(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111294337 B
(45)授权公告日 2024.07.23

(21)申请号 202010044548.1
(22)申请日 2020.01.15
(65)同一申请的已公布的文献号
申请公布号 CN 111294337 A
(43)申请公布日 2020.06.16
(73)专利权人 平安科技(深圳)有限公司
地址 518000 广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼
(72)发明人 吴振全
(74)专利代理机构 广州三环专利商标代理有限公司 44202
专利代理师 熊永强 彭程
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
(56)对比文件
US 2018332016 A1,2018.11.15
审查员 白生斌

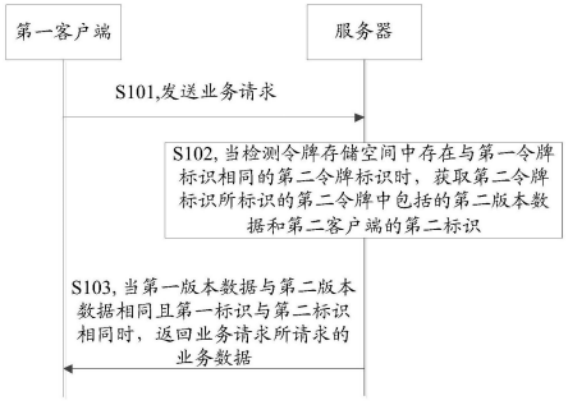
权利要求书2页 说明书11页 附图3页

(54)发明名称

一种基于令牌的鉴权方法及装置

(57)摘要

本申请实施例公开了一种基于令牌的鉴权方法及装置,其中方法包括:服务器接收第一客户端发送的业务请求,该业务请求中包括该第一客户端的第一标识和第一令牌,该第一令牌中包括第一令牌标识和第一版本数据,当检测到令牌存储空间中存在与该第一令牌标识相同的第二令牌标识时,获取该第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,该令牌存储空间用于存储该服务器授权使用的令牌,当该第一版本数据与该第二版本数据相同且该第一标识与该第二标识相同时,向该第一客户端返回该业务请求所请求的业务数据。采用本申请实施例,可以令牌(如JWT)鉴权的安全性。



CN 111294337 B

1.一种基于令牌的鉴权方法,其特征在于,包括:

服务器接收第一客户端发送的业务请求,所述业务请求中包括所述第一客户端的第一标识和第一令牌,所述第一令牌中包括第一令牌标识和第一版本数据;

若检测到令牌存储空间中存在与所述第一令牌标识相同的第二令牌标识,则所述服务器获取所述第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,所述令牌存储空间用于存储所述服务器授权使用的令牌;

检测所述第一版本数据与所述第二版本数据是否相同,包括:分别计算所述第一版本数据的哈希值和所述第二版本数据的哈希值,并比较所述第一版本数据的哈希值与所述第二版本数据的哈希值是否相等,当所述第一版本数据的哈希值与所述第二版本数据的哈希值相等时,确定所述第一版本数据与所述第二版本数据相同,当所述第一版本数据的哈希值与所述第二版本数据的哈希值不相等时,确定所述第一版本数据与所述第二版本数据不相同;

检测所述第一标识和所述第二标识是否相同,包括:比较所述第一标识的哈希值与所述第二标识的哈希值是否相同,当所述第一标识的哈希值与所述第二标识的哈希值相同时,确定所述第一标识与所述第二标识相同,当所述第一标识的哈希值与所述第二标识的哈希值不相同时,确定该第一标识与该第二标识不相同;

若所述第一版本数据与所述第二版本数据相同、且所述第一标识与所述第二标识相同,则所述服务器向所述第一客户端返回所述业务请求所请求的业务数据;

其中,所述第二令牌中还包括令牌有效期;

所述服务器向所述第二客户端发放所述第二令牌之后,所述方法还包括:

若基于所述令牌有效期检测到所述第二令牌失效,则所述服务器从所述令牌存储空间中删除所述第二令牌;

所述服务器向所述第一客户端返回所述业务请求所请求的业务数据之后,所述方法还包括:

所述服务器对所述第二令牌中包括的令牌有效期进行延长;

所述方法还包括:

若所述第一版本数据与所述第二版本数据不相同,则所述服务器针对所述业务请求返回请求失败响应,所述请求失败响应用于拒绝所述业务请求;

若所述第一标识与所述第二标识不相同,则所述服务器对所述业务请求所请求的业务数据进行数据脱敏处理,得到目标业务数据,并向所述第一客户端返回所述目标业务数据;

所述方法还包括:

当接收到所述第一客户端发送的退出登录请求时,所述服务器从所述令牌存储空间中删除与所述第一令牌标识相同的所述第二令牌标识所标识的第二令牌。

2.根据权利要求1所述的方法,其特征在于,所述服务器接收第一客户端发送的业务请求之前,所述方法还包括:

服务器根据第二客户端发送的登录请求生成第二令牌,并将所述第二令牌存储在令牌存储空间中,所述第二令牌中包括第二令牌标识、所述第二客户端的第二标识以及第二版本数据;

所述服务器向所述第二客户端发放所述第二令牌,以使所述第二客户端基于所述第二

令牌在所述服务器上进行鉴权。

3.根据权利要求2所述的方法,其特征在于,所述方法还包括:

若检测到所述令牌存储空间中不存在与所述第一令牌标识相同的第二令牌标识,则所述服务器针对所述业务请求返回请求失败响应,所述请求失败响应用于拒绝所述业务请求。

4.一种基于令牌的鉴权装置,所述装置用于执行如权利要求1-3任一项所述的方法,其特征在于,包括:

接收模块,用于接收第一客户端发送的业务请求,所述业务请求中包括所述第一客户端的第一标识和第一令牌,所述第一令牌中包括第一令牌标识和第一版本数据;

获取模块,用于当检测到令牌存储空间中存在与所述第一令牌标识相同的第二令牌标识时,获取所述第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,所述令牌存储空间用于存储所述服务器授权使用的令牌;

所述获取模块还用于,检测所述第一版本数据与所述第二版本数据是否相同,包括:分别计算所述第一版本数据的哈希值和所述第二版本数据的哈希值,并比较所述第一版本数据的哈希值与所述第二版本数据的哈希值是否相等,当所述第一版本数据的哈希值与所述第二版本数据的哈希值相等时,确定所述第一版本数据与所述第二版本数据相同,当所述第一版本数据的哈希值与所述第二版本数据的哈希值不相等时,确定所述第一版本数据与所述第二版本数据不相同;

