(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106209727 B
(45)授权公告日 2020.09.01

(21)申请号 201510214169.1

(22)申请日 2015.04.29

(65)同一申请的已公布的文献号
申请公布号 CN 106209727 A

(43)申请公布日 2016.12.07

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 周志章

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

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

(56)对比文件
CN 104135494 A,2014.11.05
US 2011225641 A1,2011.09.15

审查员 孙丽

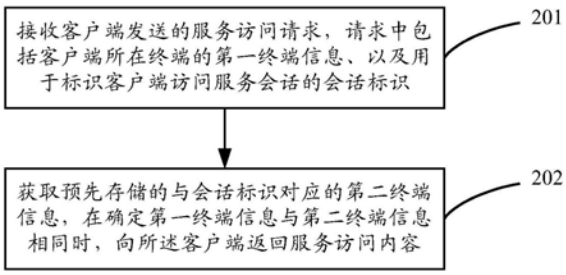
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种会话访问方法和装置

(57)摘要

本申请提供一种会话访问方法和装置,其中方法包括:接收客户端发送的服务访问请求,所述服务访问请求中包括客户端所在终端的第一终端信息、以及用于标识客户端访问服务会话的会话标识;获取预先存储的与所述会话标识对应的第二终端信息,在确定所述第一终端信息与第二终端信息相同时,向所述客户端返回服务访问内容。本申请提高了应用访问的安全性。




CN 106209727 B

1.一种会话访问方法,其特征在于,包括:

接收客户端在登录后发送的服务访问请求,所述服务访问请求中包括客户端所在终端的第一终端信息、以及用于标识客户端访问服务会话的会话标识;所述客户端的服务访问采用短链接方式;所述会话标识是为本次访问分配的会话标识;

获取预先存储的与所述会话标识对应的第二终端信息,在确定所述第一终端信息与第二终端信息相同时,向所述客户端返回服务访问内容;

在所述接收客户端发送的服务访问请求之前,还包括:

接收所述客户端发送的会话授权请求,所述会话授权请求中包括所述第二终端信息;

向所述客户端返回授权的所述会话标识,并存储所述会话标识与所述第二终端信息的对应关系;

所述终端信息,包括:所述终端的网络连接属性信息。

2.根据权利要求1所述的方法,其特征在于,所述网络连接属性信息,包括:终端的IP地址或者MAC地址。

3.一种会话访问装置,其特征在于,包括:

请求接收模块,用于接收客户端在登录后发送的服务访问请求,所述服务访问请求中包括客户端所在终端的第一终端信息、以及用于标识客户端访问服务会话的会话标识;所述客户端的服务访问采用短链接方式;所述会话标识是为本次访问分配的会话标识;所述终端信息,包括:所述终端的网络连接属性信息;

内容反馈模块,用于获取预先存储的与所述会话标识对应的第二终端信息,在确定所述第一终端信息与第二终端信息相同时,向所述客户端返回服务访问内容;

所述请求接收模块,还用于在接收客户端发送的服务访问请求之前,接收客户端发送的会话授权请求,所述会话授权请求中包括所述第二终端信息;

所述内容反馈模块,还用于向所述客户端返回授权的所述会话标识,并存储所述会话标识与所述第二终端信息的对应关系。

4.根据权利要求3所述的装置,其特征在于,所述网络连接属性信息,包括:终端的IP地址或者MAC地址。

# 一种会话访问方法和装置

## 技术领域

[0001] 本申请涉及网络技术，特别涉及一种会话访问方法和装置。

## 背景技术

[0002] 基于B/S(Browser/Server，浏览器/服务器)模式的互联网应用，在服务器为浏览器对应的客户端提供应用数据时，出于数据访问的安全考虑，通常只将应用数据授权给具有登录权限的用户。并且，该互联网应用的访问是短链接的方式，客户端每次向服务器发送数据请求时都要与服务器建立会话，并且携带会话标识来保持对同一个应用的访问状态。但是，由于会话标识是存储在客户端，容易被随意复制，一旦被其他终端复制该会话标识并用以向服务器请求会话，将使应用访问存在安全隐患。

