(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 103237019 A
(43)申请公布日 2013.08.07

(21)申请号 201310116005.6

(22)申请日 2013.04.03

(71)申请人 中国科学院合肥物质科学研究院
地址 230031 安徽省合肥市科学岛智能所 1130 信箱

(72)发明人 崔超远 王儒敬 乌云

(74)专利代理机构 安徽省合肥新安专利代理有限责任公司 34101
代理人 赵晓薇

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/66(2006.01)

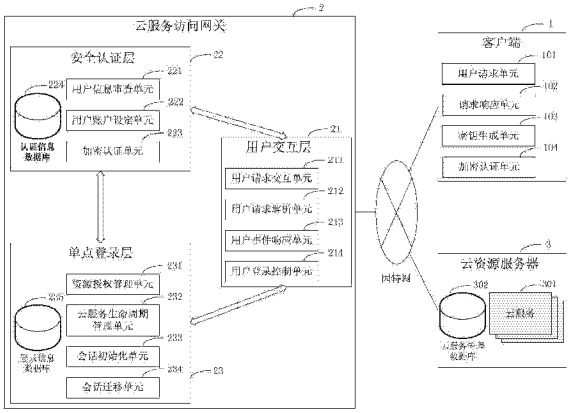
权利要求书3页 说明书10页 附图5页

(54)发明名称

一种云服务访问网关系统和方法

(57)摘要

本发明涉及一种云服务访问网关系统和方法，系统包括客户端、云服务访问网关、云资源服务器。所述云服务访问网关，包括用户交互层、安全认证层和单点登录层三个功能层，根据云服务访问网关系统安全和管理的需要，与客户端和云资源服务器进行频繁的数据传输和同步信息处理，实现加密认证和单点登录的协同动作。方法是客户端的用户通过请求交互、解析、信息审查、资源授权等会话初始化单元，实现用户登录云服务访问网关系统，登录认证；用户登录云服务访问网关，请求云服务；用户登录云服务访问网关，进行云服务迁移。本发明通过一次注册、一次登陆和多次访问的形式，简化了用户利用云服务的手续，也为云资源管理提供了较大的便利条件。



CN 103237019 A

1. 一种云服务访问网关系统，包括客户端（1）、云服务访问网关（2）、云资源服务器（3），其中：

所述客户端（1），通过因特网与各个云资源服务器（3）、云服务访问网关（2）建立连接，进行数据和事件交互；

所述云服务访问网关（2），包括至少一个网关服务器，用来接收和处理来自用户的请求和来自云计算中心的事件响应，并为二者建立数据和事件交互的通道；

所述云资源服务器（3），包括云服务（302）和云服务管理数据库（301），是部署在云计算中心的服务器，为云服务提供物理和逻辑依托；

其特征在于：

所述云服务访问网关（2），包括用户交互层（21）、安全认证层（22）和单点登录层（23）；

所述用户交互层（21），包括用户请求交互单元（211），用户请求解析单元（212），用户事件响应单元（213），用户登陆控制单元（214），用于和客户端（1）进行信息交互，进行用户注册、用户登录、账户修改、云服务定制、云服务访问、云服务前移；

所述安全认证层（22），包括用户信息审查单元（221），用户账户设定单元（222），加密认证单元（223），认证信息数据库（224），用于对用户登录信息进行合法性验证，安全认证层（22 ）账户生成后和单点登录层（23）的登录信息数据库进行账户信息同步；

所述单点登录层（23），包括资源授权管理单元（231），云服务生命周期管理单元（232），会话初始化单元（233），会话迁移单元（234），登录信息数据库（235），用于实现利用单一用户 ID 进行跨应用服务访问，单点登录层（23）将登陆状态的信息和账户修改信息同步到云资源服务器（3），同时将信息同步完成的结果通知安全认证层（22），单点登录层（23）处理服务定制请求、服务创建请求、服务迁移请求后，反馈通知到用户交互层（21）；

云服务访问网关（2）中的用户交互层（21）、安全认证层（22）和单点登录层（23）三个功能层，根据云服务访问网关系统安全和管理的需要，与客户端（1）和云资源服务器（3）进行频繁的数据传输和同步信息处理，实现加密认证和单点登录的协同动作。

2. 根据权利要求 1 所述一种云服务访问网关系统，其特征在于：所述客户端（1）包括硬件和软件，其中硬件为计算机，或为智能手机，或为触摸式电脑，硬件之间通过网络有线或无线连接。

3. 根据权利要求 1 所述一种用于云服务访问网关系统，其特征在于：所述云服务（302）包括至少一个用户，最终访问的是基础设施服务，或应用系统服务中的邮件系统服务、数据库系统服务。

4. 一种云服务访问网关系统的方法，其特征在于云服务访问网关系统的执行流程包括如下步骤：

用户请求交互单元（211），接收来自客户端（1）的请求，并将云服务访问网关的请求处理结果向客户端（1）回复；

用户请求解析单元（212），根据用户请求内容将请求分为账户注册请求、用户登录请求、账户修改请求、云服务定制请求、云服务访问请求和云服务迁移请求；

用户事件响应单元（213），将具体请求发送到安全认证层（22）或单点登录层（23）将请求回复通知给用户，请求交互单元（211）；

用户信息审查单元（221），接受并对具体请求信息或资源需求信息进行验证，确认这些

信息是否合法且符合云服务访问网关系统规范，加密认证单元（223）将加密的随机数作为加密认证请求，返回给用户交互层（21）；

用户账户设定单元（222），创建和修改用户账户及用户公钥，并将用户信息设置到认证信息数据库（224），

资源授权管理单元（231），为用户所请求资源进行授权，并将用户注册、登录、资源利用状况，设置到登录信息数据库（235）；

云服务生命周期管理单元（232），记录用户登陆系统的时刻及用户状态；

会话初始化单元（233），建立用户与应用服务的通信连接，会话迁移单元（234）针对用户对资源的利用变更，请求为用户重建通信连接，并保证用户无需登出云平台即进行会话迁移。

5. 根据权利要求 4 所述一种云服务访问网关系统的方法，其特征在于所述云服务访问网关系统的方法还包括：用户登录云服务访问网关（2），登录认证、用户登录云服务访问网关（2），请求云服务、用户登录云服务访问网关（2），进行云服务迁移；

用户登录云服务访问网关（2），登录认证的流程步骤为：

用户通过客户端（1）以用户 ID 向云服务访问网关（2）提交登录请求（A01）；

云服务访问网关（2）针对登录请求（A01）对用户身份合法性进行验证，首先云服务访问网关（2）生成随机数，并通过用户事先登录的公钥对该随机数加密，将加密结果作为加密认证请求（A02）发送给客户端（1）；

客户端（1）使用与事先登陆在网关上公钥相对应的私钥，将所述加密结果进行解密，并将解密结果作为加密认证回复（A03）返回到云服务访问网关（2）；

如果所述解密结果与所述随机数相同，云服务访问网关（2）认为登陆成功，向客户端（1）返回，登录认证成功（A04）；

用户登录云服务访问网关（2），请求云服务的流程步骤为：

登录云服务访问网关（2）后，用户通过客户端（1）发出云服务访问请求（A05）；

云服务访问网关（2）尝试与目标服务建立通信通道，向云服务发出会话创建请求（A06）；

云服务根据当前资源使用情况和服务定制情况，创建会话 ID、启动云服务并向云服务访问网关（2）回复会话创建成功（A07）；

云服务访问网关（2）将会话信息录入数据库后，向客户端（1）回复云服务访问成功（A08）；

客户端（1）的用户与云服务交互（A09）；

用户登录云服务访问网关（2），进行云服务迁移的流程步骤为：

当业务需求发生改变时，用户向云服务访问网关（2）发送云服务迁移请求（A10）；

云服务访问网关（2）负责注销当前云服务的会话连接，并向新的目标云服务发送会话迁移请求（A11）；

云服务根据当前资源使用情况和服务定制情况，创建会话 ID、启动云服务并向云服务访问网关（2）回复会话迁移成功（A12）；

云服务访问网关（2）将会话信息录入数据库后，向客户端（1）回复云服务迁移成功（A13）；

客户端(1)由此实现用户与云服务交互(A14)。

一种云服务访问网关系统和方法

技术领域

[0001] 本申请涉及云计算领域，特别涉及云环境下用户加密认证和资源单点登录的一种云服务访问网关系统和方法。

背景技术

[0002] 云计算涉及到多种计算机资源的交互和整合，如硬件基础设施、数据库系统以及各种应用服务系统等。这些资源在物理上异地分布、逻辑上单一呈现，不同资源之间存在不同的用户管理策略和调用接口，它们可以通过单独或联合的形式，为用户提供根据其业务需求变化的可选择服务。随着云环境下用户数量的增多，以及用户对异种云服务利用的增多，不仅需要在多台服务器上进行登录认证，还需要在多个云服务之间进行频繁的登录和登出操作。用户信息受到非法截获和破坏的可能性会增大，安全性得不到保障，还会导致系统访问的延迟。而针对多用户多目标服务的管理也因为用户 ID 的不统一变得越来越复杂，例如，同一用户以不同身份登录不同服务会为云资源计费造成困难。