所述获取模块还用于,检测所述第一标识和所述第二标识是否相同,包括:比较所述第一标识的哈希值与所述第二标识的哈希值是否相同,当所述第一标识的哈希值与所述第二标识的哈希值相同时,确定所述第一标识与所述第二标识相同,当所述第一标识的哈希值与所述第二标识的哈希值不相同时,确定该第一标识与该第二标识不相同;

发送模块,用于当所述第一版本数据与所述第二版本数据相同、且所述第一标识与所述第二标识相同时,向所述第一客户端返回所述业务请求所请求的业务数据。

5.一种服务器,其特征在于,包括处理器、输入设备、输出设备和存储器,所述处理器、输入设备、输出设备和存储器相互连接,其中,所述存储器用于存储计算机程序,所述计算机程序包括程序指令,所述处理器被配置用于调用所述程序指令,执行如权利要求1-3任一项所述的方法。

6.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有计算机程序,所述计算机程序包括程序指令,所述程序指令当被处理器执行时使所述处理器执行如权利要求1-3任一项所述的方法。

一种基于令牌的鉴权方法及装置

技术领域

[0001] 本申请涉及计算机技术领域,尤其涉及一种基于令牌的鉴权方法及装置。

背景技术

[0002] 随着计算机技术的发展,万维网(web)应用中基于令牌(token)的身份验证越来越多。JSON Web Token(简称JWT)是目前最常用的跨域身份验证解决方案。跨域是指一个统一资源定位符(Uniform Resource Locator,URL)请求的协议、域名、端口三者之间任意一个与当前页面的URL不同,即JWT同时支持超文本标记语言(Hyper Text Markup Language,HTML)和原生语言所写的web应用的身份验证。JWT是一个开放的标准(RFC 7519),由于JWT的信息是被数字签名过的,所以JWT可以在服务器和客户端之间安全地传送消息。

[0003] 然而,在服务器端,JWT签发后,在JWT的有效期内,JWT会一直有效。又因为JWT存储在客户端上,一旦客户端上的JWT被不法分子盗用,不法分子就可以轻易获取到用户的信息或财产,引发严重的安全问题。

发明内容

[0004] 本申请实施例提供一种基于令牌的鉴权方法及装置,可以提高令牌(如JWT)鉴权的安全性。

[0005] 第一方面,本申请实施例提供了一种基于令牌的鉴权方法,该方法包括:

[0006] 服务器接收第一客户端发送的业务请求,该业务请求中包括该第一客户端的第一标识和第一令牌,该第一令牌中包括第一令牌标识和第一版本数据;若检测到令牌存储空间中存在与该第一令牌标识相同的第二令牌标识,则服务器获取该第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,该令牌存储空间用于存储服务器授权使用的令牌;若该第一版本数据与该第二版本数据相同且该第一标识与该第二标识相同,则服务器向该第一客户端返回该业务请求所请求的业务数据。

[0007] 结合第一方面,在一种可能的实施方式中,服务器接收第一客户端发送的业务请求之前,该方法还包括:

[0008] 服务器根据第二客户端发送的登录请求生成第二令牌,并将该第二令牌存储在令牌存储空间中,该第二令牌中包括第二令牌标识、该第二客户端的第二标识以及第二版本数据;服务器向该第二客户端发放该第二令牌,以使该第二客户端基于该第二令牌在该服务器上进行鉴权。

[0009] 结合第一方面,在一种可能的实施方式中,上述第二令牌中还包括令牌有效期。服务器向该第二客户端发放该第二令牌之后,该方法还包括:若基于该令牌有效期检测到该第二令牌失效,则服务器从该令牌存储空间中删除该第二令牌;服务器向该第一客户端返回该业务请求所请求的业务数据之后,该方法还包括:服务器对该第二令牌中包括的令牌有效期进行延长。

[0010] 结合第一方面,在一种可能的实施方式中,该方法还包括:服务器分别计算该第一

版本数据的哈希值和该第二版本数据的哈希值,并比较该第一版本数据的哈希值与该第二版本数据的哈希值是否相等;当该第一版本数据的哈希值与该第二版本数据的哈希值相等时,服务器确定该第一版本数据与该第二版本数据相同;当该第一版本数据的哈希值与该第二版本数据的哈希值不相等时,服务器确定该第一版本数据与该第二版本数据不相同。

[0011] 结合第一方面,在一种可能的实施方式中,该方法还包括:若检测到该令牌存储空间中不存在与该第一令牌标识相同的第二令牌标识,则服务器针对该业务请求返回请求失败响应,该请求失败响应用于拒绝该业务请求。

[0012] 结合第一方面,在一种可能的实施方式中,该方法还包括:若该第一版本数据与该第二版本数据不相同,则服务器针对该业务请求返回请求失败响应,该请求失败响应用于拒绝该业务请求;若该第一标识与该第二标识不相同,则服务器对该业务请求所请求的业务数据进行数据脱敏处理,得到目标业务数据,并向该第一客户端返回该目标业务数据。

[0013] 结合第一方面,在一种可能的实施方式中,该方法还包括:当接收到该第一客户端发送的退出登录请求时,服务器从该令牌存储空间中删除与该第一令牌标识相同的该第二令牌标识所标识的第二令牌。

[0014] 第二方面,本申请实施例提供了一种基于令牌的鉴权装置,该装置包括:

[0015] 接收模块,用于接收第一客户端发送的业务请求,该业务请求中包括该第一客户端的第一标识和第一令牌,该第一令牌中包括第一令牌标识和第一版本数据;

[0016] 获取模块,用于当检测到令牌存储空间中存在与该第一令牌标识相同的第二令牌标识时,获取该第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,该令牌存储空间用于存储服务器授权使用的令牌;

[0017] 发送模块,用于当该第一版本数据与该第二版本数据相同且该第一标识与该第二标识相同时,向该第一客户端返回该业务请求所请求的业务数据。

[0018] 结合第二方面,在一种可能的实施方式中,该装置还包括生成模块和存储模块。该生成模块,用于根据第二客户端发送的登录请求生成第二令牌;该存储模块,用于将该第二令牌存储在令牌存储空间中,该第二令牌中包括第二令牌标识、该第二客户端的第二标识以及第二版本数据;上述发送模块,还用于向该第二客户端发放该第二令牌,以使该第二客户端基于该第二令牌进行鉴权。

[0019] 结合第二方面,在一种可能的实施方式中,上述第二令牌中还包括令牌有效期。该装置还包括删除模块和有效期延长模块。该删除模块,用于当基于该令牌有效期检测到该第二令牌失效时,从该令牌存储空间中删除该第二令牌;该有效期延长模块,用于对该第二令牌中包括的令牌有效期进行延长。