## 发明内容

[0003] 有鉴于此，本申请提供一种会话访问方法和装置，以提高应用访问的安全性。

[0004] 具体地，本申请是通过如下技术方案实现的：

[0005] 第一方面，提供一种会话访问方法，包括：

[0006] 接收客户端发送的服务访问请求，所述服务访问请求中包括客户端所在终端的第一终端信息、以及用于标识客户端访问服务会话的会话标识；

[0007] 获取预先存储的与所述会话标识对应的第二终端信息，在确定所述第一终端信息与第二终端信息相同时，向所述客户端返回服务访问内容。

[0008] 第二方面，提供一种会话访问装置，包括：

[0009] 请求接收模块，用于接收客户端发送的服务访问请求，所述服务访问请求中包括客户端所在终端的第一终端信息、以及用于标识客户端访问服务会话的会话标识；

[0010] 内容反馈模块，用于获取预先存储的与所述会话标识对应的第二终端信息，在确定所述第一终端信息与第二终端信息相同时，向所述客户端返回服务访问内容。

[0011] 本申请提供的会话访问方法和装置，通过在确定发送服务访问请求的终端与存储的终端相同时，才向客户端返回服务访问内容，可以避免终端不同时的会话访问，从而提高了应用访问的安全性。

## 附图说明

[0012] 图1是本申请一示例性实施例示出的一种互联网应用的访问系统；

[0013] 图2是本申请一示例性实施例示出的一种会话访问方法的流程图；

[0014] 图3是本申请一示例性实施例示出的另一种会话访问方法的流程图；

[0015] 图4是本申请一示例性实施例示出的一种会话访问装置的结构图。

## 具体实施方式

[0016] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及

附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0017] 图1示例了B/S模式下的互联网应用的访问系统，该系统可以包括客户端11和服务器12，例如，客户端是通过终端13上运行的浏览器打开的天猫网站，而服务器12是天猫网站对应的天猫服务器。本申请实施例的会话访问方法和装置，应用于客户端和服务器之间的通信，如下首先简单说明上述客户端11与服务器12之间的通信特点：

[0018] 仍以上述的天猫客户端对天猫服务器的访问为例，在浏览器上显示的天猫网站中的内容可以是服务器12提供的，并且通常服务器12只将内容提供给具有登录权限的用户，因此用户会在天猫网站注册得到账号和密码。

[0019] 在得到账号和密码后，客户端和浏览器之间的访问采用短链接方式，具体的，例如，天猫网站上可以包括多个网络资源的链接，比如服饰详情链接、商家信息链接等，短链接方式的特点是，每次当用户点击一个链接时(相当于发起一次数据请求)，都要与服务器建立一次会话，当本次链接对应的数据请求结束，则会话释放；下一次再在天猫网站点击下一个链接时(相当于又发起一次数据请求)，则又要建立一次会话。这多次的会话建立都是用户在登录天猫以后对天猫网站的访问操作，也就是说，从用户登录天猫到退出对天猫的访问，中间可能会向服务器发起多次数据请求，建立多次会话。

[0020] 对于上述的访问过程，服务器侧会对该访问进行记录，记录方式是，对于用户登录天猫到退出对天猫的整个访问过程，分配一个会话ID，在整个访问中的多次会话，都携带该相同的会话ID，这样服务器就可以据此确定该多次会话访问都是对应于同一个用户对天猫的一次访问。即某用户在登录天猫时，服务器为其分配会话ID，在用户访问天猫的过程中，每次数据请求创建会话时都携带该会话ID，服务器根据该会话ID将用户本次登录的访问过程关联记录，属于同一个用户对天猫的一次访问。

[0021] 本申请实施例的会话访问方法，应用于在用户登录天猫之后，每次创建会话时，服务器侧根据本实施例的会话访问方法确定用户是否有访问权限。图2示例了服务器执行的会话访问方法，包括：

[0022] 201、接收客户端发送的服务访问请求，所述服务访问请求中包括客户端所在终端的第一终端信息、以及用于标识客户端访问服务会话的会话标识；

[0023] 202、获取预先存储的与所述会话标识对应的第二终端信息，在确定所述第一终端信息与第二终端信息相同时，向所述客户端返回服务访问内容。

[0024] 其中，在201中的服务访问请求，例如是用户在登录天猫之后点击网站上的一个资源链接，向服务器12发送所述的服务访问请求。客户端可以在该请求中携带所在终端的终端信息，该客户端所在终端例如是图1中所示的终端13，客户端天猫网站是运行在该终端13的浏览器上；所述的终端信息例如是IP地址、MAC地址这类网络连接属性信息，这种信息具有较难复制的特点。客户端还在服务访问请求中携带会话标识，该会话标识可以是用户首次登录天猫网站时，服务器为用户的本次访问分配的会话ID。