[0003] 现有技术中，有通过加密认证来提高系统安全性的方法，也有通过单点登录来提高用户管理便利性的方法。

[0004] 2012 年，日本专利“特开 JP 2012-247858 号公报”，公开了云计算环境下基于密钥确认用户身份的认证方法和系统。该系统的客户端不需要保存密钥对中的私钥，而是根据用户密码在认证过程中即时生成，因此即使客户端设备丢失，也不会导致用于认证的私钥信息泄露。但是该方法必须一台密码管理服务器来生成密钥对，并将其中的公钥发送至另一台公钥管理服务器，如果公钥在发送过程中被破坏或恶意截获，将会导致整个认证系统无效，安全性也无从保证。特别是当用户由于业务需求要进行云服务迁移时，上述密钥生成、认证数据加密、认证数据解密的步骤必须要重复执行，会降低系统的响应速度，也为跨服务管理带来不便。随着云计算资源整合深度的提高和云服务种类的增多，用户的这种需求也会增强，因此迫切需要一种安全、通用、简洁的认证方法和认证系统。

[0005] 2013 年，日本专利“特开 JP 2013-8140 号公报”针对特开 JP 2012-247858 号公报情况，提出了一种只进行一次登陆就可以访问多个云服务的单点登陆认证系统。该系统和云服务所依托数据中心的认证系统协同工作，用户只需在终端进行一次认证登录，就可以实现业务需要时的服务迁移。但是该系统的主要缺点是，用户的首次登录是基于明文传输的密码认证，而非基于密文传输的密钥认证，因此安全性不高，为云服务的访问和迁移中带来安全隐患。

发明内容

[0006] 有鉴于此，本发明的目的是：提供一种云服务访问网关系统，该系统综合采用用户交互层、安全认证层、单点登录层和云服务访问技术，该三个功能层能够同时提高系统安全性、降低系统处理延迟、加强对用户的一元化管理，便于实现云服务间迁移。

[0007] 本发明的技术方案是：

[0008] 一种云服务访问网关系统，包括客户端、云服务访问网关、云资源服务器，其中：

[0009] 所述客户端，通过因特网与各个云资源服务器、云服务访问网关建立连接，进行数据和事件交互，该客户端包括硬件和软件，其中硬件为计算机，或为智能手机，或为触摸式电脑，硬件之间通过网络有线或无线连接；

[0010] 所述云服务访问网关，包括至少一个网关服务器，用来接收和处理来自用户的请求和来自云计算中心的事件响应，并为二者建立数据和事件交互的通道；

[0011] 所述云资源服务器，包括云服务和云服务管理数据库，是部署在云计算中心的服务器，为云服务提供物理和逻辑依托，该云服务包括至少一个用户最终访问的基础设施服务，或应用系统服务，如：邮件系统服务、数据库系统服务。

[0012] 特别是：所述云服务访问网关，包括用户交互层、安全认证层和单点登录层；

[0013] 所述用户交互层，包括用户请求交互单元，用户请求解析单元，用户事件响应单元，用户登陆控制单元，用于和客户端进行信息交互，进行用户注册、用户登录、账户修改、云服务定制、云服务访问、云服务前移；

[0014] 所述安全认证层，包括用户信息审查单元，用户账户设定单元，加密认证单元，认证信

[0015] 息数据库，用于对用户登录信息进行合法性验证，安全认证层在账户生成后和单点登录层的登录信息数据库进行账户信息同步；

[0016] 所述单点登录层，包括资源授权管理单元，云服务生命周期管理单元，会话初始化单元，会话迁移单元，登录信息数据库，用于实现利用单一用户 ID 进行跨应用服务访问，单点登录层将登陆状态的信息和账户修改信息同步到云资源服务器，同时将信息同步完成的结果通知安全认证层，单点登录层处理服务定制请求、服务创建请求、服务迁移请求后，反馈通知用户交互层；

[0017] 云服务访问网关中的用户交互层、安全认证层和单点登录层三个功能层，根据云服务访问网关系统安全和管理的需要，与客户端和云资源服务器进行频繁的数据传输和同步信息处理，实现加密认证和单点登录的协同动作。

[0018] 一种云服务访问网关系统的方法，特别是：云服务访问网关系统的执行流程包括如下步骤：

[0019] 用户请求交互单元，接收来自客户端的请求，并将云服务访问网关的请求处理结果向客户端回复；

[0020] 用户请求解析单元，根据用户请求内容将请求分为账户注册请求、用户登录请求、账户修改请求、云服务定制请求、云服务访问请求和云服务迁移请求；

[0021] 用户事件响应单元，将具体请求发送到安全认证层或单点登录层将请求回复通知给用户，请求交互单元；

[0022] 用户信息审查单元，接受并对具体请求信息或资源需求信息进行验证，确认这些信息是否合法且符合云服务访问网关系统规范，加密认证单元将加密的随机数作为加密认证请求，返回给用户交互层；

[0023] 用户账户设定单元，创建和修改用户账户及用户公钥，并将用户信息设置到认证信息数据库，

[0024] 资源授权管理单元，为用户所请求资源进行授权，并将用户注册、登录、资源利用

状况，设置到登录信息数据库；

[0025] 云服务生命周期管理单元，记录用户登陆系统的时刻及用户状态；

[0026] 会话初始化单元，建立用户与应用服务的通信连接，会话迁移单元针对用户对资源的利用变更，请求为用户重建通信连接，并保证用户无需登出云服务平台即进行会话迁移；

[0027] 所述云服务访问网关系统的方法还包括：用户登录云服务访问网关，登录认证、用户登录云服务访问网关，请求云服务、用户登录云服务访问网关，进行云服务迁移；

[0028] 用户登录云服务访问网关，登录认证的流程步骤为：

[0029] 用户通过客户端以用户 ID 向云服务访问网关提交登录请求；

[0030] 云服务访问网关针对登录请求对用户身份合法性进行验证，首先云服务访问网关生成随机数，并通过用户事先登录的公钥对该随机数加密，将加密结果作为加密认证请求发送给客户端；