[0020] 结合第二方面,在一种可能的实施方式中,该装置还包括计算模块、比较模块以及确定模块。该计算模块,用于分别计算该第一版本数据的哈希值和该第二版本数据的哈希值;该比较模块,用于比较该第一版本数据的哈希值与该第二版本数据的哈希值是否相等;该确定模块,用于当该第一版本数据的哈希值与该第二版本数据的哈希值相等时,确定该第一版本数据与该第二版本数据相同;该确定模块,还用于当该第一版本数据的哈希值与该第二版本数据的哈希值不相等时,确定该第一版本数据与该第二版本数据不相同。

[0021] 结合第二方面,在一种可能的实施方式中,上述发送模块,还用于当检测到该令牌存储空间中不存在与该第一令牌标识相同的第二令牌标识时,针对该业务请求返回请求失

败响应,该请求失败响应用于拒绝该业务请求。

[0022] 结合第二方面,在一种可能的实施方式中,该装置还包括数据脱敏模块。上述发送模块,还用于当该第一版本数据与该第二版本数据不相同或该第一标识与该第二标识不相同时,针对该业务请求返回请求失败响应,该请求失败响应用于拒绝该业务请求;该数据脱敏模块,用于当该第一标识与该第二标识不相同时,对该业务请求所请求的业务数据进行数据脱敏处理,得到目标业务数据;上述发送模块,还用于向该第一客户端返回该目标业务数据。

[0023] 结合第二方面,在一种可能的实施方式中,上述删除模块,还用于当接收到该第一客户端发送的退出登录请求时,从该令牌存储空间中删除与该第一令牌标识相同的该第二令牌标识所标识的第二令牌。

[0024] 第三方面,本申请实施例提供了一种服务器,包括处理器、输入设备、输出设备和存储器,该处理器、输入设备、输出设备和存储器相互连接,其中,该存储器用于存储支持服务器执行上述方法的计算机程序,该计算机程序包括程序指令,该处理器被配置用于调用该程序指令,执行上述第一方面的基于令牌的鉴权方法。

[0025] 第四方面,本申请实施例提供了一种计算机可读存储介质,该计算机可读存储介质存储有计算机程序,该计算机程序包括程序指令,该程序指令当被处理器执行时使该处理器执行上述第一方面的基于令牌的鉴权方法。

[0026] 本申请实施例通过接收第一客户端发送的业务请求,该业务请求中包括该第一客户端的第一标识和第一令牌,该第一令牌中包括第一令牌标识和第一版本数据,当检测到令牌存储空间中存在与该第一令牌标识相同的第二令牌标识时,获取该第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,当该第一版本数据与该第二版本数据相同且该第一标识与该第二标识相同时,向该第一客户端返回该业务请求所请求的业务数据。本申请实施例通过多重检验(第一令牌是否合法(即令牌存储空间中是否存在与第一令牌标识相同的第二令牌标识)、第一令牌是否失效(即第一版本数据与第二版本数据是否相同)以及第一客户端是否为合法客户端(即第一标识与第二标识是否相同)),只有多重检验均通过时,才向第一客户端返回业务数据,可以确保每个令牌都必须在生成的令牌设备上使用,杜绝跨设备使用令牌,从而可以提高令牌(如JWT)鉴权的安全性。

附图说明

[0027] 为了更清楚地说明本申请实施例技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图是本申请的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0028] 图1是本申请实施例提供的基于令牌的鉴权方法的一示意流程图;

[0029] 图2是本申请实施例提供基于令牌的鉴权方法的另一示意流程图;

[0030] 图3是本申请实施例提供的基于令牌的鉴权装置的结构示意图;

[0031] 图4是本申请实施例提供的服务器的结构示意图。

具体实施方式

[0032] 下面将结合本申请实施例中的附图,对本申请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申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,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,都属于本申请保护的范围。

[0033] 应当理解,本申请的说明书和权利要求书及所述附图中的术语“第一”、“第二”等是用于区别不同对象,而不是用于描述特定顺序。此外,术语“包括”和“具有”以及它们任何变形,意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元,而是可选地还包括没有列出的步骤或单元,或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0034] 还应当理解,在本文中提及“实施例”意味着,结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置展示该短语并不一定均是指相同的实施例,也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是,本文所描述的实施例可以与其它实施例相结合。

[0035] 还应当进一步理解,在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合,并且包括这些组合。

[0036] 下面将结合附图1-附图2,对本申请实施例提供的基于令牌的鉴权方法进行介绍。

[0037] 参见图1,是本申请实施例提供基于令牌的鉴权方法的一示意流程图。如图1所示,该基于令牌的鉴权方法可包括步骤:

[0038] S101,第一客户端向服务器发送业务请求。相应地,服务器接收业务请求。

[0039] 在一些可行的实施方式中,第一客户端可以根据用户的操作生成业务请求。第一客户端可以向服务器发送该业务请求,相应地,服务器接收该业务请求。该业务请求可以用于请求业务数据。可以理解的是,服务器可以为每一个客户端分配一个令牌,客户端在向服务器请求业务数据时,可以携带服务器分配给这个客户端的令牌,该令牌可以用于鉴权,即鉴定这个客户端是否是服务器授权的合法客户端。该业务请求中可以包括该第一客户端的第一标识和第一令牌,该第一令牌可以包括第一令牌标识和第一版本数据。该第一标识可以用于唯一标识该第一客户端,该第一版本数据可以为该第一令牌的版本号。版本号通常由2至4个部分组成:主版本号、次版本号、内部版本号和修订号。主版本号和次版本号是必选的;内部版本号和修订号是可选的,但是如果定义了修订号部分,则内部版本号就是必选的。所有定义的部分都必须是大于或等于0的整数。比如,第一版本数据为版本号:1.1.0。

[0040] 其中,本申请实施例中所涉及的令牌可以为JWT。第一客户端可以为手机、便捷式电脑、台式电脑等终端,也可以为终端上的浏览器、应用程序等。第一标识可以为第一客户端的客户端标识,比如客户端的互联网协议(Internet Protocol,IP)地址或物理地址(Media Access Control Address,MAC地址)、浏览器标识等。

[0041] S102,当检测令牌存储空间中存在与第一令牌标识相同的第二令牌标识时,服务器获取第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识。

[0042] 在一些可行的实施方式中,服务器在接收到上述业务请求之后,可以提取该业务请求中携带的第一令牌,并可以从该第一令牌中提取第一令牌标识。服务器可以在令牌存储空间中检测是否存在与该第一令牌标识相同的第二令牌标识。若服务器在该令牌存储空间中检测到与该第一令牌标识相同的第二令牌标识,说明该第一令牌是服务器授权的合法令牌,也说明该第一令牌是真实的,则服务器可以从该令牌存储空间中提取该第二令牌标

