书关联,以便用户设备采用所述 被授权的数字证书能够对与所述有分配权限的数字证书对应的资源进行操作。

4. 根据权利要求 1 所述的方法,其特征在于,在具有授权权限的数字证书将对应的资源授权给被授权的数字证书后,所述允许对所述请求的操作,包括:

根据所述被授权的数字证书的权限,对与所述具有分配权限的数字证书对应的资源进行操作。

5. 一种云计算中实现资源管理的设备,其特征在于,包括:

接收模块,用于接收用户设备发送的用于注册的第二消息,所述第二消息中携带请求的角色;

执行模块,用于根据预先配置的角色与数字证书的对应关系,为所述用户设备分配数字证书,并记录数字证书与角色的对应关系,其中,不同的角色对应不同的数字证书;将分配的数字证书发送给所述用户设备,以便所述用户设备采用所述数字证书请求操作;

所述接收模块,还用于接收用户设备发送的用于对资源进行操作的第一消息,所述第一消息中携带数字证书及请求的操作;

获取模块,用于根据预先记录的数字证书与角色的对应关系以及角色与操作的对应关系,获取与所述数字证书对应的操作列表;

所述执行模块,还用于如果所述请求的操作属于所述操作列表,则允许对所述请求的操作。

6. 根据权利要求 5 所述的设备,其特征在于,当所述数字证书为具有创建虚拟机权限

的数字证书,所述请求的操作为创建虚拟机时,所述执行模块具体用于创建与所述具有创建权限的数字证书对应的虚拟机,并记录数字证书与虚拟机的对应关系。

7. 根据权利要求 5 所述的设备,其特征在于,当所述数字证书为具有分配权限的数字证书,所述请求的操作为将所述具有分配权限的数字证书对应的虚拟机分配给被授权的数字证书时,所述执行模块具体用于将所述具有分配权限的数字证书对应的虚拟机分配给所述被授权的数字证书;更新已记录的数字证书与资源的对应关系,使得与所述有分配权限的数字证书对应的资源,与所述被授权的数字证书关联,以便用户设备采用所述被授权的数字证书能够对与所述有分配权限的数字证书对应的资源进行操作。

8. 根据权利要求 5 所述的设备,其特征在于,在具有授权权限的数字证书将对应的资源授权给被授权的数字证书后,所述执行模块具体用于根据所述被授权的数字证书的权限,对与所述具有授权权限的数字证书对应的资源进行操作。

9. 一种云计算中实现资源管理的系统,其特征在于,包括:

UPF,用于接收用户设备发送的用于注册的第二消息,所述第二消息中携带请求的角色;根据预先配置的角色与数字证书的对应关系,为所述用户设备分配数字证书,并记录数字证书与角色的对应关系其中,不同的角色对应不同的数字证书;将分配的数字证书发送给所述用户设备,以便所述用户设备采用所述数字证书请求操作;

云管理设备,用于接收用户设备发送的用于对资源进行操作的第一消息,所述第一消息中携带数字证书及请求的操作;根据 UPF 中记录的数字证书与角色的对应关系以及角色与操作的对应关系,获取与所述数字证书对应的操作列表;如果所述请求的操作属于所述操作列表,则允许对所述请求的操作。

云计算中实现资源管理的方法、设备及系统

技术领域

[0001] 本发明涉及网络通信技术，尤其涉及一种云计算中实现资源管理的方法、设备及系统。

背景技术

[0002] 云计算网络中包括具有强大计算能力的“云”和用户终端，云计算的核心理念就是通过不断提高“云”的处理能力，进而减少用户终端的处理负担，最终使用户终端简化成一个单纯的输入输出设备，并能按需享受“云”的强大计算处理能力。

[0003] 现有云计算网络中，云网络可以为用户分配安全认证证书，用户采用该安全认证证书访问云网络。但是，现有的安全认证证书只是能够对用户进行安全认证，不能实现分权分域管理。

发明内容

[0004] 本发明实施例是提供一种云计算中实现资源管理的方法、设备及系统，用以实现云计算中对资源的分权分域管理。

[0005] 本发明实施例提供了一种云计算中实现资源管理的方法，包括：

[0006] 接收用户设备发送的用于对资源进行操作的第一消息，所述第一消息中携带数字证书及请求的操作；

[0007] 根据预先记录的数字证书与角色的对应关系以及角色与操作的对应关系，获取与所述数字证书对应的操作列表；

[0008] 如果所述请求的操作属于所述操作列表，则允许对所述请求的操作。

[0009] 本发明实施例提供了一种云计算中实现资源管理的设备，包括：

[0010] 接收模块，用于接收用户设备发送的用于对资源进行操作的第一消息，所述第一消息中携带数字证书及请求的操作；

[0011] 获取模块，用于根据预先记录的数字证书与角色的对应关系以及角色与操作的对应关系，获取与所述数字证书对应的操作列表；

[0012] 执行模块，用于如果所述请求的操作属于所述操作列表，则允许对所述请求的操作。

[0013] 本发明实施例提供了一种云计算中实现资源管理的系统，包括：

[0014] UPF，用于接收用户设备发送的用于注册的第二消息，所述第二消息中携带请求的角色；根据预先配置的角色与数字证书的对应关系，为所述用户设备分配数字证书，并记录数字证书与角色的对应关系；将分配的数字证书发送给所述用户设备，以便所述用户设备采用所述数字证书请求操作；

[0015] 云管理设备，用于接收用户设备发送的用于对资源进行操作的第一消息，所述第一消息中携带数字证书及请求的操作；根据 UPF 中记录的数字证书与角色的对应关系以及角色与操作的对应关系，获取与所述数字证书对应的操作列表；如果所述请求的操作属于

所述操作列表，则允许对所述请求的操作。

[0016] 由上述技术方案可知，本发明实施例通过在访问云资源中采用数字证书，该数字证书对应不同的角色，不同的角色对应不同的操作，因此，通过该数字证书可以使得具有不同权限或者不同区域的用户能够执行的操作不同，实现对用户的分权分域管理。

