(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102457507 A
(43)申请公布日 2012.05.16

(21)申请号 201010527248.5

(22)申请日 2010.10.29

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 陈小华 李一凡 王治平 林兆骥

(74)专利代理机构 北京派特恩知识产权代理事务所(普通合伙) 11270
代理人 王黎延 迟姗

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

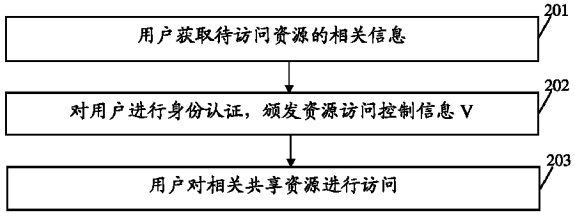
权利要求书 2 页 说明书 7 页 附图 2 页

(54)发明名称

云计算资源安全共享方法、装置及系统

(57)摘要

本发明公开了一种云计算资源安全共享方法，方法包括：用户向云计算服务商服务器发送资源访问请求，资源访问请求中携带待访问资源的相关信息；云计算服务商服务器根据待访问资源的相关信息获取待访问资源所属的业务提供商服务器信息，并向待访问资源所属的业务提供商服务器发送认证请求；认证请求中携带有用户的标识信息；业务提供商服务器根据用户的标识信息对用户进行身份认证，并在认证通过后向用户或云计算服务商服务器发送资源访问控制信息；云计算服务商服务器对资源访问控制信息进行认证，并在认证通过后向用户提供待访问资源。本发明还公开了一种云计算资源安全共享装置。本发明提高了共享资源访问的效率及其安全性。



CN 102457507 A

1. 一种云计算资源安全共享方法，其特征在于，所述方法包括：

云计算服务商服务器接收用户发送的资源访问请求，所述资源访问请求中携带待访问资源的相关信息；

所述云计算服务商服务器根据所述待访问资源的相关信息获取待访问资源所属的业务提供商服务器信息，并向待访问资源所属的业务提供商服务器发送认证请求；所述认证请求中携带有所述用户的标识信息；

所述业务提供商服务器根据所述用户的标识信息对所述用户进行身份认证，颁发资源访问控制信息；

所述云计算服务商服务器对所述资源访问控制信息进行认证，并在认证通过后向所述用户提供待访问资源。

2. 根据权利要求 1 所述的方法，其特征在于，云计算服务商服务器接收用户发送的资源访问请求之前，所述方法还包括：

通过业务提供商服务器设置资源的访问权限，并向用户提供资源的相关信息。

3. 根据权利要求 1 所述的方法，其特征在于，所述颁发资源访问控制信息具体为：

将资源访问控制信息颁发给所述用户或所述云计算服务商服务器；其中，将资源访问控制信息颁发给所述用户时，所述用户向所述云计算服务商服务器发送所述资源访问控制信息。

4. 根据权利要求 1 所述的方法，其特征在于，所述资源的相关信息包括所述业务提供商服务器为用户设置的用户编号信息、资源编号信息、所述业务提供商服务器标识信息。

5. 根据权利要求 4 所述的方法，其特征在于，所述资源的相关信息还包括所述资源的有效时间信息；

所述业务提供商服务器标识信息中包括所述业务提供商服务器的 IP 地址信息，以及，所述业务提供商服务器的名称信息、或提供通信端口标识信息、或硬件标识信息。

6. 根据权利要求 1 所述的方法，其特征在于，云计算服务商服务器接收用户发送的资源访问请求之前，所述方法还包括：

所述业务提供商服务器接收所述用户的注册请求，并为所述用户提供注册标识及访问密码；

所述业务提供商服务器根据所述用户的标识信息对所述用户进行身份认证具体为：

所述业务提供商服务器根据所述云计算服务商服务器提供的所述用户的标识信息，获取所述用户注册的 IP 地址信息，向所述用户发送登录接口，通过所述登录接口接收所述用户输入的注册标识及访问密码，并进行验证。