识所标识的第二令牌,并可以获取该第二令牌中包括的第二版本数据和第二客户端的第二标识。其中,该第二标识可以用于唯一标识该第二客户端,该第二标识与上述第一标识可以是同一类标识。比如,第一标识和第二标识均为IP地址。该第二版本数据可以为该第二令牌的版本号。比如,第二版本数据为版本号:1.1.1。第一令牌标识可以用于唯一标识该第一令牌,比如,第一令牌标识可以为服务器对该第一令牌中的数据/信息进行哈希(Hash)运算后得到的哈希值。可选的,第一令牌标识还可以为服务器利用HS256算法对该第一令牌中的数据/信息加密生成的签名数据。第二令牌标识可以用于唯一标识该第二令牌,且第二令牌标识可以与第一令牌标识属于同一类标识,比如第一令牌标识为哈希值,第二令牌标识也为哈希值;第一令牌标识为签名数据,第二令牌标识也为签名数据。该令牌存储空间可以为Redis缓存或特定的一个缓存空间或关系数据库。本申请实施例通过检测第一客户端发送的业务请求中携带的第一令牌是否在服务器中存在,来判断第一客户端是否盗用其他客户端的令牌获取业务数据,从而防止不同客户端使用一个令牌导致的数据泄露,提高数据的安全性。

[0043] 可选的,若服务器在该令牌存储空间中未检测到与该第一令牌标识相同的第二令牌标识,说明该第一令牌不是服务器授权的合法令牌,也说明该第一令牌是伪造的,则服务器可以针对上述业务请求返回请求失败响应。该请求失败响应可以用于拒绝该业务请求。

[0044] S103,当第一版本数据与第二版本数据相同且第一标识与第二标识相同时,服务器向第一客户端返回业务请求所请求的业务数据。相应地,第一客户端接收业务请求所请求的业务数据。

[0045] 在一些可行的实施方式中,服务器在获取到上述第二版本数据和第二标识之后,可以检测上述第一版本数据与该第二版本数据是否相同。若检测到该第一版本数据和该第二版本数据相同,说明上述第一令牌是最新版本的令牌,也可以说明上述第一令牌未失效,则服务器可以检测上述第一标识和上述第二标识是否相同。若检测到该第一标识与该第二标识相同,说明上述第一客户端和上述第二客户端是同一个客户端,也说明发送上述业务请求的第一客户端是服务器授权的合法客户端,还可以说明第一令牌不是第一客户端盗用的,则服务器可以向第一客户端返回上述业务请求所请求的业务数据。相应地,第一客户端可以接收该业务请求所请求的业务数据,并展示该业务数据。本申请实施例在确定第一令牌是合法令牌(即令牌存储空间中存在与第一令牌标识相同的第二令牌标识)之后,判断第一令牌是否失效(第一版本数据与第二版本数据是否相同)以及第一客户端是否为合法客户端(第一标识与第二标识是否相同),在第一令牌未失效(即第一版本数据与第二版本数据相同)且第一客户端为合法客户端(即第一标识与第二标识相同)时,服务器才向第一客户端返回业务请求所请求的业务数据,通过多重检验,可以确保每个令牌都必须在生成的令牌设备上使用,杜绝跨设备使用令牌,提高令牌鉴权的安全性。

[0046] 可选的,若检测到上述第一版本数据和上述第二版本数据不相同,说明上述第一令牌不是最新版本的令牌,也可以说明上述第一令牌已失效,则服务器可以针对上述业务请求返回请求失败响应。该请求失败响应可以用于拒绝该业务请求。进一步可选的,若检测到上述第一标识与上述第二标识不相同,说明上述第一客户端和上述第二客户端不是同一个客户端,也说明发送上述业务请求的第一客户端不是服务器授权的合法客户端,还说明第一令牌可能是第一客户端盗用的,故第一客户端不能访问服务器中的数据,则服务器可

以针对上述业务请求返回请求失败响应。

[0047] 再进一步可选的,若检测到上述第一标识与上述第二标识不相同,则服务器可以对上述业务请求所请求的业务数据进行数据脱敏处理,得到目标业务数据,并可以将该目标业务数据返回给第一客户端。同时,服务器可以向第一客户端发送身份验证提示信息,该身份验证提示信息用于提示用户进行身份验证。用户通过第一客户端接收到该目标业务数据和身份验证提示信息之后,可以在第一客户端上进行身份验证。第一客户端将用户输入的身份验证信息(账号密码、指纹、虹膜或手势等)发送给服务器,服务器接收到第一客户端发送的身份验证信息之后,对其进行身份验证。若身份验证通过,则服务器可以向第一客户端发送上述业务请求所请求的业务数据。若身份验证未通过,则服务器不做处理。

[0048] 在一些可行的实施方式中,服务器在检测上述第一版本数据与上述第二版本数据是否相同时,可以计算该第一版本数据的哈希值,并可以计算该第二版本数据的哈希值,比较该第一版本数据的哈希值是否与该第二版本数据的哈希值相同。如果该第一版本数据的哈希值与该第二版本数据的哈希值相同,则服务器可以确定该第一版本数据与该第二版本数据相同。如果该第一版本数据的哈希值与该第二版本数据的哈希值不相同,则服务器可以确定该第一版本数据与该第二版本数据不相同。由于哈希运算是把任意长度的输入(又叫做预映射pre-image)通过散列算法变换成固定长度的输出,简单来说就是将任意长度的消息压缩到某一固定长度的消息,所以本申请实施例将数据量大的数据通过哈希运算映射成数据量小的数据,即比较不同版本数据的哈希值,可以提高检测的效率。同理,服务器在检测上述第一标识与上述第二标识是否相同时,也可以比较该第一标识的哈希值与该第二标识的哈希值是否相同。如果该第一标识的哈希值与该第二标识的哈希值相同,则服务器可以确定该第一标识与该第二标识相同。如果该第一标识的哈希值与该第二标识的哈希值不相同,则服务器可以确定该第一标识与该第二标识不相同。