附图说明

[0017] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

- [0018] 图 1 为本发明第一实施例的方法流程示意图；
- [0019] 图 2 为本发明第二实施例对应的系统结构示意图；
- [0020] 图 3 为本发明第二实施例对应的方法流程示意图；
- [0021] 图 4 为本发明实施例中证书系统的示意图；
- [0022] 图 5 为本发明第三实施例的方法流程示意图；
- [0023] 图 6 为本发明第四实施例的方法流程示意图；
- [0024] 图 7 为本发明第五实施例的方法流程示意图；
- [0025] 图 8 为本发明实施例中应用场景的示意图；
- [0026] 图 9 为本发明实施例中资源共享前后的示意图；
- [0027] 图 10 为本发明第六实施例的设备结构示意图；
- [0028] 图 11 为本发明第七实施例的系统结构示意图。

具体实施方式

[0029] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0030] 图 1 为本发明第一实施例的方法流程示意图，包括：

[0031] 步骤 11：云计算中实现资源管理的系统接收用户设备发送的用于对资源进行操作的第一消息，所述第一消息中携带数字证书及请求的操作；

[0032] 步骤 12：云计算中实现资源管理的系统根据预先记录的数字证书与角色的对应关系以及角色与操作的对应关系，获取与所述数字证书对应的操作列表；

[0033] 步骤 13：如果所述请求的操作属于所述操作列表，则允许对所述请求的操作。

[0034] 本实施例通过在访问云资源中采用数字证书，该数字证书对应不同的角色，不同的角色对应不同的操作，因此，通过该数字证书可以使得具有不同权限或者不同区域的用户能够执行的操作不同，实现对用户的分权分域管理。

[0035] 图 2 为本发明第二实施例对应的系统结构示意图，包括用户设备 (USER) 21、发放工作流引擎 (Provisioning Orchestration Engine, POE) 22、用户数据功能 (User Profile Function, UPF) 实体 23、虚拟机桌面 (VDESKTOP) 24 和云资源管理设备 25。其中，用户设备

21 可以对应企业、家庭、个人，例如，将一个企业所使用的终端设备作为一个用户设备。POE
22 是用户的开户入口，例如，用户在注册时，用户设备可以通过该 POE 向 UPF 发送用于注册
的消息，在 UPF 完成用户注册。UPF 23 用于为申请注册的用户分配数字证书和资源，并保存
相互的对应关系。虚拟机桌面 24 是用户的访问接口，例如，用户设备通过该虚拟机桌面向
云资源管理设备请求对指定资源的指定操作。云资源管理设备 25 用于接收用户设备通过
虚拟机桌面发送的用于对资源操作的消息，之后，根据该消息中携带的相关信息从 UPF 进
行认证，如果通过认证，则允许用户设备执行相应的操作。

[0036] 对于上述的各设备之间的具体交互内容可以参见下述的方法实施例。

[0037] 图 3 为本发明第二实施例对应的方法流程示意图，包括：

[0038] 步骤 31：用户设备向 POE 发送用于注册的第二消息，该第二消息中携带请求的角色。

[0039] 本实施例中，为了实现分权分域管理，可以为不同的数字证书分配不同的角色，不同的角色具有不同的权限，不同的权限可以执行不同的操作，例如，角色可以包括 admin、operation、guest，其中，admin 可以进行所有操作，operation 可以进行查看和修改操作，guest 仅可以查看。则采用 admin 对应的数字证书的用户可以创建、删除、修改和查看，采用 operation 对应的数字证书的用户可以修改和查看，采用 guest 对应的数字证书的用户仅可以查看。

[0040] 步骤 32：POE 将该第二消息转发给 UPF。

[0041] 步骤 33：UPF 接收到该第二消息后，为该用户设备分配数字证书，并记录用户设备与数字证书及角色的对应关系。

[0042] 其中，UPF 可以采用随机的方式，为不同的角色分配不同的数字证书，需要保证不同的角色对应不同的数字证书。

[0043] 例如，图 4 为本发明实施例中证书系统的示意图，参见图 4，在 UPF 中可以保存证书
系统，该证书系统包括操作列表 (PriInfo)、角色列表 (RoleInfo) 和用户列表 (UserInfo)。
操作列表中包括 n 个操作 (Pri)，角色列表中包括 n 个角色 (Role)，用户列表中包括 n 个用
户 (User)。可以理解的是，操作、角色、用户的个数可以是不一样的。

[0044] 其中，每个操作的组成可以参见表 1，每个角色的组成可以参见表 2，每个用户的组
成可以参见表 3。

[0045] 表 1

[0046]

数据	描述
PRIDESC	权限描述
PRIVID	权限 ID
PRIVNAME	操作名称
SERVICETYPE	系统服务类型

[0047] 表 2

[0048]

数据	描述
ROLEDESC	角色描述
ROLEID	角色 ID
ROLENAMES	角色名称
PRIVID	权限 ID

[0049] 表 3

[0050]

数据	描述
CERTCONTENT	证书内容
CERTID	证书 ID
CREATEDTIME	创建时间
STATUS	证书状态
ROLEID	角色 ID
RESOWNER	资源拥有者

[0051] 上述三个列表中,操作列表和角色列表可以是预先配置的,用户列表可以是随着用户设备申请数字证书而不断更新的。例如,当 User ~ 1 请求角色 ~ 1 时,UPF 可以为其随机分配一个数字证书(该随机分配的数字证书与其他角色的数字证书不相同),并将其数字证书的 ID 号记录在表 3 中的证书 ID 项中。即,假设角色 ~ 1 对应的数字证书为证书 ~ 1,则 User ~ 1 对应表 3 中的资源拥有者为 User ~ 1,证书 ID 为证书 ~ 1,角色 ID 为角色 ~ 1。另外,创建时间是创建数字证书时的时间,证书内容是指用户进行认证的公私密钥对,在生成证书时可以根据预置(包括用户名、时间戳等)条件生成证书的证书内容,证书状态可以为 active 或则 inactive,当证书失效时,证书的状态就会被置为 inactive。

[0052] 另外,可以理解的是,一个用户设备可以请求多个角色,以对应获取多个数字证书,之后,可以将该多个数字证书分配给使用该用户设备的不同用户使用。例如,一个企业可以申请对应 admin、operation、guest 等不同角色的数字证书,之后,将不同角色对应的数字证书分配给不同的人员使用。

[0053] 步骤 34 :UPF 将分配的数字证书通过 POE 返回给用户设备。

[0054] 至此,完成了用户开户,之后,用户设备可以采用分配的数字证书请求需要的操作。

[0055] 步骤 35 :用户设备采用分配的数字证书请求操作。

[0056] 本实施例通过为用户分配数字证书,且不同的数字证书具有不同的角色,可以执

行不同的操作,因此可以实现分权分域管理。

[0057] 下面以操作作为创建虚拟机为例,具体流程可以参见图 5。

[0058] 图 5 为本发明第三实施例的方法流程示意图,本实施例以用户设备请求创建虚拟机为例,参见图 5,本实施例包括:

[0059] 步骤 51 :用户设备获取数字证书。具体内容可以参见步骤 31-34。

[0060] 步骤 52 :用户设备通过虚拟机桌面向云资源管理设备发送用于对资源进行操作的第一消息,所述第一消息中携带数字证书及请求的操作。

[0061] 步骤 53 :云资源管理设备对该第一消息进行认证。

[0062] 例如,如果第一消息在发送时经过了加密处理,则云资源管理设备需要解密。另外,云资源管理设备还可以向 UPF 获取用户信息,判断该数字证书是否对该用户设备所有以验证用户合法性。具体地加解密算法以及用户合法性验证过程可以采用通常方法实现。

[0063] 特别地,本实施例在经过上述验证后,还需要进行权限验证,具体如下:

[0064] 步骤 54 :云资源管理设备从 UPF 中获取与该数字证书对应的操作列表。

[0065] 具体地,可以首先根据表 3 获取与数字证书对应的角色 ID,再根据表 2 获取与角色 ID 对应的权限 ID,之后根据表 1 获取与权限 ID 对应的操作名称。该数字证书对应的所有操作名称则可以组成操作列表。例如,如果数字证书对应的角色为 admin,则对应的操作列表包括创建、删除、修改和查看;如果数字证书对应的角色为 operation,则对应的操作列表包括修改和查看;如果数字证书对应的角色为 guest,则对应的操作仅包括查看。

[0066] 步骤 55 :如果所述请求的操作属于所述操作列表,则允许对所述请求的操作,例如,创建虚拟机。

[0067] 例如,本实施例中假设该用户采用的数字证书可以执行创建操作,并且请求的操作为创建虚拟机,则云资源管理设备创建虚拟机。

[0068] 为了进一步实现数据共享,本实施例还可以包括:

[0069] 步骤 56 :云资源管理设备记录数字证书与虚拟机的对应关系。

[0070] 在某些场景下可能需要数字证书之间的互相授权,例如需要将数字证书~1 下的资源分配给数字证书~2 使用,以实现资源共享。

[0071] 本实施例通过采用数字证书访问云资源管理设备,且不同的数字证书具有不同的角色,可以执行不同的操作,因此可以实现分权分域管理。

[0072] 图 6 为本发明第四实施例的方法流程示意图,本实施例以将某一数字证书下的虚拟机分配给另一数字证书使用为例,参见图 6,本实施例包括:

[0073] 步骤 61 :用户设备获取数字证书。

[0074] 具体内容可以参见步骤 51。

[0075] 步骤 62 :用户设备通过虚拟机桌面向云资源管理设备发送用于对资源进行操作的第一消息,该第一消息中携带数字证书及请求的操作。

[0076] 其中,本实施例中假设用户设备获取的数字证书为证书~1,请求的操作是将证书~1 对应的虚拟机分配给证书~2 使用。

[0077] 步骤 63 :云资源管理设备对该第一消息进行认证。

[0078] 步骤 64 :云资源管理设备从 UPF 中获取与该数字证书对应的操作列表。

[0079] 其中,步骤 63-64 的具体内容可以参见步骤 53-54。

[0080] 步骤 65 :如果所述请求的操作属于所述操作列表,则允许对所述请求的操作,例如分配虚拟机。在分配虚拟机时可以是在云资源管理设备中增加资源和证书 ID 的对应关系。

[0081] 例如,如果证书~1 对应的操作包括分配资源,则本实施例中云资源管理设备可以将证书~1 对应的虚拟机分配给证书~2。

[0082] 步骤 66 :云资源管理设备更新数字证书与虚拟机的对应关系。

[0083] 例如,原有的是虚拟机~1 对应证书~1,但是经过上述处理,则虚拟机~1 对应的证书包括证书~1 和证书~2。

[0084] 通过图 6 所示的流程,证书~2 可以具有对证书~1 所属的资源的操作权限,例如,采用证书~2 也可以对虚拟机~1 进行操作,具体下一个实施例。

[0085] 本实施例通过采用数字证书访问云资源管理设备,且不同的数字证书具有不同的角色,可以执行不同的操作,因此可以实现分权分域管理。另外,本实施例通过将一数字证书下的资源分配给另一数字证书使用,可以实现资源共享。

[0086] 图 7 为本发明第五实施例的方法流程示意图,本实施例以被授权的数字证书对具有授权权限的数字证书的资源进行操作为例,参见图 7,本实施例包括 :

[0087] 步骤 71 :用户设备获取数字证书。

[0088] 步骤 72 :用户设备通过虚拟机桌面向云资源管理设备发送用于对资源进行操作的第一消息,所述第一消息中携带数字证书及请求的操作。

[0089] 步骤 73 :云资源管理设备对该第一消息进行认证。

[0090] 步骤 74 :云资源管理设备从 UPF 中获取与该数字证书对应的操作列表。

[0091] 步骤 75 :如果所述请求的操作属于所述操作列表,则允许对所述请求的操作,例如,重启虚拟机。

[0092] 其中,步骤 71-75 的具体内容类似于步骤 61-65,与步骤 61-65 不同的是,图 6 所示的实施例中采用的数字证书是具有授权权限的数字证书(如证书~1),而本实施例中采用的数字证书是被授权的数字证书(如证书~2)。

[0093] 另外,通过图 6 所示的流程,云资源管理设备中已经更新了资源与数字证书的对应关系,所以,采用证书~2 也可以对虚拟机~1 进行证书~2 具有的权限的操作,例如,证书~2 具有重启虚拟机的权限,请求的操作是重启虚拟机,则本实施例中采用证书~2 可以重启虚拟机。

[0094] 本实施例通过采用被授权的数字证书访问具有授权权限的数字证书所属的资源,实现了资源共享。

[0095] 本发明实施例的上述方法可以应用于如下场景 :

[0096] 企业级应用 :该系统应用于企业中,企业管理者相当于 USER,对于企业内部不通层次的员工可以申请不通的证书,证书的角色以及证书角色对应的操作的功能可以由企业管理者要求,系统在初始化时提供.USER 可以将证书分配给企业内部不同层次的员工,执行相应的操作,在人事变更或者企业内部结构整改时,只需要动态修改子用户持有的证书角色,即可完成整个企业的分权分域。