7. 根据权利要求 1 所述的方法，其特征在于，云计算服务商服务器接收用户发送的资源访问请求之前，所述方法还包括：

向所述用户提供访问资源的云计算服务商服务器的 IP 地址信息；

所述用户根据所述云计算服务商服务器的 IP 地址信息向所述云计算服务商服务器发送资源访问请求。

8. 根据权利要求 1 至 7 任一项所述的方法，其特征在于，所述云计算资源包含云存储资源。

9. 一种云计算资源安全共享装置，其特征在于，所述装置包括接收单元、获取单元、第

一发送单元、第一认证单元、第二发送单元、第二认证单元和提供单元，其中，

接收单元，用于接收用户发送的资源访问请求，所述资源访问请求中携带待访问资源的相关信息；

获取单元，用于根据所述待访问资源的相关信息获取待访问资源所属的业务提供商服务器信息；

第一发送单元，用于向待访问资源所属的业务提供商服务器发送认证请求；所述认证请求中携带有所述用户的标识信息；

第一认证单元，用于根据所述用户的标识信息对所述用户进行身份认证；

第二发送单元，用于在所述第一认证单元认证通过后向所述用户或所述云计算服务商服务器发送资源访问控制信息；

第二认证单元，用于对所述资源访问控制信息进行认证；

提供单元，用于在所述第二认证单元认证通过后向所述用户提供待访问资源。

10. 根据权利要求 9 所述的装置，其特征在于，所述装置还包括：

设置及提供单元，用于通过业务提供商服务器设置资源的访问权限，并向用户提供资源的相关信息。

11. 根据权利要求 9 所述的装置，其特征在于，所述资源的相关信息包括所述业务提供商服务器为用户设置的用户编号信息、资源编号信息、所述业务提供商服务器标识信息。

12. 根据权利要求 11 所述的装置，其特征在于，所述资源的相关信息还包括所述资源的有效时间信息；

所述业务提供商服务器标识信息中包括所述业务提供商服务器的 IP 地址信息，以及，所述业务提供商服务器的名称信息、或提供通信端口标识信息、或硬件标识信息。

13. 一种云计算资源访问系统，其特征在于，所述系统包括业务提供商服务器和云计算服务商服务器；其中，

业务提供商服务器，用于向资源所有者提供设置资源所有者的资源的访问权限；以及，接收到云计算服务商服务器发送的资源访问请求后，根据所述用户的标识信息对所述用户进行身份认证，并在认证通过后向所述用户发送资源访问控制信息；

云计算服务商服务器，用于接收用户发送的资源访问请求，所述资源访问请求中携带待访问资源的相关信息；根据所述待访问资源的相关信息获取待访问资源所属的业务提供商服务器信息，并向待访问资源所属的业务提供商服务器发送认证请求；所述认证请求中携带有所述用户的标识信息；以及，对所述资源访问控制信息进行认证，并在认证通过后向所述用户提供待访问资源。

14. 根据权利要求 13 所述的系统，其特征在于，所述业务提供商服务器将资源访问控制信息颁发给所述用户或所述云计算服务商服务器；其中，将资源访问控制信息颁发给所述用户时，由所述用户向所述云计算服务商服务器发送所述资源访问控制信息。

云计算资源安全共享方法、装置及系统

技术领域

[0001] 本发明涉及资源访问技术，尤其涉及一种云计算资源安全共享方法、装置及系统。

背景技术

[0002] 云计算是分布式处理、并行处理和网格计算等结合的技术。云计算的核心思想，是将大量用网络连接的计算资源统一管理和调度，构成一个计算资源池向用户按需服务。

[0003] 通过使用云计算服务，业务提供商服务器可以降低企业运行成本，向用户提供可靠的资源访问服务。已经有越来越多的业务提供商服务器选择云计算服务向用户提供相关业务服务。

[0004] 业务提供商服务器使用云计算向用户提供业务服务。业务提供商服务器将业务资源提供给资源所有者使用，资源所有者对业务资源具有使用和共享权限。资源所有者向其他用户共享业务资源。当前，采用的共享方案为，资源所有者要想将共享资源共享给其他人，需要在业务提供商服务器设置资源的共享权限，允许其他用户的访问。而其他用户要想取得共享资源，也需要登录到业务提供商服务器，通过业务提供商服务器，才能看到所共享的资源。

[0005] 这种方式具有许多的缺点。首先，限制了用户灵活使用共享资源的方式。用户只有通过登录业务提供商服务器提供的服务站点，才能获得相应的业务提供商服务器在云计算服务商服务器储存的资源。其次，要求业务提供商服务器具有较大的服务提供能力。业务提供商服务器需要为众多的用户都提供相当于一个资源中继站的服务，这增加了业务提供商服务器的负载压力，而在云环境下，业务提供商服务器希望利用云而实现简单部署、降低成本，这就和云环境设置的初衷相违背，无疑增加了业务提供商服务器的负担。