[0049] 在一些可行的实施方式中,服务器在向第一客户端返回上述业务请求所请求的业务数据之后,可以将令牌存储空间中的上述第二令牌包括的令牌有效期进行延长。可选的,服务器可以将请求时间(发送业务请求时的时间)增加固定时长得到第二令牌有效期,将该第二令牌包括的令牌有效期延长至第二令牌有效期。例如,请求时间为2019.7.8,第二令牌包括的令牌有效期为2019.7.10,固定时长为15天,则请求时间2019.7.8增加固定时长15天得到第二令牌有效期2019.7.23,服务器可以将第二令牌包括的令牌有效期延长至第二令牌有效期2019.7.23。可选的,服务器也可以将请求时间增加随机时长得到第二令牌有效期,将该第二令牌包括的令牌有效期延长至第二令牌有效期。本申请实施例通过延长第二令牌的令牌有效期,可以避免用户在令牌有效期的临界时间发送业务请求时,被强制下线。

[0050] 在本申请实施例中,服务器通过接收第一客户端发送的业务请求,该业务请求中包括该第一客户端的第一标识和第一令牌,该第一令牌中包括第一令牌标识和第一版本数据,当检测到令牌存储空间中存在与该第一令牌标识相同的第二令牌标识时,获取该第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,该令牌存储空间用于存储服务器授权使用的令牌,当该第一版本数据与该第二版本数据相同且该第一标识与该第二标识相同时,向该第一客户端返回该业务请求所请求的业务数据。可以提高令牌(如JWT)鉴权的安全性。

[0051] 参见图2,是本申请实施例提供基于令牌的鉴权方法的另一示意流程图。如图2所

示,该基于令牌的鉴权方法可包括步骤:

[0052] S201,第二客户端向服务器发送登录请求。相应地,服务器接收登录请求。

[0053] 在一些可行的实施方式中,用户可以在第二客户端上输入登录信息,该登录信息可以包括用户标识(即用户账号)和密码。第二客户端可以向服务器发送登录请求,相应地,服务器接收该登录请求。该登录请求中可以包括用户标识、会话标识、用户敏感信息、客户端标识、浏览器标识、登录态时间戳等一种或多种信息。

[0054] S202,服务器根据登录请求生成第二令牌,并将第二令牌存储在令牌存储空间中。

[0055] 在一些可行的实施方式中,服务器接收到上述登录请求之后,可以将该登录请求中携带的各种信息存储在令牌存储空间(如键值存储系统Redis)中。服务器可以生成第二版本数据,并可以确定令牌有效期,其中第二版本数据可以为令牌版本号,令牌有效期可以包括令牌失效时间。服务器可以利用JWT签名算法(如HS256或RS256)对该登录请求中携带的各种信息、该第二版本数据和该令牌有效期进行加密生成签名数据(如一段标识),并可以将该签名数据作为第二令牌标识。服务器可以将该签名数据(第二令牌标识)、该第二版本数据、该令牌有效期以及该登录请求中携带的各种信息封装成第二令牌(JWT),并可以将该第二令牌存储在令牌存储空间中。可选的,服务器在生成签名数据之后,还可以根据预设规则确定第二令牌标识。服务器可以将该签名数据、该第二令牌标识、该第二版本数据、该令牌有效期以及该登录请求中携带的各种信息封装成第二令牌(JWT),并可以将该第二令牌存储在令牌存储空间中。

[0056] 在一些可行的实施方式中,服务器可以基于上述第二令牌的令牌有效期检测该第二令牌是否失效,即检测当前时间是否到达令牌失效时间。当该第二令牌的令牌有效期到达时,则服务器可以从该令牌存储空间中删除该第二令牌。可选的,服务器可以定时检测,比如每天的00:00检测令牌存储空间中存储的各个令牌是否失效。本申请实施例通过定期检测令牌存储空间中存储的各个令牌是否失效,可以及时清理失效的令牌,避免不法分子利用失效的令牌进行鉴权,且鉴权成功,导致用户的数据泄露。

[0057] 在一些可行的实施方式中,服务器可以定期更新令牌中的签名数据,即服务器每隔一段时间利用JWT签名算法重新对该登录请求中携带的各种信息、该第二版本数据和该令牌有效期进行加密生成新的签名数据,并可以生成新的令牌。

[0058] S203,服务器向第二客户端发放第二令牌。相应地,第二客户端接收第二令牌。

[0059] 在一些可行的实施方式中,服务器在生成上述第二令牌之后,可以向第二客户端发送该第二令牌,相应地,第二客户端可以接收该第二令牌。第二客户端在接收到该第二令牌之后,可以基于该第二令牌在服务器上进行鉴权。

[0060] S204,第一客户端向服务器发送业务请求。相应地,服务器接收业务请求。

[0061] S205,当检测令牌存储空间中存在与第一令牌标识相同的第二令牌标识时,服务器获取第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识。

[0062] S206,当第一版本数据与第二版本数据相同且第一标识与第二标识相同时,服务器向第一客户端返回业务请求所请求的业务数据。相应地,第一客户端接收业务请求所请求的业务数据。

[0063] 在一些可行的实施方式中,本申请实施例的步骤S204-步骤S206的实现方式可参考图1所示的实施例中步骤S101-步骤S103的实现方式,在此不再赘述。

[0064] S207,第一客户端向服务器发送退出登录请求。相应地,服务器接收退出登录请求。

[0065] S208,服务器从令牌存储空间中删除与第一令牌标识相同的第二令牌标识所标识的第二令牌。

[0066] 在一些可行的实施方式中,服务器向第一客户端返回上述业务请求所请求的业务数据之后,用户在第一客户端上点击退出登录控件时,第一客户端可以生成退出登录请求,该退出登录请求中可以携带上述第一令牌。第一客户端可以向服务器发送该退出登录请求,相应地,服务器接收该退出登录请求。服务器在接收到该退出登录请求之后,可以从该令牌存储空间(如Redis)中删除与该第一令牌标识相同的第二令牌标识所标识的第二令牌,以使该第一令牌失效,从而提高安全性。本申请实施例的令牌有效性由服务器控制,服务器可以单独使一个令牌失效。

[0067] 在另一些可行的实施方式中,服务器向第一客户端返回上述业务请求所请求的业务数据之后,用户可以在第一客户端上点击更改密码控件、忘记密码控件或注销账户控件。第一客户端可以根据用户点击不同的控件生成不同的请求,并可以向服务器发送该生成的不同的请求,其中更改密码控件对应更改密码请求,忘记密码控件对应忘记密码请求,注销账户控件对应注销账户请求。当服务器接收到更改密码请求、忘记密码请求和注销账户请求中的任一种请求时,服务器可以对该令牌存储空间(如Redis)中的上述第二版本数据进行更改,以生成新的版本数据。服务器可以利用JWT签名算法重新对该新的版本数据、令牌有效值以及上述登录请求中携带的各种信息进行加密生成新的签名数据,并可以确定新的令牌有效期。服务器可以将该新的签名数据、该新的版本数据、该新的令牌有效期以及该登录请求中携带的各种信息封装成新的令牌,并将新的令牌存储在该令牌存储空间中。可选的,服务器将新的令牌存储在该令牌存储空间中之后,可以删除该令牌存储空间中的上述第二令牌,以使上述第一令牌失效。服务器可以下发新的令牌给第一客户端。