[0025] 在202中，服务器12可以将服务访问请求中携带的终端信息，与本次预先存储的与会话ID对应的终端信息进行比较，可以将服务访问请求中携带的终端信息称为第一终端信息，本地存储的终端信息称为第二终端信息，该第二终端信息可以是服务器在为用户分配

会话ID时记录的。如果第一终端信息与第二终端信息相同，则可以确定是同一个终端发起的访问，则可以向客户端返回服务访问内容，比如对应网站链接的数据资源。

[0026] 通过图2所示的会话访问方法，服务器就可以确保访问应用的终端的一致性，防止不同终端之间复制会话ID的情况发生。比如，用户在终端13上登录天猫时服务器分配了访问会话的会话ID，如果用户在另一个终端上访问天猫，即使仍然是同一账号密码对应的同一用户，但是更换终端后通常服务器侧将终止本次访问的授权，而如果上述另一个终端也携带了会话ID，服务器侧只根据会话ID判断用户是否有访问权限，则容易造成在更换终端后仍然能够访问，这种随意访问增加了安全隐患。本实施例的服务器不仅根据会话ID，还根据终端信息，只有发起当前会话的终端与授权会话时的终端相同时，才允许继续访问，从而确保了访问安全性。

[0027] 图3示例了服务器侧处理会话访问的另一流程图，如图3所示，包括：

[0028] 301、接收所述客户端发送的会话授权请求；

[0029] 例如，用户可以在天猫网站输入账号和密码，携带在会话授权请求中提交到服务器进行验证。该会话授权请求还可以包括客户端所在的终端的终端信息，可以称为第二终端信息，比如是终端的IP地址。

[0030] 302、存储会话标识与第二终端信息的对应关系；

[0031] 例如，服务器接收到301中的会话授权请求后，对账号和密码进行验证，在验证通过后，为用户的本次访问分配会话标识，并存储该会话标识与会话授权请求中携带的第二终端信息的对应关系。

[0032] 303、向所述客户端返回授权的所述会话标识；

[0033] 例如，服务器在本步骤将为用户分配的会话ID返回至客户端。

[0034] 304、接收客户端发送的服务访问请求；

[0035] 例如，在用户登录天猫之后，点击网站的资源链接发起服务访问请求，该请求中携带上述303中分配的会话ID，还携带客户端所在终端的终端信息，可以称为第一终端信息。

[0036] 305、获取预先存储的与所述会话标识对应的第二终端信息，在确定所述第一终端信息与第二终端信息相同；

[0037] 例如，服务器根据304中的会话ID，获取与该会话ID对应的第二终端信息，并判断第二终端信息与第一终端信息是否相同。如果不同，则表明本次访问的终端不是服务器授权会话ID时的终端，则拒绝访问；否则，继续306，向用户返回访问内容。

[0038] 306、向所述客户端返回服务访问内容。

[0039] 为实现上述的会话访问方法，本申请实施例还提供一种会话访问装置，该装置应用于服务器侧，如图4所示，该装置可以包括：请求接收模块41和内容反馈模块42；其中，