[0097] 这样,整个企业内部的管理完全由证书来管理,操作灵活、简单,管理高效。资源共享可以实现企业内部的工作委托,例如 :A 因出差将资源委托为 B,那么 B 便可完成 B 持有证

书的权限对于 A 资源的操作。

[0098] 家庭级应用：对于家庭级应用，资源共享能起到更大的作用。以家庭为单位作为 USER，可根据家庭中的用户来申请不同的证书角色，这样，在一个家庭中，所有家庭成员可对同一资源进行不同权限操作。家庭成员之间可以实现资源共享，从而最大限度的节省资源。

[0099] 当然，本发明实施例并不限于上述应用，可以应用于各种应用中，可以提供的动态的调配来满足用户的需求。

[0100] 在采用本发明实施例的方法之后，每个用户设备可以对应多个证书，例如，图 8 为本发明实施例中应用场景的示意图，参见图 8，每个用户设备 (USER) 可以对应一个证书集，该证书集中包括多个证书，不同证书具有不同的权限，其中用户设备例如为企业、家庭、个人。由于证书具有不同的权限，采用不同证书时可以执行的操作不同，因此可以实现分权分域管理。

[0101] 另外，本发明实施例通过一个证书将其下的资源分配给另一个证书，可以实现资源共享，例如，图 9 为本发明实施例中资源共享前后的示意图，参见图 9，资源共享前，USER ~ 1 (对应的数字证书为证书~ 1) 可以访问的资源为 VM ~ 1，USER ~ 2 (对应的数字证书为证书~ 2) 可以访问的资源为 VM ~ 2；当证书~ 2 授权给证书~ 1 实现资源共享后，USER ~ 1 (对应的数字证书为证书~ 1) 可以访问的资源为 VM ~ 1 和 VM ~ 2，USER ~ 2 (对应的数字证书为证书~ 2) 可以访问的资源为 VM ~ 2。

[0102] 综上所述，本发明实施例中的数字证书不仅可以实现认证功能，另外通过对数字证书进行授权，授权包括操作和资源，可以通过数字证书进行分权分域管理以及资源共享，使得分权分域操作更加合理。通过采用具有分权分域功能的数字证书，可以使得接入用户请求时便可以完成通用鉴权与业务鉴权，使得整个系统的管理层次更加分明。同时资源共享可以避免整个系统中的资源浪费，用户对于资源的整体需求也会收缩，从而节省用户资源效益，同时资源操作更加灵活。

[0103] 图 10 为本发明第六实施例的设备结构示意图，包括接收模块 101、获取模块 102 和执行模块 103；接收模块 101 用于接收用户设备发送的用于对资源进行操作的第一消息，所述第一消息中携带数字证书及请求的操作；获取模块 102 用于根据预先记录的数字证书与角色的对应关系以及角色与操作的对应关系，获取与所述数字证书对应的操作列表；执行模块 103 用于如果所述请求的操作属于所述操作列表，则允许对所述请求的操作。

[0104] 其中，当所述数字证书为具有创建虚拟机权限的数字证书，所述请求的操作为创建虚拟机时，所述执行模块具体用于创建与所述具有创建权限的数字证书对应的虚拟机，并记录数字证书与虚拟机的对应关系。

[0105] 或者，当所述数字证书为具有分配权限的数字证书，所述请求的操作为将所述具有分配权限的数字证书对应的虚拟机分配给被授权的数字证书时，所述执行模块具体用于将所述具有分配权限的数字证书对应的虚拟机分配给所述被授权的数字证书；更新已记录的数字证书与资源的对应关系，使得与所述有授权权限的数字证书对应的资源，与所述被授权的数字证书关联，以便用户设备采用所述被授权的数字证书能够对与所述有授权权限的数字证书对应的资源进行操作。

[0106] 或者，在具有授权权限的数字证书将对应的资源授权给被授权的数字证书后，所

述执行模块具体用于根据所述被授权的数字证书的权限,对与所述具有授权权限的数字证书对应的资源进行操作。

[0107] 本实施例通过在访问云资源中采用数字证书,该数字证书对应不同的角色,不同的角色对应不同的操作,因此,通过该数字证书可以使得具有不同权限或者不同区域的用户能够执行的操作不同,实现对用户的分权分域管理。

[0108] 图 11 为本发明第七实施例的系统结构示意图,包括 UPF 111 和云管理设备 112 ; UPF 111 用于接收用户设备发送的用于注册的第二消息,所述第二消息中携带请求的角色;根据预先配置的角色与数字证书的对应关系,为所述用户设备分配数字证书,并记录数字证书与角色的对应关系;将分配的数字证书发送给所述用户设备,以便所述用户设备采用所述数字证书请求操作;云管理设备 112 用于接收用户设备发送的用于对资源进行操作的第一消息,所述第一消息中携带数字证书及请求的操作;根据 UPF 中记录的数字证书与角色的对应关系以及角色与操作的对应关系,获取与所述数字证书对应的操作列表;如果所述请求的操作属于所述操作列表,则允许对该请求的操作。

[0109] 本实施例通过在访问云资源中采用数字证书,该数字证书对应不同的角色,不同的角色对应不同的操作,因此,通过该数字证书可以使得具有不同权限或者不同区域的用户能够执行的操作不同,实现对用户的分权分域管理。

[0110] 可以理解的是,上述方法及设备中的相关特征可以相互参考。另外,上述实施例中的“第一”、“第二”等是用于区分各实施例,而并不代表各实施例的优劣。

[0111] 本领域普通技术人员可以理解:实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成,前述的程序可以存储于计算机可读取存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0112] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