[0068] 在本申请实施例中,服务器根据登录请求生成第二令牌并将该第二令牌发放给第二客户端,当第一客户端向服务器发送业务请求时,服务器接收第一客户端发送的业务请求,该业务请求中包括该第一客户端的第一标识和第一令牌,该第一令牌中包括第一令牌标识和第一版本数据,当检测到令牌存储空间中存在与该第一令牌标识相同的第二令牌标识时,获取该第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,该令牌存储空间用于存储服务器授权使用的令牌,当该第一版本数据与该第二版本数据相同且该第一标识与该第二标识相同时,向该第一客户端返回该业务请求所请求的业务数据。可以提高令牌(如JWT)鉴权的安全性。

[0069] 上述详细阐述了本申请实施例的基于令牌的鉴权方法,为了便于更好地实施本申请实施例的上述方案,本申请实施例还提供了相应的装置和服务器。

[0070] 参加图3,是本申请实施例提供基于令牌的鉴权装置的结构示意图。如图3所示,该基于令牌的鉴权装置100可包括:

[0071] 接收模块101,用于接收第一客户端发送的业务请求,该业务请求中包括该第一客户端的第一标识和第一令牌,该第一令牌中包括第一令牌标识和第一版本数据;

[0072] 获取模块102,用于当检测到令牌存储空间中存在与该第一令牌标识相同的第二令牌标识时,获取该第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端

的第二标识,该令牌存储空间用于存储服务器授权使用的令牌;

[0073] 发送模块103,用于当该第一版本数据与该第二版本数据相同且该第一标识与该第二标识相同时,向该第一客户端返回该业务请求所请求的业务数据。

[0074] 在一些可行的实施方式中,该基于令牌的鉴权装置100还包括生成模块104和存储模块105。该生成模块104,用于根据第二客户端发送的登录请求生成第二令牌;该存储模块105,用于将该第二令牌存储在令牌存储空间中,该第二令牌中包括第二令牌标识、该第二客户端的第二标识以及第二版本数据;上述发送模块103,还用于向该第二客户端发放该第二令牌,以使该第二客户端基于该第二令牌进行鉴权。

[0075] 在一些可行的实施方式中,上述第二令牌中还包括令牌有效期。该基于令牌的鉴权装置还包括删除模块106和有效期延长模块107。该删除模块106,用于当基于该令牌有效期检测到该第二令牌失效时,从该令牌存储空间中删除该第二令牌;该有效期延长模块107,用于对该第二令牌中包括的令牌有效期进行延长。

[0076] 在一些可行的实施方式中,该基于令牌的鉴权装置100还包括计算模块108、比较模块109以及确定模块110。该计算模块108,用于分别计算该第一版本数据的哈希值和该第二版本数据的哈希值;该比较模块109,用于比较该第一版本数据的哈希值与该第二版本数据的哈希值是否相等;该确定模块110,用于当该第一版本数据的哈希值与该第二版本数据的哈希值相等时,确定该第一版本数据与该第二版本数据相同;该确定模块110,还用于当该第一版本数据的哈希值与该第二版本数据的哈希值不相等时,确定该第一版本数据与该第二版本数据不相同。

[0077] 在一些可行的实施方式中,上述发送模块103,还用于当检测到该令牌存储空间中不存在与该第一令牌标识相同的第二令牌标识时,针对该业务请求返回请求失败响应,该请求失败响应用于拒绝该业务请求。

[0078] 在一些可行的实施方式中,该基于令牌的鉴权装置100还包括数据脱敏模块111。上述发送模块103,还用于当该第一版本数据与该第二版本数据不相同或该第一标识与该第二标识不相同时,针对该业务请求返回请求失败响应,该请求失败响应用于拒绝该业务请求;该数据脱敏模块111,用于当该第一标识与该第二标识不相同时,对该业务请求所请求的业务数据进行数据脱敏处理,得到目标业务数据;上述发送模块103,还用于向该第一客户端返回该目标业务数据。

[0079] 在一些可行的实施方式中,上述删除模块106,还用于当接收到该第一客户端发送的退出登录请求时,从该令牌存储空间中删除与该第一令牌标识相同的该第二令牌标识所标识的第二令牌。

[0080] 其中,上述获取模块102、上述生成模块104、上述存储模块105、上述删除模块106、上述有效期延长模块107、上述计算模块108、上述比较模块109、上述确定模块110以及上述数据脱敏模块111可以为一个模块,如处理模块。

[0081] 具体实现中,各个模块和/或单元的实现还可以对应参照图1或图2所示的方法实施例中的服务器的相应描述,执行上述实施例中服务器所执行的方法和功能。

[0082] 在本申请实施例中,基于令牌的鉴权装置通过接收第一客户端发送的业务请求,该业务请求中包括该第一客户端的第一标识和第一令牌,该第一令牌中包括第一令牌标识和第一版本数据,当检测到令牌存储空间中存在与该第一令牌标识相同的第二令牌标识

时,获取该第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,该令牌存储空间用于存储服务器授权使用的令牌,当该第一版本数据与该第二版本数据相同且该第一标识与该第二标识相同时,向该第一客户端返回该业务请求所请求的业务数据。可以提高令牌(如JWT)鉴权的安全性。

[0083] 参见图4,是本申请实施例提供的服务器的结构示意图。如图4所示,本申请实施例中的服务器可以包括:一个或多个处理器401;一个或多个输入设备402,一个或多个输出设备403和存储器404。上述处理器401、输入设备402、输出设备403和存储器404通过总线405连接。存储器404用于存储计算机程序,所述计算机程序包括程序指令,处理器401用于执行存储器402存储的程序指令。

[0084] 其中,上述输入设备402用于接收第一客户端发送的业务请求,该业务请求中包括该第一客户端的第一标识和第一令牌,该第一令牌中包括第一令牌标识和第一版本数据。上述处理器401被配置用于调用所述程序指令执行:当检测到令牌存储空间中存在与该第一令牌标识相同的第二令牌标识时,获取该第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识,该令牌存储空间用于存储服务器授权使用的令牌。上述输出设备403用于当该第一版本数据与该第二版本数据相同且该第一标识与该第二标识相同时,向该第一客户端返回该业务请求所请求的业务数据。