[0040] 请求接收模块41，用于接收客户端发送的服务访问请求，所述服务访问请求中包括客户端所在终端的第一终端信息、以及用于标识客户端访问服务会话的会话标识；

[0041] 例如，终端信息可以包括：终端的网络连接属性信息。所述网络连接属性信息，例如包括：终端的IP地址或者MAC地址。

[0042] 内容反馈模块42，用于获取预先存储的与所述会话标识对应的第二终端信息，在确定所述第一终端信息与第二终端信息相同时，向所述客户端返回服务访问内容。

[0043] 进一步的，所述请求接收模块41，还用于在接收客户端发送的服务访问请求之前，

接收客户端发送的会话授权请求，所述会话授权请求中包括所述第二终端信息；

[0044] 所述内容反馈模块42，还用于向所述客户端返回授权的所述会话标识，并存储所述会话标识与所述第二终端信息的对应关系。

[0045] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

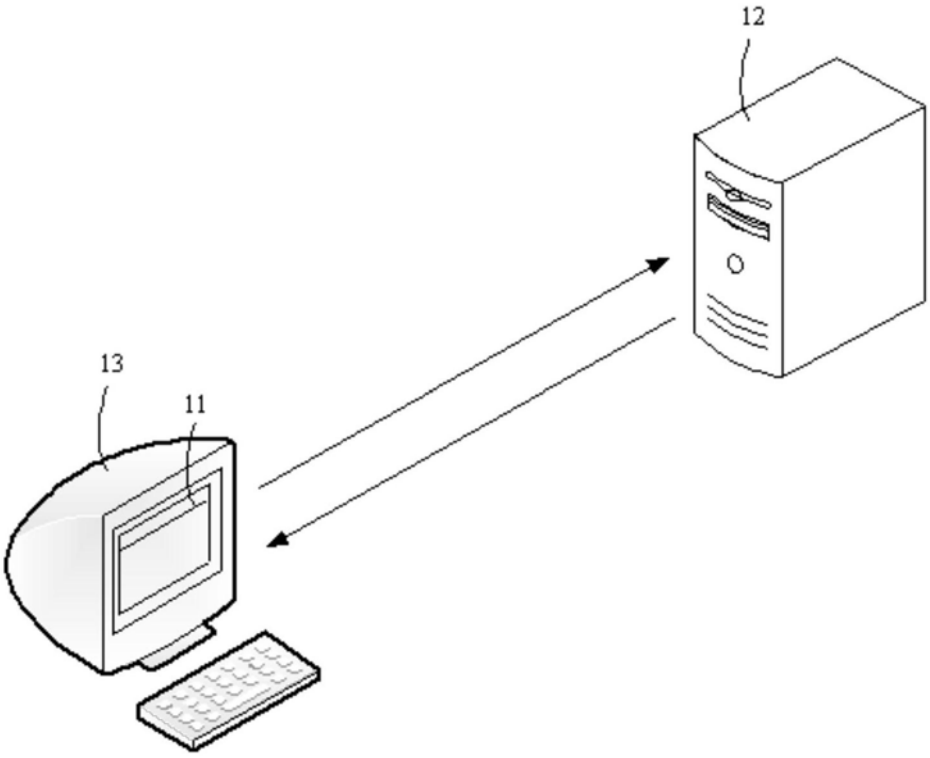

12
13
11

图1

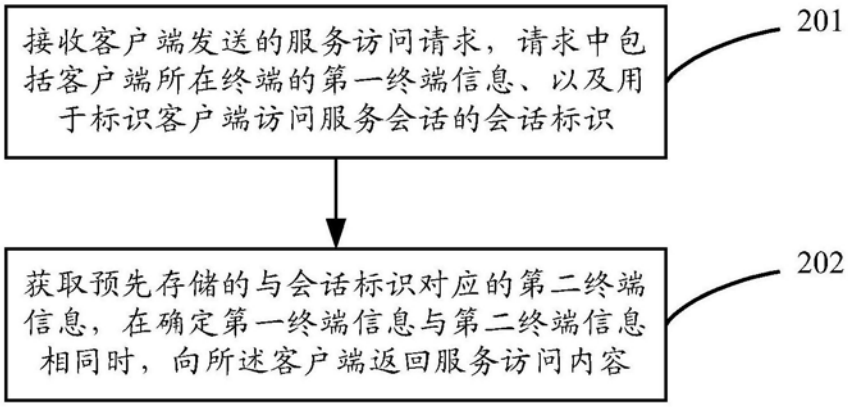

接收客户端发送的服务访问请求，请求中包括客户端所在终端的第一终端信息、以及用于标识客户端访问服务会话的会话标识
201
获取预先存储的与会话标识对应的第二终端信息，在确定第一终端信息与第二终端信息相同时，向所述客户端返回服务访问内容
202