[0031] 客户端使用与事先登陆在网关上公钥相对应的私钥，将所述加密结果进行解密，并将解密结果作为加密认证回复返回到云服务访问网关；

[0032] 如果所述解密结果与所述随机数相同，云服务访问网关认为登陆成功，向客户端返回，登录认证成功；

[0033] 用户登录云服务访问网关，请求云服务的流程步骤为：

[0034] 登录云服务访问网关后，用户通过客户端发出云服务访问请求；

[0035] 云服务访问网关尝试与目标服务建立通信通道，向云服务发出会话创建请求；

[0036] 云服务根据当前资源使用情况和服务定制情况，创建会话 ID、启动云服务并向云服务访问网关回复会话创建成功；

[0037] 云服务访问网关将会话信息录入云服务管理数据库后，向客户端回复云服务访问成功；

[0038] 客户端的用户与云服务交互；

[0039] 用户登录云服务访问网关，进行云服务迁移的流程步骤为：

[0040] 当业务需求发生改变时，用户向云服务访问网关发送云服务迁移请求；

[0041] 云服务访问网关负责注销当前云服务的会话连接，并向新的目标云服务发送会话迁移请求；

[0042] 云服务根据当前资源使用情况和服务定制情况，创建会话 ID、启动云服务并向云服务访问网关回复会话迁移成功；

[0043] 云服务访问网关将会话信息录入云服务管理数据库后，向客户端回复云服务迁移成功；

[0044] 客户端由此实现用户与云服务交互。

[0045] 有益效果

[0046] 目前现有技术中，云计算解决了分布式计算环境中软硬件资源的整合和利用模式，将物理上异地分布的资源以云服务的形式提供给用户，并能按照用户需求重新配置和组合这些资源。用户访问云服务时虽然无须考虑资源的物理依托，但用户的每一个操作都会导致数据在不同地理位置的多个物理服务器之间进行传输，这不仅增加了系统处理的延迟，也增加了用户信息被截获和盗取的可能。另一方面，业务需求发生变化时，用户会登出

当前云服务系统转而登录下一个目标服务，频繁的登录认证不仅降低系统的安全性，也为用户管理和云资源管理带来不便。

[0047] 本申请综合考虑这几方面的问题，提出云服务访问网关的系统和方法，以加密认证确保用户登录云服务的安全性，以单点登录确保用户利用云服务的便利性，避免认证信息和云服务管理信息在不同服务器之间的传输，防止系统处理延迟。从云服务提供方的角度来看，一次登陆认证和多次服务迁移的实现，用于解决分布式计算环境中跨服务器访问的安全问题和跨资源访问的一元化管理问题。

[0048] 对于本发明的有益效果分析如下：

[0049] 其一，相对于现有技术，本发明提供的云服务访问网关系统，包括客户端、云服务访问网关、云资源服务器，用来接收和处理来自客户端用户的请求和来自云计算中心云资源服务器的事件响应。作为建立数据和事件响应的交互通道，云服务访问网关上集成有安全认证层、单点登陆层和用户交互层；

[0050] 用户通过用户交互层进行用户注册、用户登录、账户修改、云服务定制、云服务访问、云服务前移；云服务访问网关接收到客户端登录请求后，客户端和安全认证层中的加密认证单元对用户身份合法性进行加密验证，安全认证层账户生成后和单点登录层的登录信息数据库进行账户信息同步；

[0051] 用户登录云服务访问网关后，提出云服务利用请求，单点登陆层根据用户预先定制的云服务内容，为用户进行服务连接；当用户业务需求发生改变而提出新的服务申请后，单点登录层将登陆状态的信息和账户修改信息同步到云资源服务器，同时将信息同步完成的结果通知安全认证层，单点登录层处理服务定制请求、服务创建请求、服务迁移请求后，反馈通知用户交互层；

[0052] 本发明具体实施方式中，在云服务访问网关系统图 4 到图 6 中，三个功能层因为安全和管理的需要，与客户端和云资源服务器进行频繁的数据传输和信息处理，实现加密认证和单点登录的协同动作，通过一次加密认证的登录，实现跨云服务的访问；云服务访问网关采用各层交互传输的技术手段，解决云服务访问网关系统的执行效率和安全性。

[0053] 其二，在一种云服务访问网关系统的方法中，通过密钥认证的方式对用户进行一次性身份验证，允许对所有被授权的云服务进行访问，同时允许用户根据自身业务需求的转变来重定向目标云服务。云服务访问网关能够保护用户与云计算中心云资源服务器之间数据传输的安全性和事件响应的简洁性。

[0054] 用户进行一次性身份验证过程中传输的数据，都是经过密钥加密的密文信息，而不是基于明文的用户密码信息，因此可以防止第三方对密码的恶意推断和盗取。而且，云服务访问网关对用户身份进行验证是基于用户密钥对，即经过密钥对中的公钥和私钥协同工作才能实现验证目的，即使网关服务器和客户端被恶意攻击，也不会由于公钥或私钥的泄漏而造成安全漏洞。

[0055] 云服务发生迁移的过程中，用户不需要对当前服务进行登出操作和对新的目标服务进行登入操作，只需根据初次加密认证登陆在网关数据库中的用户信息实现目标的转移。这样，通过采取统一的用户身份和密钥管理方法，既能实现单一用户 ID 跨不同应用系统的云服务访问和云服务切换，又能减少多个用户 ID 和多套密码系统造成的管理成本和安全漏洞。现有技术是安全了就繁琐，简单了就不安全，而本发明是既简单又安全。

[0056] 云服务有别于其他应用服务系统的本质区别是，云服务是一种可度量的服务模式。云服务提供方通过量化用户使用的云资源进行计费，从而达到阻止用户滥用资源和优化整体资源配置的目的。面向海量云用户，如何对云计算中心成千上万种异构异质的云服务进行量化在技术上和管理上都有难度，就连单一用户以多种身份访问云服务的度量也会为管理带来很大的系统消耗。而本发明提供的云服务访问网关系统，通过一次注册、一次登陆和多次访问的形式，不仅简化了用户利用云服务的手续，也便于系统进行多种云服务的叠加计费，为云资源管理提供极大的先决便利条件。

附图说明

[0057] 图 1 是云服务访问网关的系统结构示意图；

[0058] 图 2 是云服务访问网关的系统功能示意图；

[0059] 图 3 是云服务访问网关系统的流程示意图；

[0060] 图 4 是云服务访问网关中用户交互层的处理流程示意图；

[0061] 图 5 是云服务访问网关中安全认证层的处理流程示意图；

[0062] 图 6 是云服务访问网关中单点登录层的处理流程示意图。

具体实施方式

[0063] 下文将结合附图和实施例作进一步解释。

[0064] 图 1 为云服务访问网关的系统结构示意图，在图 1 中：客户端为 1、云服务访问网关为 2、云资源服务器为 3。

[0065] 客户端 1 提供云服务访问网关 2 的用户交互接口，包括基于浏览器的图形用户界面和基于命令行的字符用户界面，用于客户端 1 的用户向云服务访问网关 2 发送请求并接受响应；

[0066] 因特网提供客户端 1 和云服务访问网关 2 的连接，是客户端 1 所在的局域网，可以是有线网或无线网；云服务访问网关 2 接收并处理来自客户端 1 的请求和来自云资源服务器 3 的响应，为用户和云服务建立事件处理通道；因特网还连接云服务访问网关 2 和云资源服务器 3，位于云服务访问网关 2 和云资源服务器 3 所在的广域网，可以是有线网或无线网；

[0067] 云资源服务器 3 是部署在云计算中心的服务器，为云服务提供物理和逻辑依托；云资源服务器 3 包括云服务，云服务是用户最终访问的应用系统，如：CPU、硬盘、网络等基础设施服务、邮件系统服务、数据库系统服务等。客户端 1 与各个云服务通过云服务访问网关 2 建立连接，进行数据和事件响应交互。

[0068] 图 2 是云服务访问网关的系统功能示意图；在图 2 中：云服务访问网关的系统的主体是云服务访问网关 2，同时需要客户端 1 和云资源服务器 3 协同完成云服务访问过程。

[0069] 客户端 1 中，用户请求单元 101，用于构造基于浏览器图形用户界面或基于命令行的字符用户界面，向云服务网关提交用户登录和利用云服务的请求；请求响应单元 102，基于浏览器或命令行接收来自云服务网关的请求处理结果和下一步操作的通知；密钥生成单元 103，用于生成用户加密认证过程中的密钥对；加密认证单元 104 用于在加密认证过程中对网关返回的加密信息进行解密操作，密钥对生成和信息加密和解密都采用公开的算法。