[0006] 然而，随着云计算服务应用的发展，用户希望能够随时随地以较灵活的方式访问云计算服务商，进而获取业务提供商服务器储存在云计算服务商服务器的共享资源。但作为业务提供商服务器的主要业务支撑的用户资源，处于安全以及网络接入便利性的考量，业务提供商服务器希望禁止用户直接访问云计算服务商服务器而获取访问资源，从而避免用户资源不会泄露给云计算服务商服务器。因此，目前迫切需要一种资源技术方案，既为用户提供一个灵活访问共享资源的方式，又能保护业务提供商服务器的用户资源。遗憾的是，由于云计算技术尚在讨论阶段，目前并无相关的技术方案可供参考。

发明内容

[0007] 有鉴于此，本发明的主要目的在于提供一种云计算资源安全共享方法、装置及系统，方便用户访问共享资源的同时，保护了业务提供商的用户资源。

[0008] 为达到上述目的，本发明的技术方案是这样实现的：

[0009] 一种云计算资源安全共享方法，包括：

[0010] 云计算服务商服务器接收用户发送的资源访问请求，所述资源访问请求中携带待访问资源的相关信息；

[0011] 所述云计算服务商服务器根据所述待访问资源的相关信息获取待访问资源所属的业务提供商服务器信息，并向待访问资源所属的业务提供商服务器发送认证请求；所述认证请求中携带有所述用户的标识信息；

[0012] 所述业务提供商服务器根据所述用户的标识信息对所述用户进行身份认证，颁发资源访问控制信息；

[0013] 所述云计算服务商服务器对所述资源访问控制信息进行认证，并在认证通过后向所述用户提供待访问资源。

[0014] 优选地，云计算服务商服务器接收用户发送的资源访问请求之前，所述方法还包括：

[0015] 通过业务提供商服务器设置资源的访问权限，并向用户提供资源的相关信息。

[0016] 优选地，所述颁发资源访问控制信息具体为：

[0017] 将资源访问控制信息颁发给所述用户或所述云计算服务商服务器；其中，将资源访问控制信息颁发给所述用户时，所述用户向所述云计算服务商服务器发送所述资源访问控制信息。

[0018] 优选地，所述资源的相关信息包括所述业务提供商服务器为用户设置的用户编号信息、资源编号信息、所述业务提供商服务器标识信息。

[0019] 优选地，所述资源的相关信息还包括所述资源的有效时间信息；

[0020] 所述业务提供商服务器标识信息中包括所述业务提供商服务器的 IP 地址信息，以及，所述业务提供商服务器的名称信息、或提供通信端口标识信息、或硬件标识信息。

[0021] 优选地，云计算服务商服务器接收用户发送的资源访问请求之前，所述方法还包括：

[0022] 所述业务提供商服务器接收所述用户的注册请求，并为所述用户提供注册标识及访问密码；

[0023] 所述业务提供商服务器根据所述用户的标识信息对所述用户进行身份认证具体为：

[0024] 所述业务提供商服务器根据所述云计算服务商服务器提供的所述用户的标识信息，获取所述用户注册的 IP 地址信息，向所述用户发送登录接口，通过所述登录接口接收所述用户输入的注册标识及访问密码，并进行验证。