[0085] 应当理解,在本申请实施例中,所称处理器401可以是中央处理单元(Central Processing Unit,CPU),该处理器还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0086] 输入设备402可以包括输入接口,输出设备403可以包括输出接口。

[0087] 该存储器404可以包括只读存储器和随机存取存储器,并向处理器401提供指令和数据。存储器404的一部分还可以包括非易失性随机存取存储器。例如,存储器404还可以存储设备类型的信息。

[0088] 具体实现中,本申请实施例中所描述的处理器401、输入设备402、输出设备403可执行本申请实施例提供的基于令牌的鉴权方法中所描述的实现方式,也可执行本申请实施例所描述的基于令牌的鉴权装置的实现方式,在此不再赘述。

[0089] 本申请实施例还提供一种计算机可读存储介质,该计算机可读存储介质存储有计算机程序,该计算机程序包括程序指令,该程序指令被处理器执行时实现图1或图2所示的基于令牌的鉴权方法,具体细节请参照图1或图2所示实施例的描述,在此不再赘述。

[0090] 上述计算机可读存储介质可以是前述任一实施例所述的基于令牌的鉴权装置或电子设备的内部存储单元,例如电子设备的硬盘或内存。该计算机可读存储介质也可以是该电子设备的外部存储设备,例如该电子设备上配备的插接式硬盘,智能存储卡(smart media card,SMC),安全数字(secure digital,SD)卡,闪存卡(flash card)等。进一步地,该计算机可读存储介质还可以既包括该电子设备的内部存储单元也包括外部存储设备。该计算机可读存储介质用于存储该计算机程序以及该电子设备所需的其他程序和数据。该计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

[0091] 本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、计算机软件或者二者的结合来实现,为了清楚地说明硬件和软件的可互换性,在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。

[0092] 本申请是参照本申请实施例的方法、装置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诊疗数据的处理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诊疗数据的处理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。

[0093] 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诊疗数据的处理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。

[0094] 这些计算机程序指令也可装载到计算机或其他可编程诊疗数据的处理设备上,使得在计算机或其他可编程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。

[0095] 尽管结合具体特征及其实施例对本申请进行了描述,显而易见的,在不脱离本申请的精神和范围的情况下,可对其进行各种修改和组合。相应地,本说明书和附图仅仅是所附权利要求所界定的本申请的示例性说明,且视为已覆盖本申请范围内的任意和所有修改、变化、组合或等同物。显然,本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样,倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内,则本申请也意图包含这些改动和变型在内。

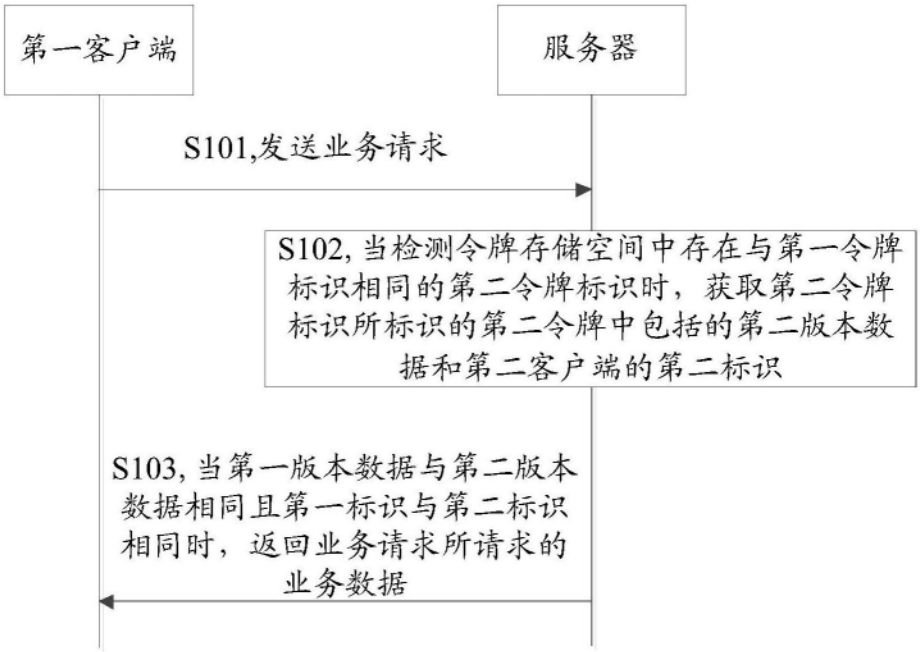

第一客户端
服务器
S101,发送业务请求
S102,当检测令牌存储空间中存在与第一令牌标识相同的第二令牌标识时，获取第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识
S103,当第一版本数据与第二版本数据相同且第一标识与第二标识相同时，返回业务请求所请求的业务数据