[0070] 云服务访问网关 2 包括三个功能层，即用户交互层 21、安全认证层 22 和单点登录层 23。

[0071] 用户交互层 21，用于和客户端 1 进行信息交互。其中，用户请求交互单元 211，用于接收来自客户端 1 的请求，并将云服务网关请求处理结果向客户端 1 回复；用户请求解析单元 212 根据用户请求内容将请求分为账户注册请求、用户登录请求、账户修改请求、云服务定制请求、云服务访问请求和云服务迁移请求；用户事件响应单元 213，用于将具体请求发送到安全认证层 22 或单点登录层 23 等待处理，然后将请求回复通知给用户交互层中的用户请求交互单元 211；用户登陆控制单元 214 在用户登陆、账户修改以及云服务访问过程中，对系统无操作时间、密码错误次数、登陆 IP 等内容进行限制。

[0072] 安全认证层 22，用于对用户登录信息进行合法性验证。其中，用户信息审查单元 221，用于对具体请求信息，如账户名、用户密钥、用户身份、住址、联系方式以及资源需求等进行验证，确认这些信息是否合法且符合系统规范；用户账户设定单元 222，用于创建和修改用户账户及用户公钥，并将用户信息设置到认证信息数据库 224，以利于统一用户 ID 和公钥的管理；加密认证单元 223，用于将加密的随机数作为加密认证请求返回给用户交互层。

[0073] 单点登录层 23，用于实现利用单一用户 ID 进行跨应用服务访问。其中，资源授权管理单元 231，为用户所请求资源进行授权，并将用户注册、登录、资源利用状况设置到登录信息数据库 235；云服务生命周期管理单元 232，用来记录用户登陆系统的时刻及用户状态；会话初始化单元 233，用于建立用户与应用服务的通信连接；会话迁移单元 234，针对用户对资源的利用变更，请求为用户重建通信连接，并保证用户无需登出云平台就可进行会话迁移，为平台管理提供便利。

[0074] 所述云资源服务器 3，用于提供云服务 301 和云服务管理数据库 302。云资源服务器 3 在图 2 中只有一个图例，但实际上有很多这样的服务器部署在云计算中心，通过网络和网关连接对外提供服务。

[0075] 云服务访问网关系统中，云服务访问网关 2 和云资源服务器 3 的软件环境及功能层都适用于计算机及其外设配件，客户端 1 可以是计算机、智能手机和触摸式电脑等设备，这些硬件通过网络相互连接。

[0076] 云服务访问网关系统是由计算机及外设配件等硬件和控制这些硬件的软件所构成。

[0077] 所述硬件中，包括：信息输入装置、信息存储装置、信息处理装置、信息传输装置和信息表示装置。信息输入装置由计算机、鼠标、键盘组成，也可以是触摸式的智能手机或平板电脑，其中客户端 1 用于为用户提供输入终端；信息存储装置可以是内存、硬盘、光盘等设备，用来存放所述云服务访问网关系统的通信数据；信息处理装置是具有计算功能的 CPU；信息传输装置是各种有线网和无线网，及其对应的信息传输接口；信息表示装置是液晶显示器或触摸是液晶平板。

[0078] 所述软件是由控制这些硬件的计算机程序和数据组成。软件可以通过信息存储装置来保存，通过信息处理装置来激活执行，也可以通过信息传输装置对外进行发布。

[0079] 图 3 是云服务访问网关系统的流程示意图；在图 3 中：

[0080] 客户端 1 在访问云服务时，通过云服务访问网关 2 进行数据传输和信号处理，最终

与云服务建立信息通信通道。该云服务访问网关系统的方法流程如下：

[0081] 步骤 A01 到步骤 A04 为用户登录云服务访问网关 2 的过程；

[0082] 步骤 A05 到步骤 A09 为用户通过云服务访问网关 2 登录所请求云服务的过程；

[0083] 步骤 A10 到步骤 A14 为用户进行云服务迁移的过程。

[0084] 具体而言，用户通过客户端 1 以用户 ID 向云服务访问网关 2 提交登录请求 A01；云服务访问网关针对登录请求 A01 对用户身份合法性进行验证，首先云服务访问网关 2 生成随机数，并通过用户事先登录的公钥对该随机数加密，然后将加密结果作为加密认证请求 A02 发送给客户端 1；客户端 1 使用与事先登陆在云服务访问网关 2 上公钥相对应的私钥将所述加密结果进行解密，并将解密结果作为加密认证回复 A03 返回到云服务访问网关 2；如果解密结果与随机数相同，云服务访问网关 2 认为登陆成功，向客户端 1 返回登录认证成功 A04。

[0085] 登录云服务访问网关 2 后，用户通过客户端 1 发出云服务访问请求 A05；云服务访问网关 2 尝试与目标服务建立通信通道，向云服务 301 发出会话创建请求 A06；云服务 301 根据当前资源使用情况和服务定制情况，创建会话 ID、启动云服务 301 并向云服务访问网关 2 回复会话创建成功 A07；云服务访问网关 2 将会话信息录入数据库后，向客户端 1 回复云服务访问成功 A08；客户端 1 由此可以实现用户与云服务交互 A09。

[0086] 当业务需求发生改变时，用户向云服务访问网关 2 发送云服务迁移请求 A10；云服务访问网关 2 负责注销当前云服务的会话连接，并向新的目标云服务发送会话迁移请求 A11；云服务 301 根据当前资源使用情况和服务定制情况，创建会话 ID、启动云服务 301 并向云服务访问网关 2 回复会话迁移成功 A12；云服务访问网关 2 将会话信息录入数据库后，向客户端 1 回复云服务迁移成功 A13；客户端 1 由此可以实现用户与云服务交互 A14。

[0087] 图 4 是云服务访问网关中用户交互层的处理流程示意图；在图 4 中：

[0088] 用户交互层 21 把用户请求分为账户注册、用户登录、账户修改、云服务定制、云服务访问、云服务前移等具体用户事件。以下分别对各个用户事件的实施方式加以说明。

[0089] 步骤 B01 到步骤 B13，是账户注册事件的处理流程。用户请求交互单元 211 收到来自客户端 1 的用户请求 B01 后，通过用户请求解析单元 212 进行解析，判断用户事件为账户注册，然后由用户事件响应单元 213 提取注册信息并将其以账户注册请求 B04 发送给安全认证层 22。安全认证层 22 进行注册信息审查 B05，然后以认证密钥请求 B06 的形式通过用户请求交互单元 211 向用户发出密钥请求 B07。客户端 1 通过密钥生成 B08 产生密钥对，并将其中的公钥进行公钥发送 B09。用户请求交互单元 211 收到公钥后，向安全认证层 22 发出公钥注册请求，当用户 ID、用户公钥以及用户其他信息录入数据库完成后，收到注册成功应答 B12，然后向客户端 1 返回请求成功应答 B13 的通知。至此，用户注册完成。

[0090] 步骤 B14 到步骤 B32，是用户登录事件的处理流程。步骤 B14 到步骤 B16 是用户交互层 21 接收并解析用户请求；步骤 B17 到步骤 B19 是向用户登录控制单元 214 进行登录目标确认；步骤 B20 是向安全认证层 22 发出用户登录请求 B20；步骤 B21 到步骤 B25 是进行加密认证；步骤 B26 到步骤 B28 是进行登录次数确认；步骤 B29 到步骤 B31 是安全认证层 22 进行登录认证并做出回复。步骤 B32 通过客户端通知用户登录请求成功应答。

[0091] 步骤 B33 到步骤 B42，是账户信息修改事件的处理流程。这个过程是建立在步骤 B14 到步骤 B32 的用户登录基础之上的，即用户登录云服务网关之后才能进行以下操作。步

骤 B33 到步骤 B35 是用户交互层 21 接收并解析用户请求；步骤 B36 到步骤 B38 是向用户登录控制单元 214 进行登录时间确认，以防止登录后长时间无操作；步骤 B39 到步骤 B41 是安全认证层 22 进行账户信息修改并做出回复。步骤 B42 通过客户端 1 通知用户账户修改成功应答。

[0092] 步骤 B43 到步骤 B52，是云服务定制事件的处理流程。这个过程是建立在步骤 B14 到步骤 B32 的用户登录基础之上的，即用户登录云服务网关之后才能进行以下操作。步骤 B43 到步骤 B45 是用户交互层 21 接收并解析用户请求；步骤 B46 到步骤 B48 是向用户登录控制单元 214 进行登录时间确认，以防止登录后长时间无操作；步骤 B49 是用户事件响应单元 213 向单点登录层 23 发出服务定制请求，以确定将来要使用的目标资源；步骤 B50 是单点登录层 23 进行云服务信息授权并做出定制成功应答 B51。步骤 B52 通过客户端 1 通知用户云服务定制请求成功应答。