[0025] 优选地，云计算服务商服务器接收用户发送的资源访问请求之前，所述方法还包括：

[0026] 向所述用户提供访问资源的云计算服务商服务器的 IP 地址信息；

[0027] 所述用户根据所述云计算服务商服务器的 IP 地址信息向所述云计算服务商服务器发送资源访问请求。

[0028] 优选地，所述云计算资源包含云存储资源。

[0029] 一种云计算资源安全共享装置，包括接收单元、获取单元、第一发送单元、第一认证单元、第二发送单元、第二认证单元和提供单元，其中，

[0030] 接收单元，用于接收用户发送的资源访问请求，所述资源访问请求中携带待访问资源的相关信息；

[0031] 获取单元，用于根据所述待访问资源的相关信息获取待访问资源所属的业务提供

商服务器信息；

[0032] 第一发送单元，用于向待访问资源所属的业务提供商服务器发送认证请求；所述认证请求中携带有所述用户的标识信息；

[0033] 第一认证单元，用于根据所述用户的标识信息对所述用户进行身份认证；

[0034] 第二发送单元，用于在所述第一认证单元认证通过后向所述用户或所述云计算服务商服务器发送资源访问控制信息；

[0035] 所述用户通过所述第一发送单元再次向所述云计算服务商服务器发送资源访问请求，该资源访问请求中携带所述资源访问控制信息及资源的相关信息；

[0036] 第二认证单元，用于对所述资源访问控制信息进行认证；

[0037] 提供单元，用于在所述第二认证单元认证通过后向所述用户提供待访问资源。

[0038] 优选地，所述装置还包括：

[0039] 设置及提供单元，用于通过业务提供商服务器设置资源的访问权限，并向用户提供资源的相关信息。

[0040] 优选地，所述资源的相关信息包括所述业务提供商服务器为用户设置的用户编号信息、资源编号信息、所述业务提供商服务器标识信息。

[0041] 优选地，所述资源的相关信息还包括所述资源的有效时间信息；

[0042] 所述业务提供商服务器标识信息中包括所述业务提供商服务器的 IP 地址信息，以及，所述业务提供商服务器的名称信息、或提供通信端口标识信息、或硬件标识信息。

[0043] 一种云计算资源访问系统，包括业务提供商服务器和云计算服务商服务器；其中，

[0044] 业务提供商服务器，用于向资源所有者提供设置资源所有者的资源的访问权限；以及，接收到云计算服务商服务器发送的资源访问请求后，根据所述用户的标识信息对所述用户进行身份认证，并在认证通过后向所述用户发送资源访问控制信息；

[0045] 云计算服务商服务器，用于接收用户发送的资源访问请求，所述资源访问请求中携带待访问资源的相关信息；根据所述待访问资源的相关信息获取待访问资源所属的业务提供商服务器信息，并向待访问资源所属的业务提供商服务器发送认证请求；所述认证请求中携带有所述用户的标识信息；以及，对所述资源访问控制信息进行认证，并在认证通过后向所述用户提供待访问资源。

[0046] 优选地，所述业务提供商服务器将资源访问控制信息颁发给所述用户或所述云计算服务商服务器；其中，将资源访问控制信息颁发给所述用户时，由所述用户向所述云计算服务商服务器发送所述资源访问控制信息。

[0047] 本发明中，业务提供商服务器通过运用云计算服务商服务器，从而能向用户提供简单易行的资源访问手段，降低了系统设置的成本，同时，又对资源所有者的共享资源进行了安全保护。本发明有利于用户灵活访问共享资源，提高了共享资源访问的效率。

附图说明

[0048] 图 1 为本发明云计算资源访问系统的组成结构示意图；

[0049] 图 2 为本发明云计算资源安全共享方法的流程图；

[0050] 图 3 为本发明云计算资源安全共享装置的组成结构示意图。

具体实施方式

[0051] 本发明的基本思想为，资源所有者通过业务提供商服务器设置共享资源的访问权限，并向用户提供共享资源的相关信息；用户向云计算服务商服务器发送资源访问请求，资源访问请求中携带待访问资源的相关信息；云计算服务商服务器根据待访问资源的相关信息获取待访问资源所属的业务提供商服务器信息，并向待访问资源所属的业务提供商服务器发送认证请求；认证请求中携带有用户的标识信息；业务提供商服务器根据用户的标识信息对用户进行身份认证，并在认证通过后向用户发送资源访问控制信息；云计算服务商服务器对资源访问控制信息进行认证，并在认证通过后向用户提供待访问资源。

[0052] 图 1 为本发明云计算资源访问系统的组成结构示意图，如图 1 所示，本发明云计算资源访问系统包括业务提供商服务器和云计算服务商服务器；其中，

[0053] 业务提供商服务器，用于由资源所有者通过业务提供商服务器设置共享资源的访问权限；以及，接收到云计算服务商服务器发送的资源访问请求后，根据所述用户的标识信息对所述用户进行身份认证，并在认证通过后向所述用户发送资源访问控制信息；

[0054] 云计算服务商服务器，用于接收用户发送的资源访问请求，所述资源访问请求中携带待访问资源的相关信息；根据所述待访问资源的相关信息获取待访问资源所属的业务提供商服务器信息，并向待访问资源所属的业务提供商服务器发送认证请求；所述认证请求中携带有所述用户的标识信息；以及，对所述资源访问控制信息进行认证，并在认证通过后向所述用户提供待访问资源。