图2

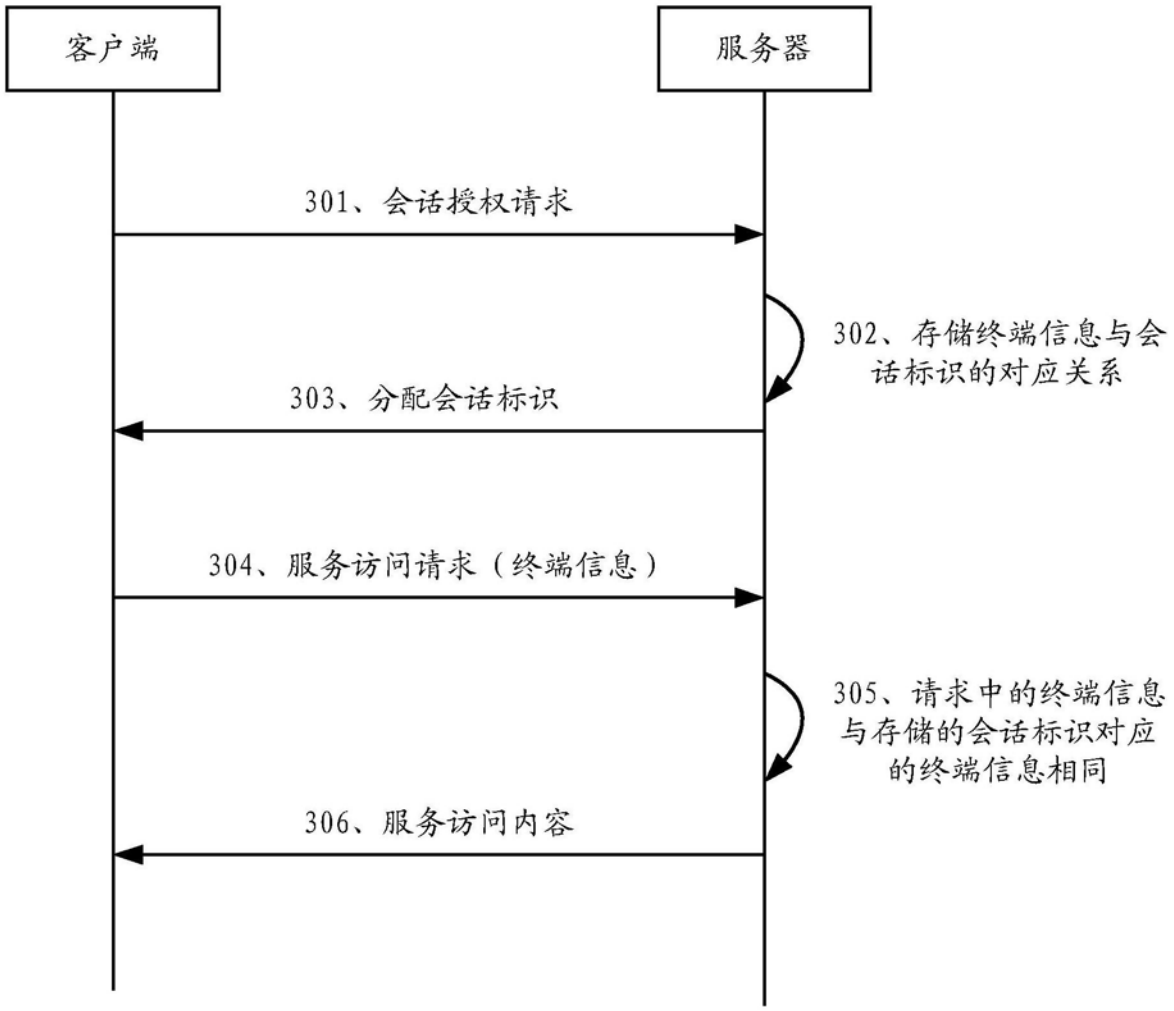

客户端
服务器
301、会话授权请求
302、存储终端信息与会话标识的对应关系
303、分配会话标识
304、服务访问请求（终端信息）
305、请求中的终端信息与存储的会话标识对应的终端信息相同
306、服务访问内容

图3

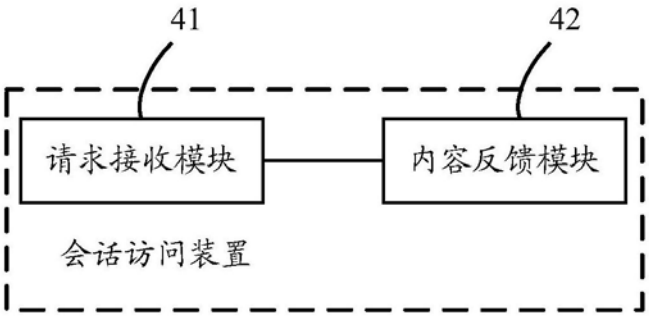

41
42
请求接收模块
内容反馈模块
会话访问装置

图4