[0093] 步骤 B53 到步骤 B61，是云服务访问事件的处理流程。这个过程是建立在步骤 B14 到步骤 B32 的用户登录基础之上的，即用户登录云服务网关之后才能进行以下操作。步骤 B53 到步骤 B55 是用户交互层 21 接收并解析用户请求；步骤 B56 到步骤 B58 是向用户登录控制单元 214 进行登录时间确认，以防止登录后长时间无操作；步骤 B59 到步骤 B60 是向单点登录层 23 发出服务访问请求并得到访问成功应答。步骤 B61 通过客户端 1 通知用户云服务访问请求成功应答。

[0094] 步骤 B62 到步骤 B70，是云服务迁移事件的处理流程。这个过程是建立在步骤 B53 到步骤 B61 的云服务访问基础之上的，即用户已经登录某个云服务之后才能进行以下操作。步骤 B62 到步骤 B64 是用户交互层 21 接收并解析用户请求；步骤 B65 到步骤 B67 是向用户登录控制单元 214 进行登录时间确认，以防止登录后长时间无操作；步骤 B68 到步骤 B69 是向单点登录层 23 发出服务迁移请求并得到迁移成功应答。步骤 B70 通过客户端 1 通知用户云服务迁移请求成功应答。

[0095] 图 5 是云服务访问网关中安全认证层的处理流程示意图；在图 5 中：

[0096] 安全认证层 22 对用户交互层 21 传递来的用户事件进行处理。以下分别对各个用户请求的实现方式加以说明。

[0097] 步骤 C01 到步骤 C10，是账户注册请求的处理流程。用户信息审查单元 221 收到账户注册请求 C01 后，执行步骤 C02，进行注册信息审查，对用户的账户名、用户 ID、用户身份、住址、联系方式进行验证，确认这些信息是否合法且符合系统规范，如果合格则要求用户提供用于加密认证的公钥，于是向用户交互层 21 发出认证密钥请求 C03；用户信息审查单元 221 收到是用户交互层 21 回复的公钥注册请求 C04，向用户账户设定单元 222 发出账户创建请求 C05；步骤 C06 是用户账户设定单元 222 进行账户创建并将公钥设置到认证信息数据库；步骤 C07 到步骤 C09，在账户生成后和单点登录层 23 的登录信息数据库进行账户信息同步，由此实现加密认证和单点登录的协同动作；至此，账户创建和账户信息同已完成，用户账户设定单元 222 向用户交互层 21 回复注册成功应答 C10。

[0098] 步骤 C11 到步骤 C23，是用户登录请求的处理流程。步骤 C11 到步骤 C23 是用户信息审查单元 221 对用户登录请求进行登录信息审查，并向加密认证单元 223 发出登录认证请求；步骤 C14 到步骤 C19 是加密认证单元 223 对用户身份合法性的最终验证，如果失败，再次发出密钥认证请求。在登录控制许可的范围内，直到该操作成功。然后，步骤 C20 到步

骤 C22 向单点登录层 23 发布登陆成功信息，云服务访问网关系统由此获得跨云服务访问的信息联动；之后，步骤 C23 向用户交互层 21 回复登录成功应答。

[0099] 步骤 C24 到步骤 C30，是账户修改请求的处理流程。这个过程是建立在步骤 C11 到步骤 C23 的用户登录成功的基础之上，即用户登录云服务网关之后才能进行以下操作。步骤 C24 到步骤 C26 是对待修改账户信息进行审查并发出修改请求；步骤 C27 是用户账户设定单元 222 对账户信息修改或对公钥重新设置；步骤 C28 到步骤 C30 向单点登录层 23 发布账户修改信息；最后，步骤 C31 向用户交互层 21 回复修改成功应答。

[0100] 图 6 是云服务访问网关中单点登录层的处理流程示意图。在图 6 中：

[0101] 单点登录层 23 对用户交互层 21 和安全认证层 22 传递来的信息进行处理。以下分别对各个请求的实施方式加以说明。

[0102] 步骤 D01 到步骤 D06，是注册信息发布的处理流程。单点登录层 23 收到注册信息发布 D01 的通知后，资源授权管理单元 231 执行步骤 D02，将注册信息登记到登录信息数据库，同时向云资源服务器 3 发出注册信息同步 D03；云资源服务器 3 执行步骤 D04，将账号注册信息登记到云服务管理数据库，由此获得有资格进行云服务访问的账户信息；资源授权管理单元 231 收到云资源管理服务器 3 回复的信息同步应答 D05，然后通知安全认证层 22 同步完成，发出信息同步应答 D06。

[0103] 步骤 D07 到步骤 D12，是登录状态发布的处理流程。步骤 D07 到步骤 D08 将登录状态登记到由单点登录层 23 管理的登录信息数据库；步骤 D09 到步骤 D11 将登陆状态的信息同步到云资源服务器 3；步骤 D12 将信息同步完成的结果通知安全认证层 22。

[0104] 步骤 D13 到步骤 D18，是修改信息发布的处理流程。这个过程是建立在用户事先登录的基础上。步骤 D13 到步骤 D14 将账户修改信息登记到由单点登录层 23 管理的登录信息数据库；步骤 D15 到步骤 D17 将账户修改信息同步到云资源服务器 3；步骤 D18 将信息同步完成的结果通知安全认证层 22。

[0105] 步骤 D19 到步骤 D26，是服务定制请求的处理流程。这个过程建立在用户事先登录云服务访问网关的基础上。资源授权管理单元 231 收到服务定制请求 D19 之后，向云资源服务器 3 发出资源状态查询 D20，确认当前资源使用情况；当收到状态查询应答 D21，获得所请求资源的可用通知后，执行授权信息登录 D22，将资源信息和用户信息登记到由单点登录层 23 管理的登录信息数据库；然后向云资源服务器 3 发出授权信息同步 D23；云资源服务器 3 执行授权信息同步 D24，由此获得有资格进行云服务访问的账户信息；资源授权管理单元 231 收到信息同步应答 D25，确定同步完成，然后回复用户交互层 21 定制成功应答 D26，通知其云服务定制完成。

[0106] 步骤 D27 到步骤 D36，是服务访问请求的处理流程。这个过程建立在用户事先登录的基础上。步骤 D27 到步骤 D29 对所请求的服务进行授权检查，如果在授权范围内，则向服务生命周期管理单元 232 发出服务创建请求；步骤 D30 到步骤 D35 是会话初始化单元 233 向云资源服务器 3 请求会话创建，如果创建成，将会话信息回复给服务生命周期管理单元 232，便于它对该会话进行管理；最后，步骤 D36 通知用户交互层 21 云服务访问成功应答。

[0107] 步骤 D37 到步骤 D53，是服务迁移请求的处理流程。这个过程建立步骤 D19 到步骤 D36 的云服务访问基础之上的，即用户已经登录某个云服务之后才能进行以下操作。步骤 D37 到步骤 D39 对所打算迁移的云服务进行授权检查，如果在授权范围内，则向服务生命

周期管理单元 232 发出服务迁移请求；步骤 D40 到步骤 D46 将进行中的会话注销；步骤 D47 到步骤 D51 执行新的会话创建；步骤 D52 到步骤 D53 通知用户交互层 21 云服务迁移成功应答。

[0108] 图 4 到图 6 所述的云服务访问网关系统中，三个功能层因为安全和管理的需要，进行频繁的数据传输和信息处理。将三个层都集成到云服务访问网关中，可以有效降低系统处理延迟。因此，本系统可以通过一次加密认证的登录，实现跨云服务的访问。