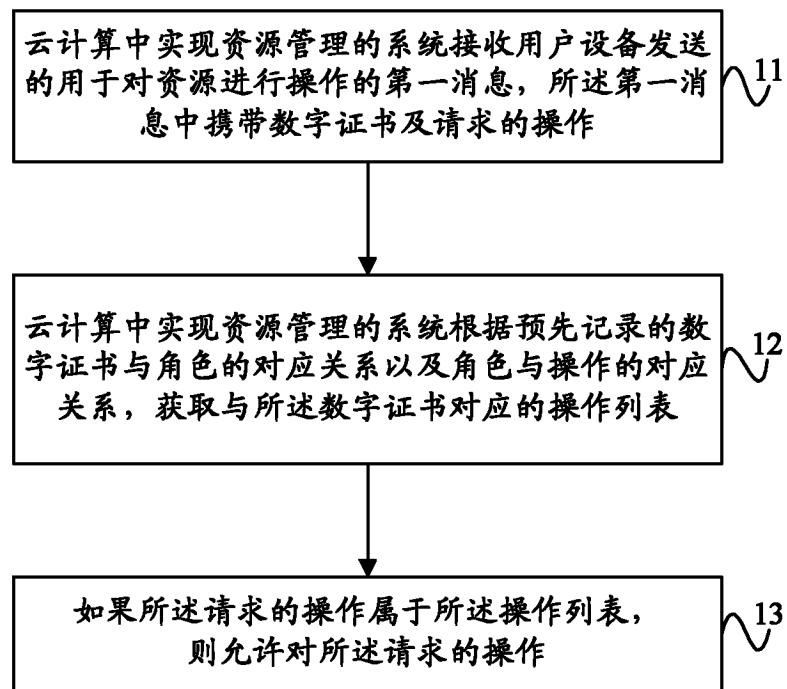


图 1

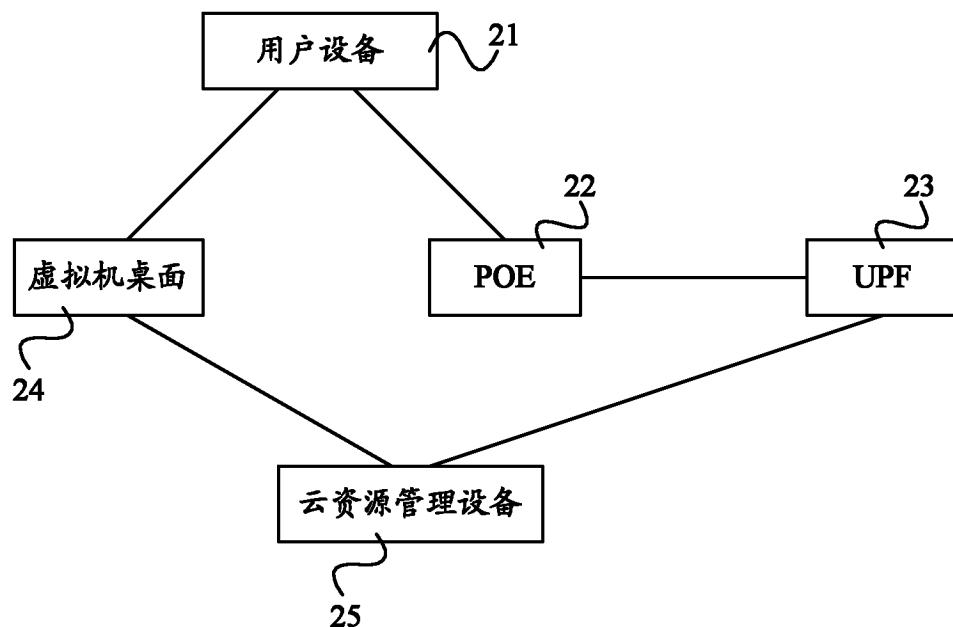


图 2

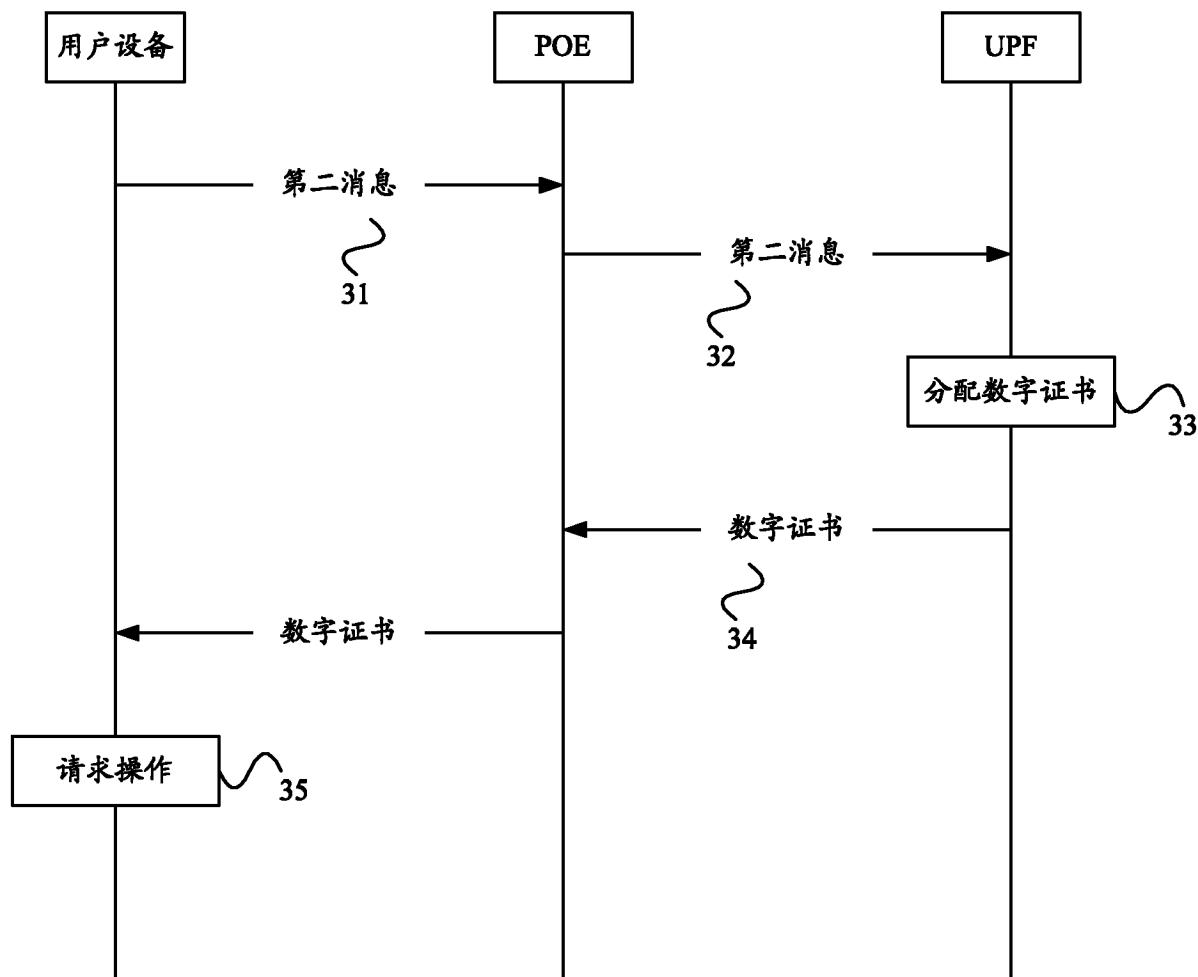