[0055] 本发明中，云计算资源包括云存储资源等。

[0056] 以下具体说明本发明用户如何通过云计算服务商访问业务提供商位于云计算服务商的共享资源。

[0057] 图 2 为本发明云计算资源安全共享方法的流程图，如图 2 所示，本发明云计算资源安全共享方法具体包括以下步骤：

[0058] 步骤 201，用户获取待访问资源的相关信息。

[0059] 具体的，在步骤 201 中，首先，资源所有者在客户端输入用户名和密码，登录到业务提供商服务器上。业务服务商服务器对资源所有者进行用户身份认证且通过后，向资源所有者发送资源信息列表，资源所有者选择待共享的资源信息，设置共享资源的访问权限，业务提供商服务器向资源所有者发送资源相关信息。这里，资源的相关信息包括所述业务提供商服务器为用户设置的用户编号信息、资源编号信息、所述业务提供商服务器标识信息，以及，所述资源的有效时间信息；其中，所述业务提供商服务器标识信息中包括所述业务提供商服务器的 IP 地址信息，以及，所述业务提供商服务器的名称信息、或提供通信端口标识信息、或硬件标识信息。

[0060] 这里，资源所有者将自身的资源信息上载到业务提供商服务器上，并在通过业务提供商服务器的身份认证（如通过用户名及访问密码的方式验证是否是合法资源使用者）后，将该资源所有者的共享资源信息提供给该资源所有者，供资源所有者对自身的共享资源的访问权限进行设置。并在设置完毕后，将所设置的共享资源的信息通知给待访问的用户，以方便用户对这些共享资源进行访问。

[0061] 具体的，资源所有者启动客户端程序输入用户名和用户密码。客户端程序以安全套接层 (SSL，Secure Sockets Layer) 协议登录认证服务器，发起会话，然后把用户名和对

应的密码发送给业务提供商服务器。

[0062] 登录密码可以由资源所有者在注册到业务提供商服务器时，由业务提供商服务器储存资源所有者注册时保存的用户名以及密码。此时，业务提供商服务器匹配该资源所有者录入的用户名和密码，如果没有匹配，结果返回错误。如果匹配，则返回业务提供商服务器的资源信息列表 resourcelist。

[0063] 资源所有者从资源列表中选择需要共享的资源信息，修改共享资源的访问控制权限，并将共享资源访问控制信息设为 V，业务提供商服务器云计算共享资源的访问控制信息 V。业务提供商服务器将共享资源信息票据 (ticket)，并返回给资源所有者。共享资源信息 ticket 可以由系统密钥进行加密后，再发送给资源所有者。

[0064] 本发明中，共享资源信息 ticket 包括用户编号 N_U，资源编号 N，业务提供商服务器 ID_S，业务提供商服务器的 IP_S，并且还可以包括用户可以使用此票据访问资源的时间值 time。

[0065] 如果以 K_S 表示系统间加密密钥，则业务提供商服务器发送给资源所有者的共享资源信息 ticket 可表示为：$\{N_U, N, ID_S, IP_S, time\}K_S$。

[0066] 本发明中，系统密钥是事先设定的，具体的设置方式与现有的密钥设置方式相同，由于不是实现本发明技术方案的重点，这里不再赘述。

[0067] 资源所有者获取 ticket 后，将获取的 ticket 发送给待访问共享资源的用户。资源所有者还将访问这些共享资源的云计算服务商服务器的 IP 地址 (IP_C) 发送给用户。

[0068] 用户接收资源信息 ticket 和云计算服务商服务器的 IP_C，并保存在本地以备份访问云计算服务商服务器，它们之间的会话结束。

[0069] 资源所有者客户端和业务提供商服务器之间会话流程利用参数可以表示如下：

[0070] 资源所有者通过 {username+password}SSL 向业务提供商服务器进行身份认证；

[0071] 业务提供商服务器向资源所有者提供资源列表：{resourcelist}SSL；

[0072] 资源所有者设置共享资源以及其访问权限 {N, V} 等信息，并向业务提供商服务器发送 {N, V}SSL；

[0073] 业务提供商服务器向资源所有者发送 {ticket}SSL；

[0074] 资源所有者向用户发送 $\{IP_C, ticket\}SSL$，其中，$ticket = \{N_U, N, ID_S, IP_S, time\}K_S$。