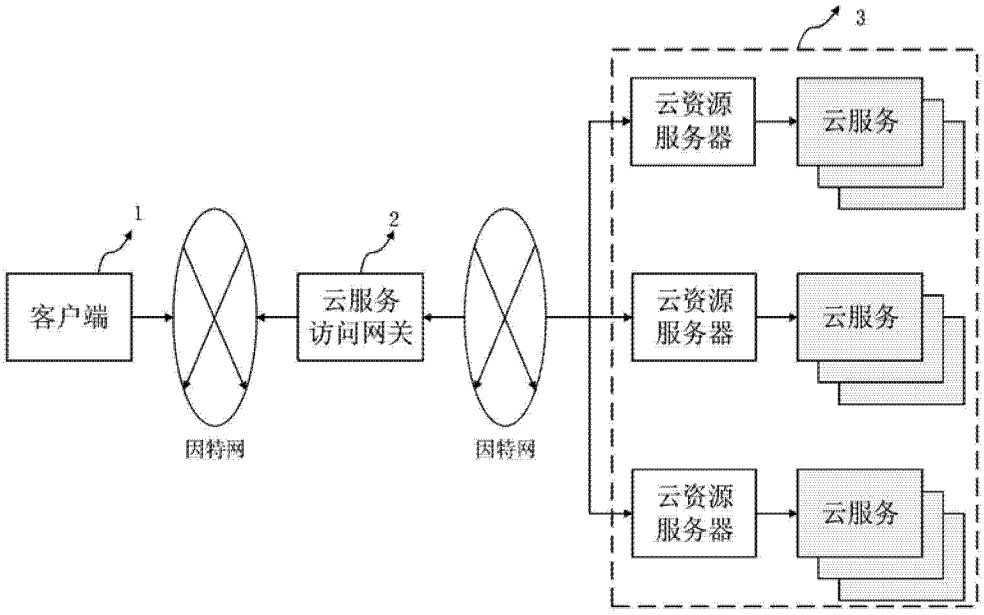

3
云资源服务器
云服务
1
客户端
2
云服务访问网关
因特网
因特网
云资源服务器
云服务
云资源服务器
云服务

图 1

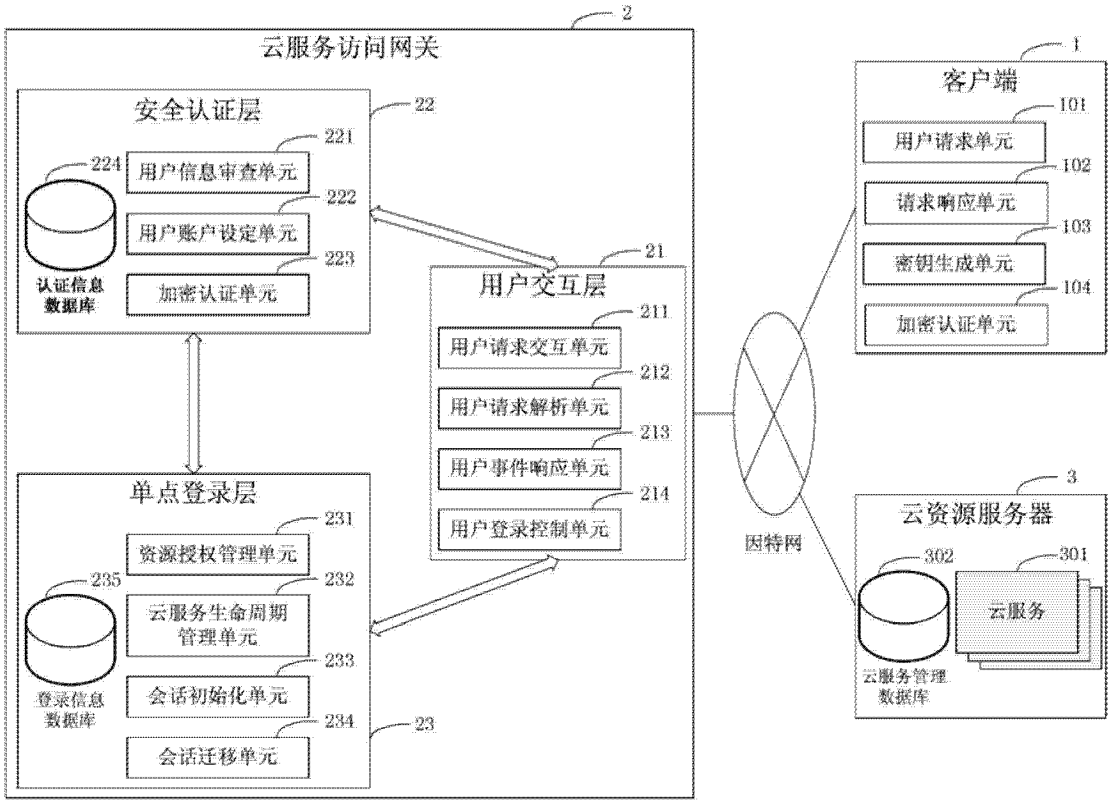

2
云服务访问网关
安全认证层
22
221
用户信息审查单元
224
222
用户账户设定单元
223
加密认证单元
认证信息数据库
21
用户交互层
211
用户请求交互单元
212
用户请求解析单元
213
用户事件响应单元
214
用户登录控制单元
单点登录层
231
资源授权管理单元
235
232
云服务生命周期管理单元
233
会话初始化单元
234
会话迁移单元
23
登录信息数据库
因特网
1
客户端
101
用户请求单元
102
请求响应单元
103
密钥生成单元
104
加密认证单元
3
云资源服务器
302
301
云服务
云服务管理数据库

图 2

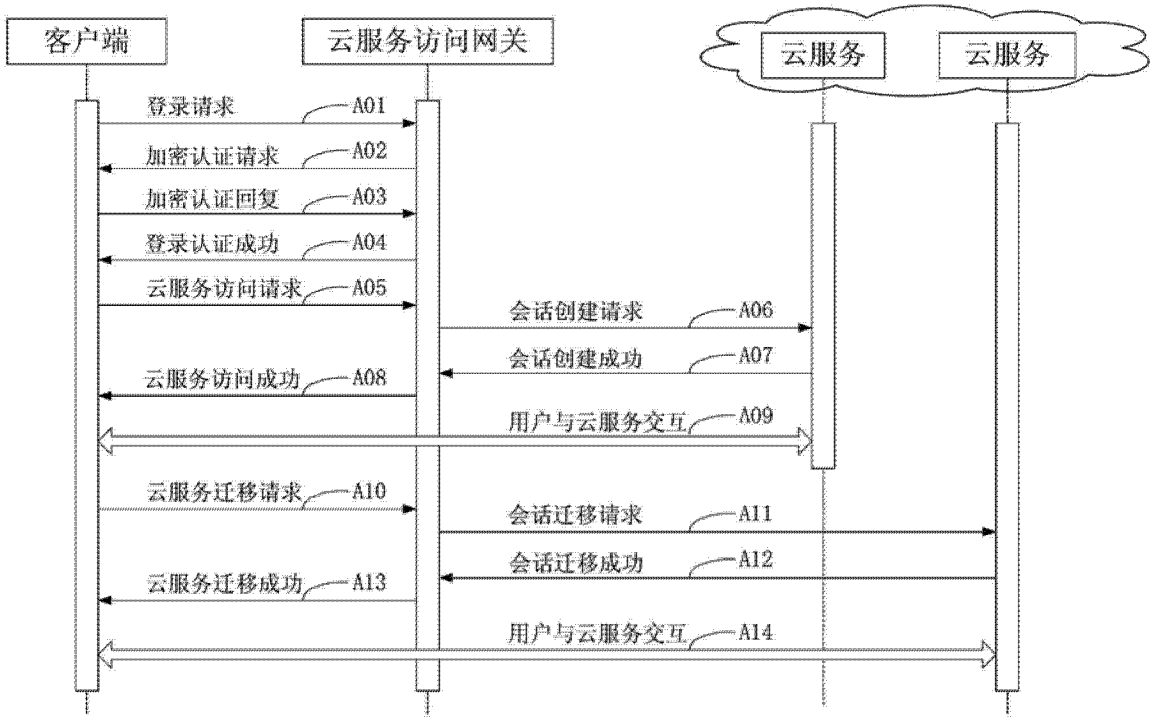

客户端
云服务访问网关
云服务
云服务
登录请求
A01
加密认证请求
A02
加密认证回复
A03
登录认证成功
A04
云服务访问请求
A05
会话创建请求
A06
会话创建成功
A07
云服务访问成功
A08
用户与云服务交互
A09
云服务迁移请求
A10
会话迁移请求
A11
会话迁移成功
A12
云服务迁移成功
A13
用户与云服务交互
A14