图 3

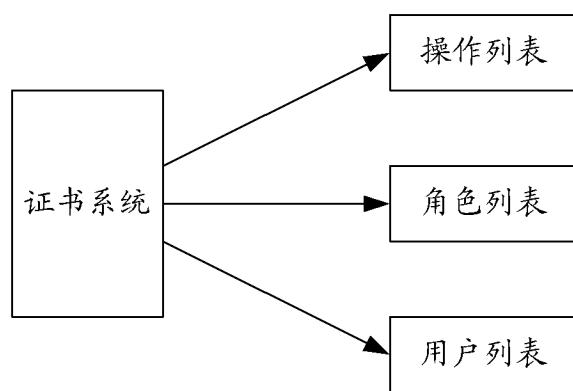


图 4

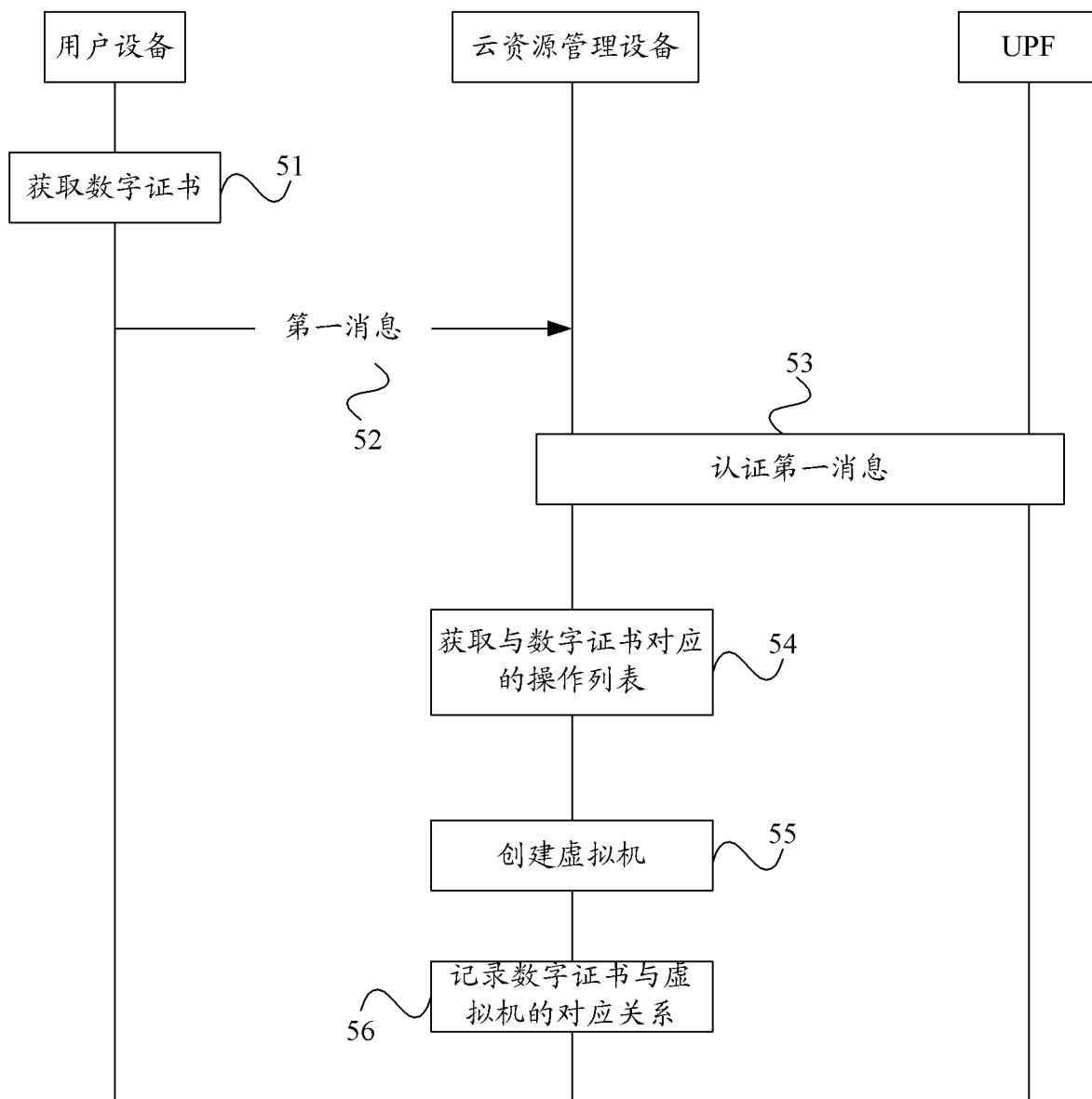


图 5