[0075] 其中，username 表示资源所有者的登录用户名，password 表示对应的密码，会话通过 SSL 协议传输。

[0076] 步骤 202，对用户进行身份认证，颁发资源访问控制信息 V。

[0077] 在步骤 202 中，用户采用 ticket 向云计算服务商服务器发送访问请求，云计算服务商服务器向业务提供商服务器发送请求，要求提供用户访问资源的身份认证和资源访问控制信息，业务提供商服务器对用户进行身份认证，颁发用户资源访问控制信息，并将资源访问控制信息发给用户。具体的，用户向资源信息委托方颁发的云计算服务商服务器 IP_C 发起访问，并发送资源访问 ticket。云计算服务商服务器利用系统密钥 (K_S) 解开票据 (ticket)，获得业务提供商服务器的 ID_S 和 IP_S，以及用户编号 N_U。云计算服务商服务器对业务提供商服务器的 ID_S 和 IP_S 进行认证，查找业务提供商服务器的注册信息。

[0078] 云计算服务商服务器向业务提供商服务器 IP_S 发起访问，向业务提供商服务器发

送用户身份认证和权限请求 P_V，云计算服务商服务器还将用户编号 N_U 发送给业务提供商服务器。这个请求信息可以用系统密钥 (K_S) 加密。

[0079] 业务提供商服务器运用系统密钥 (K_S) 解开信息，获取用户编号 N_U，根据编号查询得到用户的 IP_C，并向用户 IP_C 发起访问，要求用户提供身份认证和资源访问权限申请信息。

[0080] 用户向业务提供商服务器提供身份认证和资源访问权限申请。

[0081] 业务提供商服务器向用户客户端发送页面跳转 $action_i$，可以要求用户登录业务提供商服务器网站。此时，客户端可以跳转到业务提供商服务器网站。用户输入用户名 username 和密码 password，登录业务服务器网站。业务提供商服务器验证用户名 username 和密码 password，并和数据库用户的注册信息对照，如果一致，则允许用户访问。

[0082] 这里，用户在访问共享资源之前，也需到业务提供商服务器上进行注册，以方便访问共享资源。

[0083] 业务提供商服务器根据用户认证的结果，根据共享资源的访问控制信息，颁发共享资源访问控制信息 V，并将 V 发送给用户或发送给云计算服务商服务器。V 可以用系统密钥 K_S 加密。发送过程用密钥 (K_C) 加密。用户和业务提供商都可以运用用户在业务提供商注册的 usename 和 password 计算得到 K_C。如果将资源访问控制信息 V 发送给云计算服务商服务器，可以不进行加密。

[0084] 当将资源访问控制信息 V 发送给用户后，用户运用 K_c 解密信息，获取认证和资源权限值 V。

[0085] 云计算服务商服务器、业务提供商服务器、用户 (Client) 之间会话流程利用参数可以表述如下：

[0086] 用户向云计算服务商服务器发送 $\{ticket\}SSL$；

[0087] 云计算服务商服务器向业务提供商服务器发送 $\{\{N_U, P_V\}K_S\}SSL$；

[0088] 业务提供商服务器向用户提供认证的接口 $\{action_i\}SSL$；

[0089] 用户向业务提供商服务器发送 $\{username, password\}SSL$，进行身份认证；

[0090] 在身份认证通过后，业务提供商服务器向用户提供 $\{\{N, \{V\}K_S\}K_C\}SSL$。

[0091] 当然，如果业务提供商服务器将资源访问控制信息 V 发送给云计算服务商服务器，将直接发送。

[0092] 步骤 203，用户对相关共享资源进行访问。

[0093] 在步骤 203 中，用户运用 ticket，认证和资源访问权限值 V 向云计算服务商服务器发送请求，云计算服务商服务器资源访问控制信息 V，如果认证通过，云计算服务商服务器将共享资源发送给用户。具体的，用户运用 ticket 和认证和资源访问控制信息 V 向云计算服务商服务器发送资源访问请求。云计算服务商服务器运用系统密钥 (K_S) 解密信息，获取认证和资源访问权限值 V。云计算服务商服务器认证 V。如果认证通过，云计算服务商服务器向用户提供共享资源。

[0094] 图 3 为本发明云计算资源安全共享装置的组成结构示意图，如图 3 所示，本发明云计算资源安全共享装置包括设于用户终端中的设置及提供单元 30，设于云计算服务商服务器中的接收单元 31、获取单元 32、第一发送单元 33、第二认证单元 34 和提供单元 35，设于业务提供商服务器中的第一认证单元 36 和第二发送单元 37，其中，