图 3

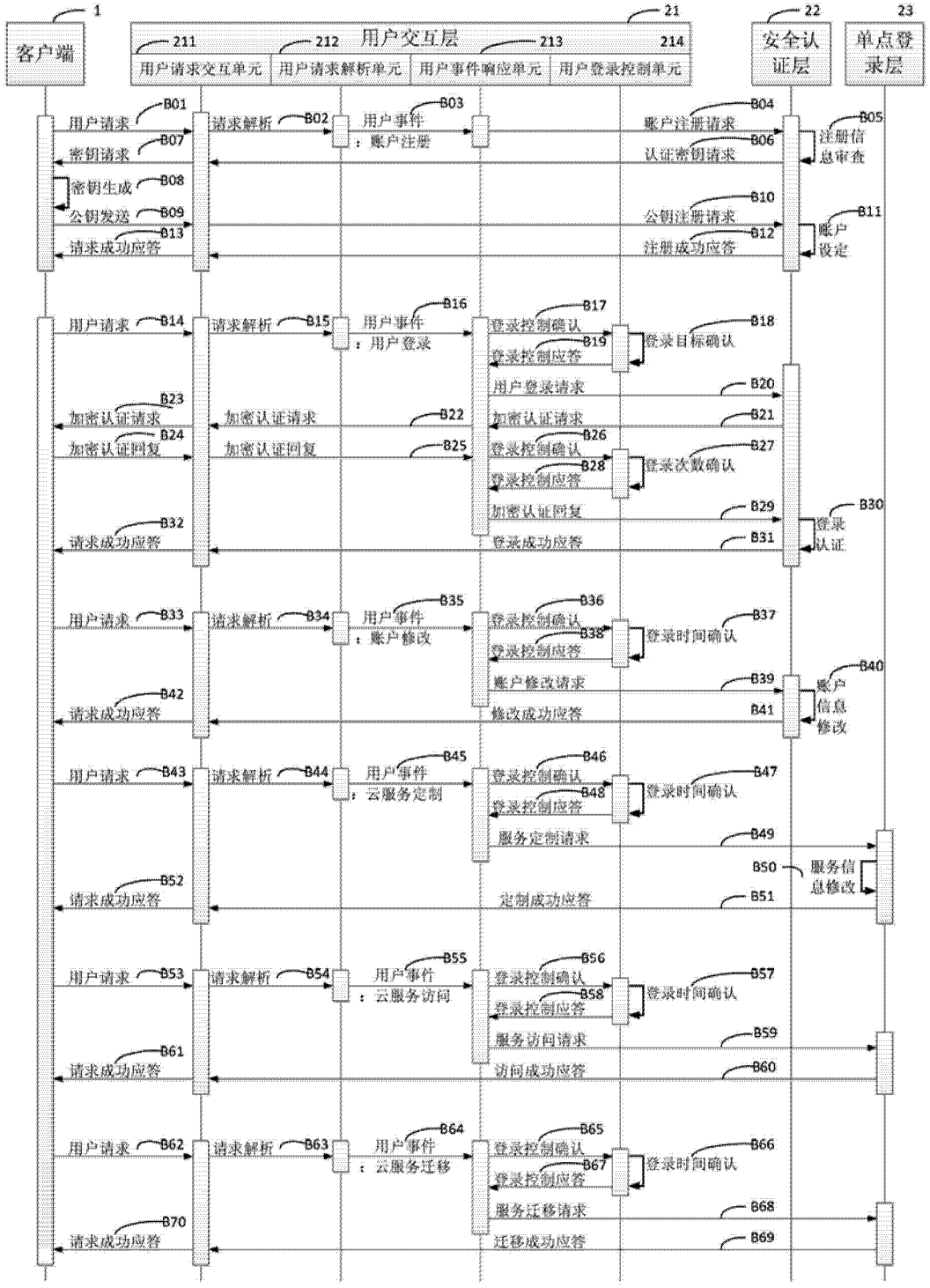

1
客户端
21
用户交互层
211
用户请求交互单元
212
用户请求解析单元
213
用户事件响应单元
214
用户登录控制单元
22
安全认证层
23
单点登录层
B01 用户请求
B02 请求解析
B03 用户事件：账户注册
B04 账户注册请求
B05 注册信息审查
B06 认证密钥请求
B07 密钥请求
B08 密钥生成
B09 公钥发送
B10 公钥注册请求
B11 账户设定
B12 注册成功应答
B13 请求成功应答
B14 用户请求
B15 请求解析
B16 用户事件：用户登录
B17 登录控制确认
B18 登录目标确认
B19 登录控制应答
B20 用户登录请求
B21 加密认证请求
B22 加密认证请求
B23 加密认证请求
B24 加密认证回复
B25 加密认证回复
B26 登录控制确认
B27 登录次数确认
B28 登录控制应答
B29 加密认证回复
B30 登录认证
B31 登录成功应答
B32 请求成功应答
B33 用户请求
B34 请求解析
B35 用户事件：账户修改
B36 登录控制确认
B37 登录时间确认
B38 登录控制应答
B39 账户修改请求
B40 账户信息修改
B41 修改成功应答
B42 请求成功应答
B43 用户请求
B44 请求解析
B45 用户事件：云服务定制
B46 登录控制确认
B47 登录时间确认
B48 登录控制应答
B49 服务定制请求
B50 服务信息修改
B51 定制成功应答
B52 请求成功应答
B53 用户请求
B54 请求解析
B55 用户事件：云服务访问
B56 登录控制确认
B57 登录时间确认
B58 登录控制应答
B59 服务访问请求
B60 访问成功应答
B61 请求成功应答
B62 用户请求
B63 请求解析
B64 用户事件：云服务迁移
B65 登录控制确认
B66 登录时间确认
B67 登录控制应答
B68 服务迁移请求
B69 迁移成功应答
B70 请求成功应答