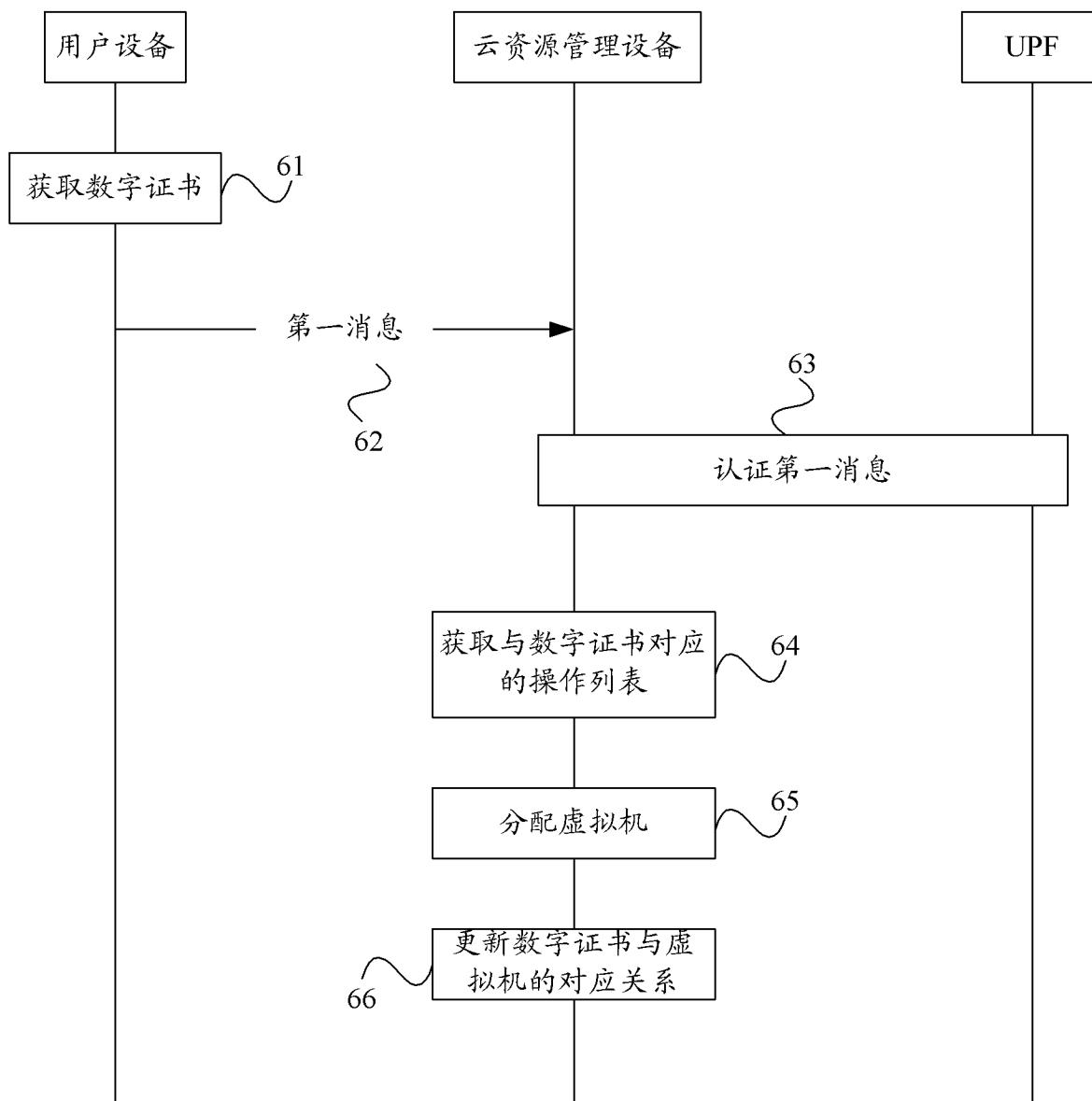


图 6

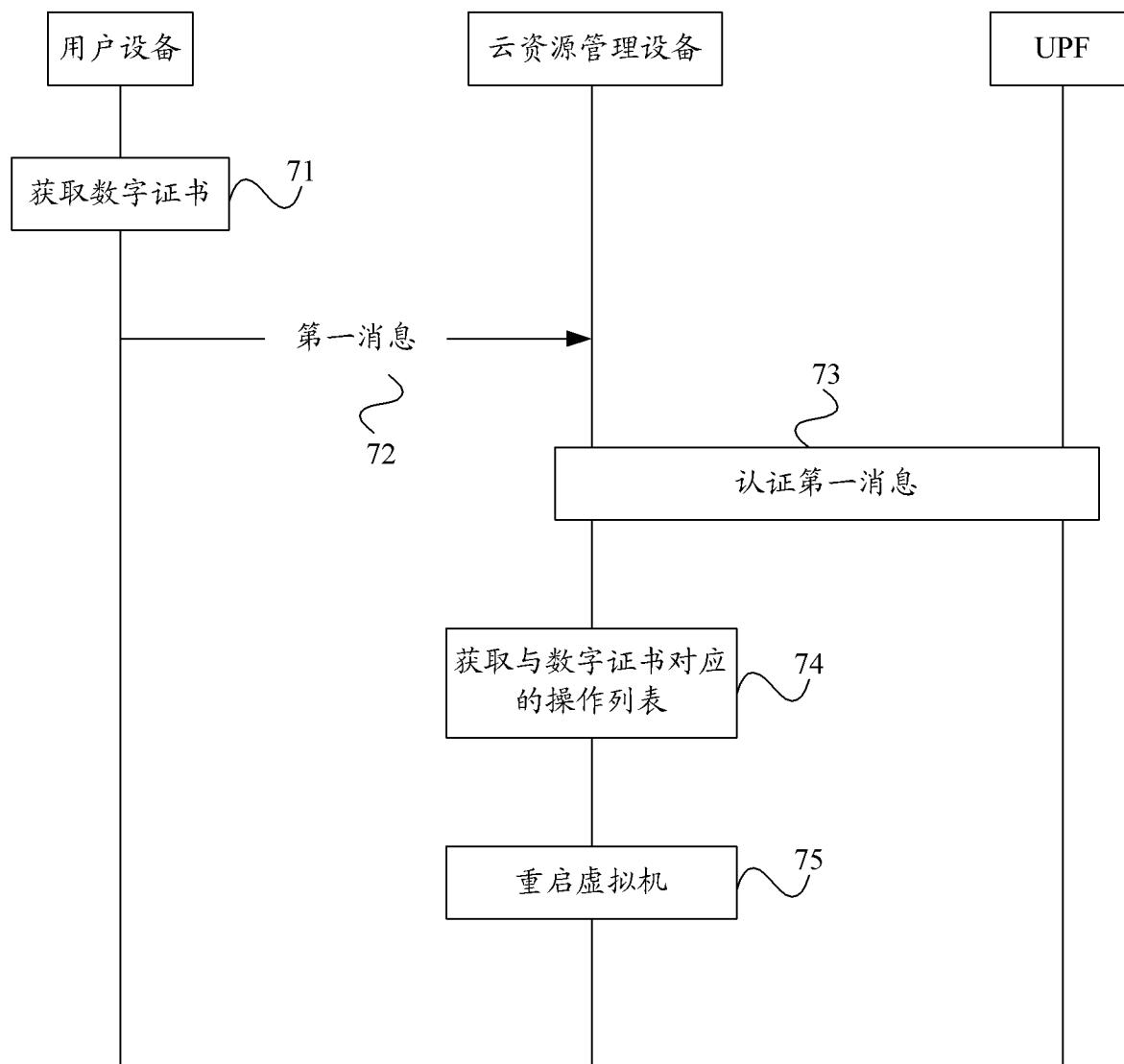


图 7

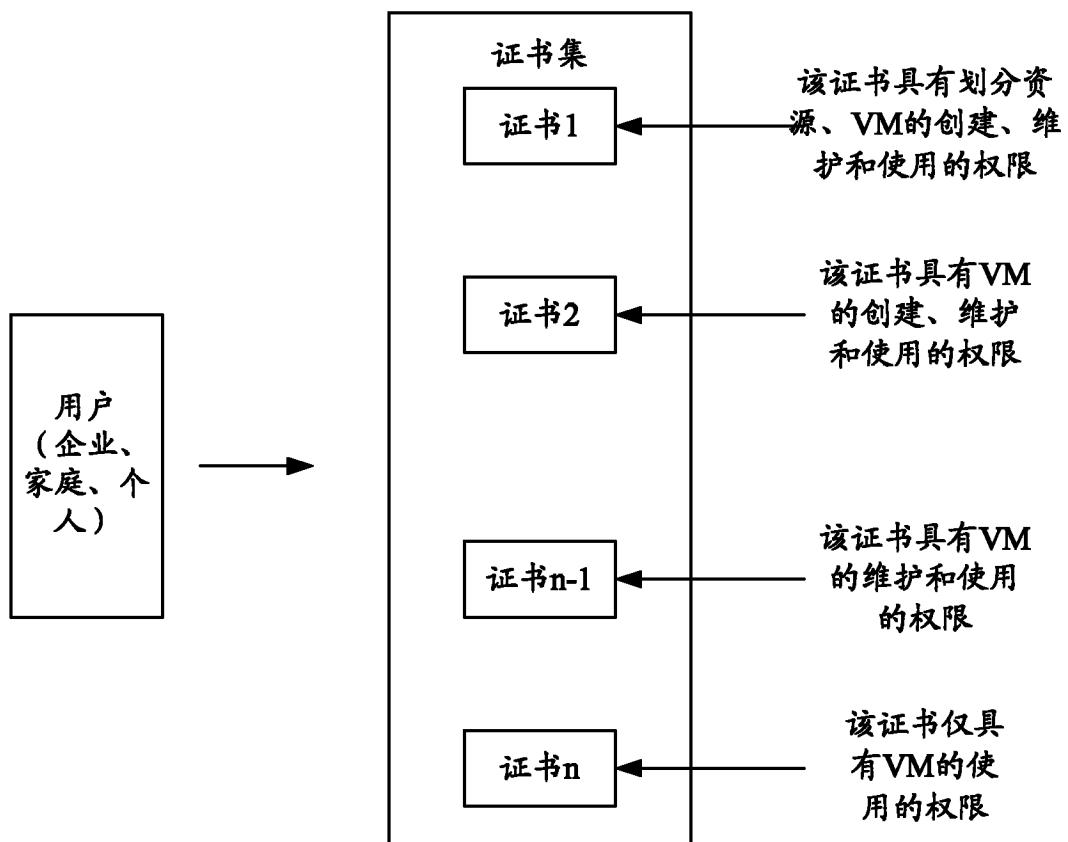