图1

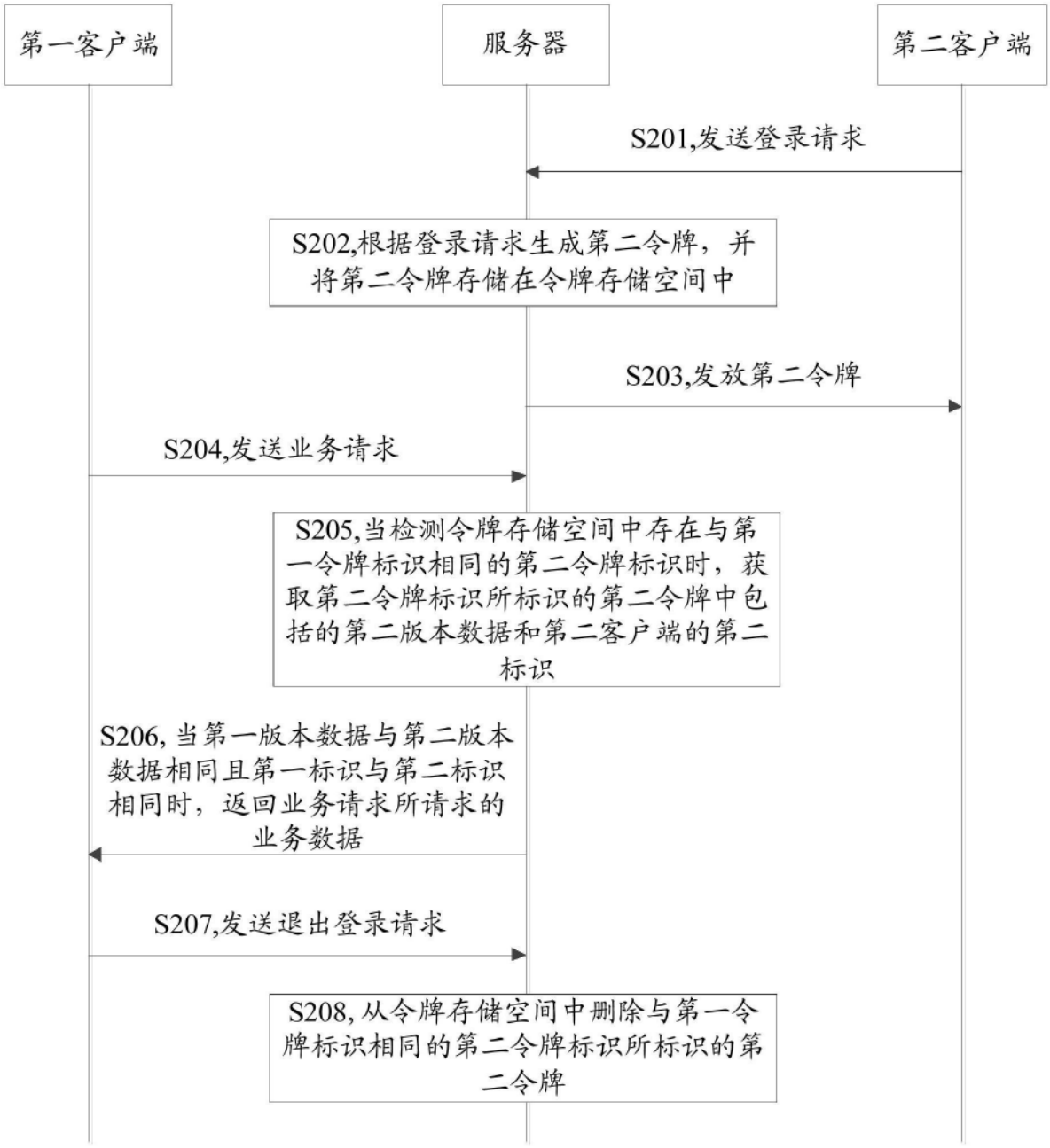

第一客户端
服务器
第二客户端
S201,发送登录请求
S202,根据登录请求生成第二令牌，并将第二令牌存储在令牌存储空间中
S203,发放第二令牌
S204,发送业务请求
S205,当检测令牌存储空间中存在与第一令牌标识相同的第二令牌标识时，获取第二令牌标识所标识的第二令牌中包括的第二版本数据和第二客户端的第二标识
S206,当第一版本数据与第二版本数据相同且第一标识与第二标识相同时，返回业务请求所请求的业务数据
S207,发送退出登录请求
S208,从令牌存储空间中删除与第一令牌标识相同的第二令牌标识所标识的第二令牌

图2

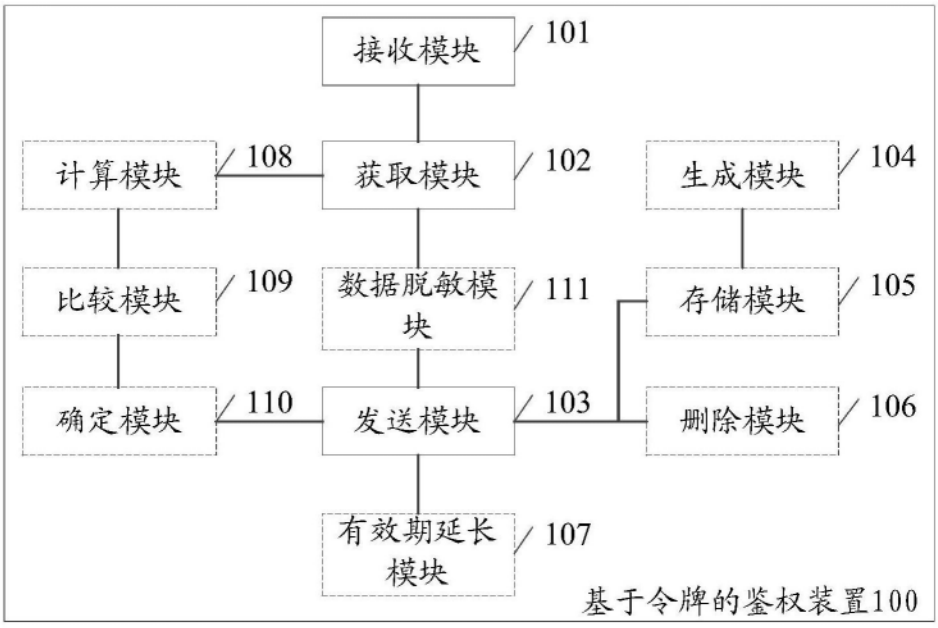

接收模块
101
计算模块
108
获取模块
102
生成模块
104
比较模块
109
数据脱敏模块
111
存储模块
105
确定模块
110
发送模块
103
删除模块
106
有效期延长模块
107
基于令牌的鉴权装置100

图3

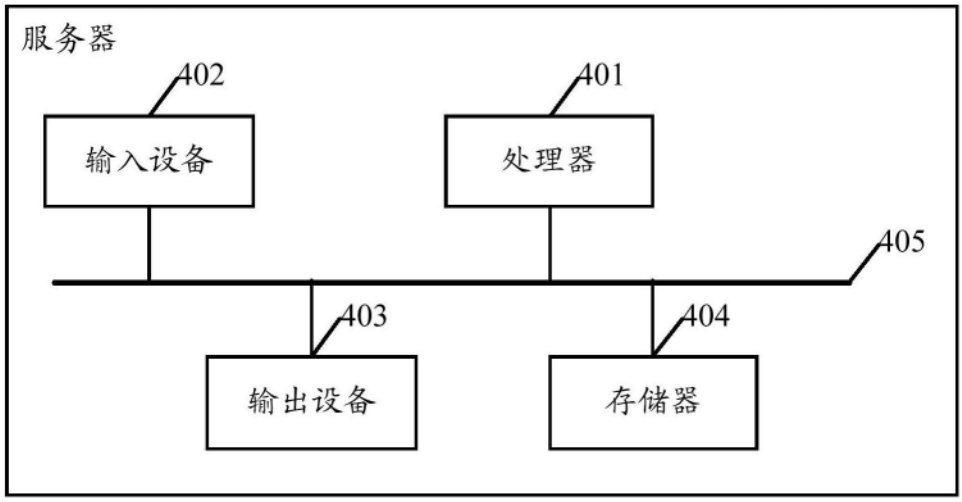

服务器
402
输入设备
401
处理器
405
403
输出设备
404
存储器

图4