图 4

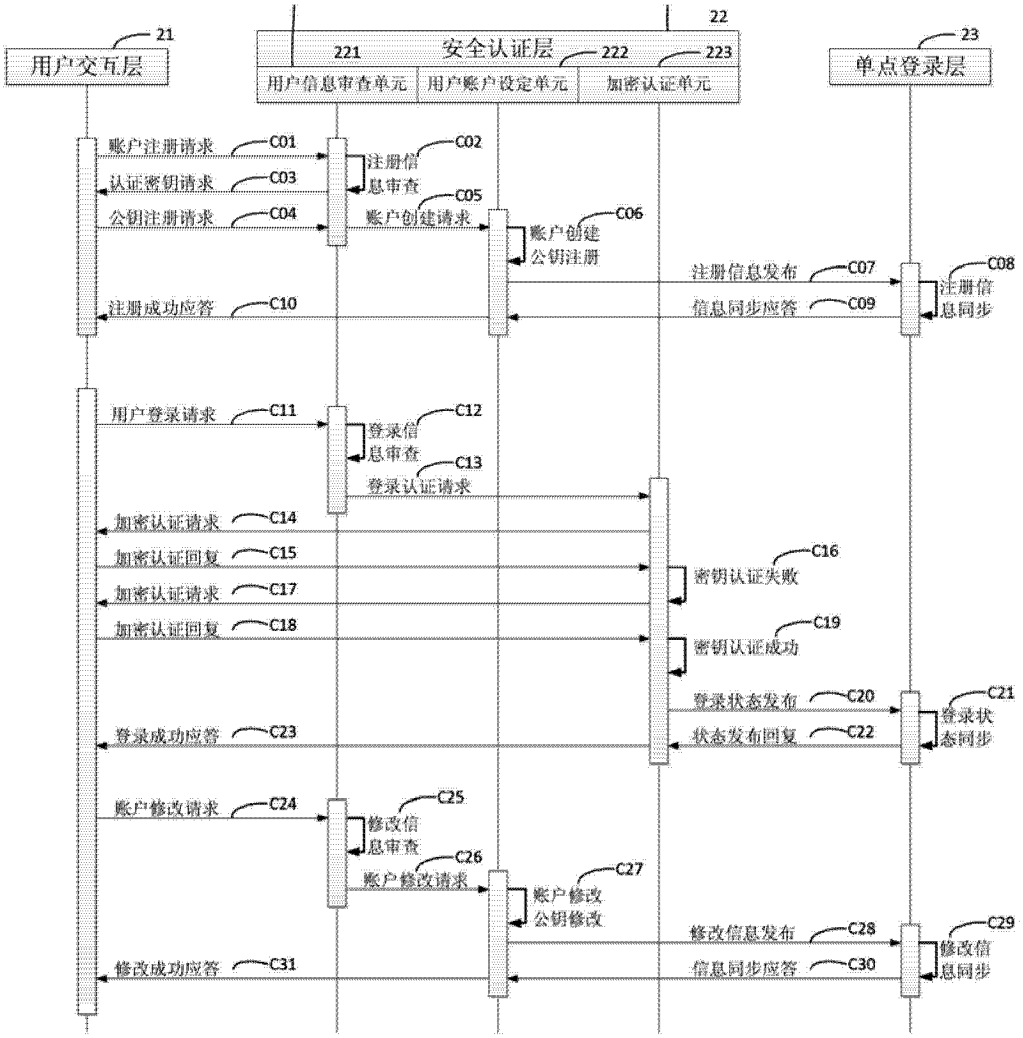

21
用户交互层
22
安全认证层
221
用户信息审查单元
222
用户账户设定单元
223
加密认证单元
23
单点登录层
账户注册请求 C01
注册信息审查 C02
认证密钥请求 C03
公钥注册请求 C04
账户创建请求 C05
账户创建公钥注册 C06
注册信息发布 C07
注册信息同步 C08
信息同步应答 C09
注册成功应答 C10
用户登录请求 C11
登录信息审查 C12
登录认证请求 C13
加密认证请求 C14
加密认证回复 C15
密钥认证失败 C16
加密认证请求 C17
加密认证回复 C18
密钥认证成功 C19
登录状态发布 C20
登录状态同步 C21
状态发布回复 C22
登录成功应答 C23
账户修改请求 C24
修改信息审查 C25
账户修改请求 C26
账户修改公钥修改 C27
修改信息发布 C28
修改信息同步 C29
信息同步应答 C30
修改成功应答 C31

图 5

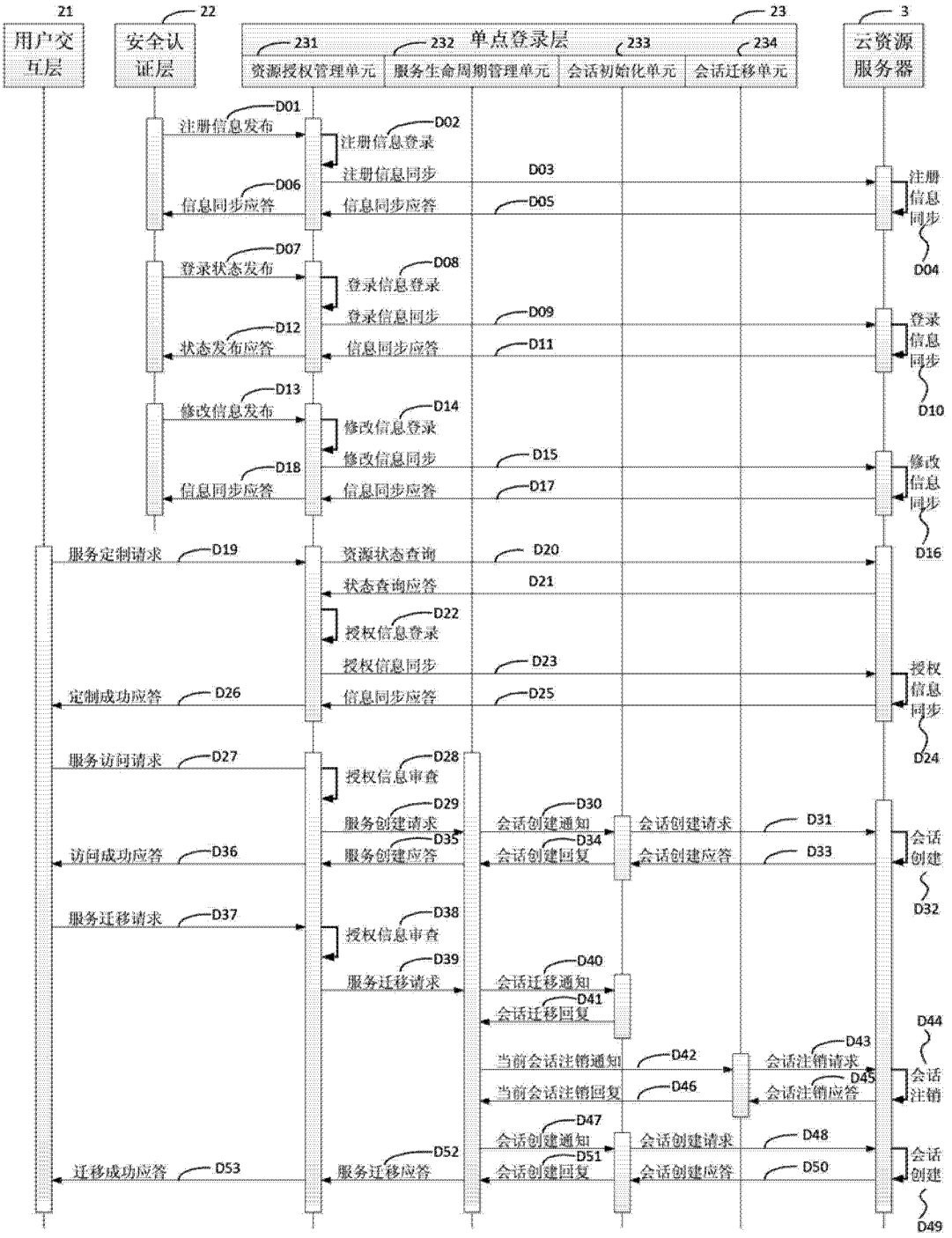

21
用户交互层
22
安全认证层
23
单点登录层
231
资源授权管理单元
232
服务生命周期管理单元
233
会话初始化单元
234
会话迁移单元
3
云资源服务器
D01
注册信息发布
D02
注册信息登录
注册信息同步
D03
D04
注册信息同步
信息同步应答
D05
D06
信息同步应答
登录状态发布
D07
D08
登录信息登录
登录信息同步
D09
D10
登录信息同步
状态发布应答
D11
D12
信息同步应答
修改信息发布
D13
D14
修改信息登录
修改信息同步
D15
D16
修改信息同步
信息同步应答
D17
D18
信息同步应答
服务定制请求
D19
资源状态查询
D20
状态查询应答
D21
D22
授权信息登录
授权信息同步
D23
D24
授权信息同步
定制成功应答
D26
信息同步应答
D25
服务访问请求
D27
D28
授权信息审查
服务创建请求
D29
会话创建通知
D30
会话创建请求
D31
D32
会话创建
访问成功应答
D36
D35
服务创建应答
会话创建回复
D34
会话创建应答
D33
服务迁移请求
D37
D38
授权信息审查
服务迁移请求
D39
会话迁移通知
D40
D41
会话迁移回复
D44
当前会话注销通知
D42
会话注销请求
D43
D45
会话注销
当前会话注销回复
D46
会话注销应答
会话创建通知
D47
会话创建请求
D48
D49
会话创建
迁移成功应答
D53
D52
服务迁移应答
会话创建回复
D51
会话创建应答
D50

图 6