[0095] 设置及提供单元 30，用于通过业务提供商服务器设置资源的访问权限，并向用户

提供资源的相关信息；

[0096] 接收单元 31，用于接收用户发送的资源访问请求，所述资源访问请求中携带待访问资源的相关信息；

[0097] 获取单元 32，用于根据所述待访问资源的相关信息获取待访问资源所属的业务提供商服务器信息；

[0098] 第一发送单元 33，用于向待访问资源所属的业务提供商服务器发送认证请求；所述认证请求中携带有所述用户的标识信息；

[0099] 第一认证单元 36，用于根据所述用户的标识信息对所述用户进行身份认证；

[0100] 第二发送单元 37，用于在所述第一认证单元认 36 证通过后向所述用户或发送资源访问控制信息；当将资源访问控制信息颁发给所述用户时，由所述用户向所述云计算服务商服务器发送所述资源访问控制信息。

[0101] 第二认证单元 34，用于对所述用户的资源访问控制信息进行认证；这里，当将资源访问控制信息发送给用户时，所述云计算服务商服务器在接收到用户发送的资源访问控制信息时，触发提供单元 35；或者，所述云计算服务商服务器在接收到所述业务提供商服务器发送的资源访问控制信息，触发提供单元 35。

[0102] 提供单元 35，用于在所述第二认证单元 34 认证通过后向所述用户提供待访问资源。

[0103] 上述资源的相关信息包括所述业务提供商服务器为用户设置的用户编号信息、资源编号信息、所述业务提供商服务器标识信息。上述资源的相关信息还包括所述资源的有效时间信息；

[0104] 所述业务提供商服务器标识信息中包括所述业务提供商服务器的 IP 地址信息，以及，所述业务提供商服务器的名称信息、或提供通信端口标识信息、或硬件标识信息。

[0105] 在图 3 所示的云计算资源安全共享装置的基础上，本发明云计算资源安全共享装置还包括：

[0106] 注册单元（未图示），设于用户终端中，用于向所述业务提供商服务器进行注册；

[0107] 第二提供单元（未图示），设于所述业务提供商服务器中，用于为所述用户提供注册标识及访问密码；

[0108] 第一认证单元 36 根据所述云计算服务商服务器提供的所述用户的标识信息，获取所述用户注册的 IP 地址信息，向所述用户发送登录接口，并通过所述登录接口接收所述用户输入的注册标识及访问密码，并进行验证。

[0109] 资源所有者向用户提供云计算服务商服务器的 IP 地址信息。

[0110] 用户终端进一步地，根据所述云计算服务商服务器的 IP 地址信息向所述云计算服务商服务器发送资源访问请求。

[0111] 本领域技术人员应当理解，本发明图 3 所示的云计算资源安全共享装置是为实现前述的云计算资源安全共享方法而设计的，上述各处理单元的实现功能可参照前述方法的相关描述而理解。图中的各处理单元的功能可通过运行于处理器上的程序而实现，也可通过具体的逻辑电路而实现。