图 8

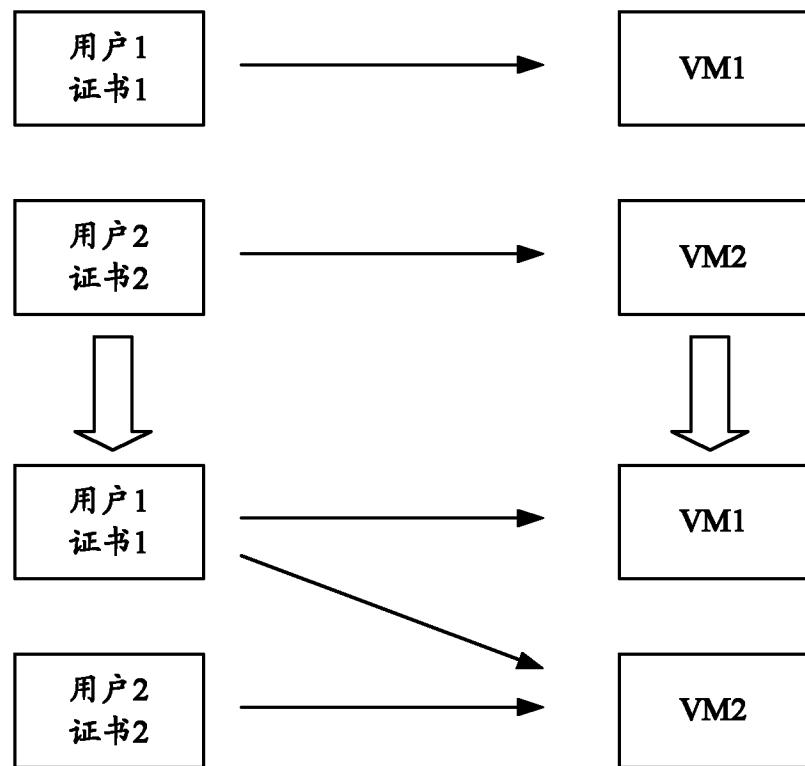


图 9

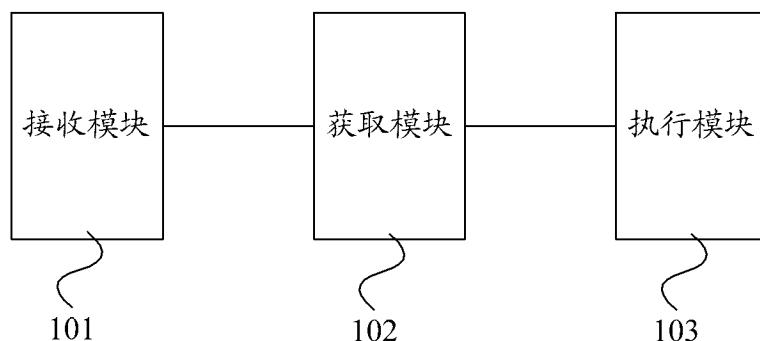


图 10



图 11