[0112] 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

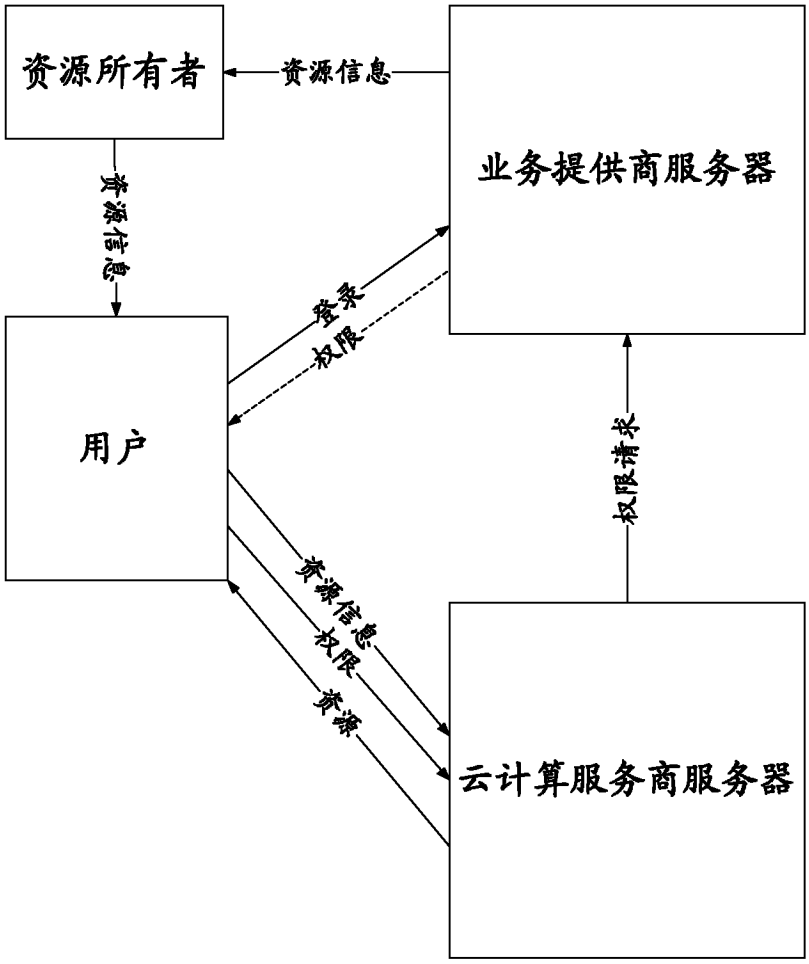

资源所有者
资源信息
业务提供商服务器
资源信息
登录
权限
用户
权限请求
资源信息
权限
资源
云计算服务商服务器

图 1

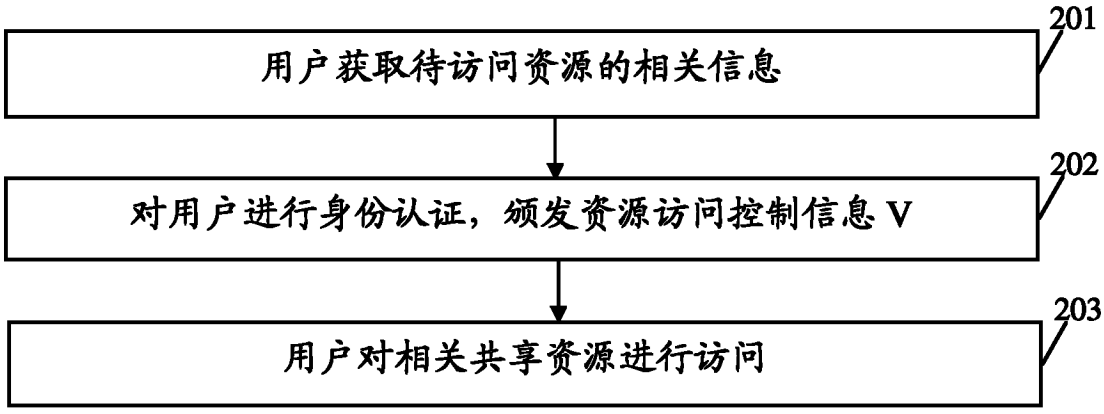

201
用户获取待访问资源的相关信息
202
对用户进行身份认证，颁发资源访问控制信息 V
203
用户对相关共享资源进行访问

图 2

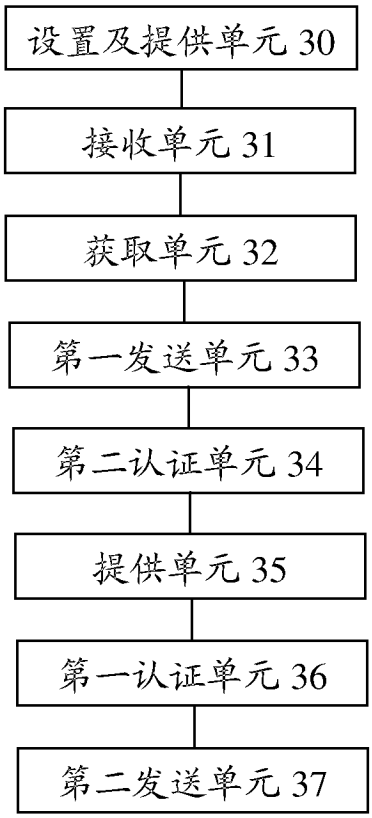

设置及提供单元 30
接收单元 31
获取单元 32
第一发送单元 33
第二认证单元 34
提供单元 35
第一认证单元 36
第二发送单元 37

图 3