(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113225351 B
(45)授权公告日 2022.12.13

(21)申请号 202110590433.7

(22)申请日 2021.05.28

(65)同一申请的已公布的文献号
申请公布号 CN 113225351 A

(43)申请公布日 2021.08.06

(73)专利权人 中国建设银行股份有限公司
地址 100033 北京市西城区金融大街25号

(72)发明人 程超 赖治国 谢发川 陶琛浩 陶昌云

(74)专利代理机构 北京品源专利代理有限公司 11332
专利代理师 孟金喆

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/60(2022.01)

(56)对比文件
CN 112187724 A,2021.01.05
CN 109857484 A,2019.06.07
CN 105491001 A,2016.04.13
CN 109101797 A,2018.12.28
CN 109547445 A,2019.03.29
CN 112688963 A,2021.04.20
CN 109450649 A,2019.03.08
US 2010192210 A1,2010.07.29

审查员 孙志飞

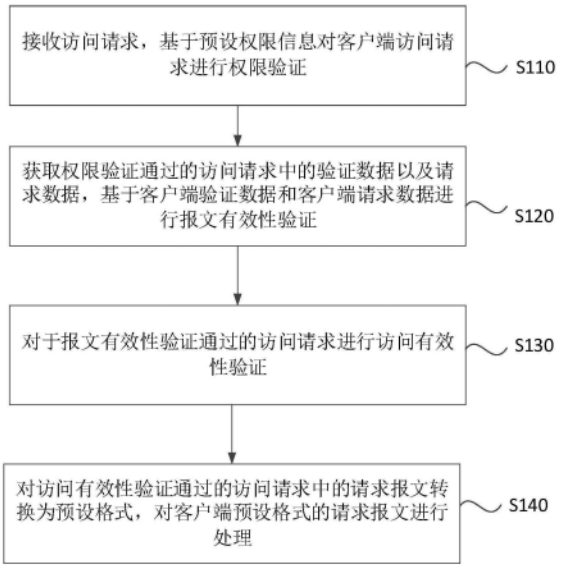
权利要求书3页 说明书13页 附图2页

(54)发明名称

一种请求处理方法、装置、存储介质及电子设备

(57)摘要

本发明涉及自动程序设计领域，公开了一种请求处理方法、装置、存储介质及电子设备。该方法包括：接收访问请求，基于预设权限信息对所述访问请求进行权限验证；获取权限验证通过的访问请求中的验证数据以及请求数据，基于所述验证数据和所述请求数据进行报文有效性验证；对于报文有效性验证通过的访问请求进行访问有效性验证；对访问有效性验证通过的访问请求中的请求报文转换为预设格式，对所述预设格式的请求报文进行处理。通过本发明实施例公开的技术方案，实现了提高应用接口的安全性和可靠性。



CN 113225351 B

1.一种请求处理方法,其特征在于,包括:

接收访问请求,基于预设权限信息对所述访问请求进行权限验证;其中,所述预设权限信息指云服务基于应用访问接口设置的各阈值信息,用于对客户端上传的访问请求进行安全过滤;

获取权限验证通过的访问请求中的验证数据以及请求数据,基于所述验证数据和所述请求数据进行报文有效性验证;

对于报文有效性验证通过的访问请求进行访问有效性验证;

对访问有效性验证通过的访问请求中的请求报文转换为预设格式,对所述预设格式的请求报文进行处理;

其中,所述基于预设权限信息对所述访问请求进行权限验证,包括:

获取访问权限白名单,确定所述访问请求的url地址是否在所述访问权限白名单中;

若是,则确定所述访问请求的权限验证为通过;

若所述访问请求的url地址不在所述访问权限白名单中,则提取所述访问请求的请求头中的token信息;

基于所述token信息确定所述访问请求对应的应用标识,确定所述应用标识是否在所述访问权限白名单内;

若是,则确定所述访问请求的权限验证为通过。

2.根据权利要求1所述的方法,其特征在于,所述验证数据包括预设签名,所述请求数据包括请求报文,所述报文有效性验证包括签名验证;

所述基于所述验证数据和所述请求数据进行报文有效性验证,包括:

对所述访问请求的请求头中的请求报文进行解密,得到解密报文;

基于所述解密报文生成验证签名,将所述验证签名与所述预设签名进行比对,若所述验证签名与所述预设签名比对成功,则确定所述请求数据的签名验证成功。

3.根据权利要求2所述的方法,其特征在于,所述基于所述解密报文生成验证签名,包括:

获取所述访问请求的请求头中设置的随机数、时间戳、应用秘钥、应用标识中的至少一项;

基于所述随机数、时间戳、应用秘钥、应用标识中的至少一项以及所述解密报文,根据预设拼接方式形成验证签名。

4.根据权利要求2所述的方法,其特征在于,所述验证数据还包括预设加密信息,所述报文有效性验证还包括加密验证;

所述基于所述验证数据和所述请求数据进行报文有效性验证,包括:

对所述解密报文进行至少一种预设加密方式的加密处理,得到验证加密信息,将所述验证加密信息与所述预设加密信息进行比对;

若所述验证加密信息与所述预设加密信息比对成功,则确定所述请求数据的加密验证成功。

5.根据权利要求2所述的方法,其特征在于,所述验证数据还包括有效时间间隔;所述报文有效性验证还包括时间戳验证;

所述基于所述验证数据和所述请求数据进行报文有效性验证,包括:

确定所述访问请求中的时间戳以及当前时间戳是否满足有效时间间隔，若是，则确定所述访问请求时间戳验证通过。

6.根据权利要求1所述的方法，其特征在于，所述访问有效性验证包括失效日期验证；

对于报文有效性验证通过的访问请求进行访问有效性验证，包括：

获取所述请求头中token信息的失效期，基于当前时间戳和所述失效期确定所述token信息是否失效；

若是，则向发送所述访问请求的客户端发送错误信息，以使所述客户端重新获取token信息

若否，则确定所述访问请求的失效日期验证通过。

7.根据权利要求6所述的方法，其特征在于，所述访问有效性验证还包括访问接口验证；

对于报文有效性验证通过的访问请求进行访问有效性验证，包括：

基于所述访问请求中的应用标识，确定所述应用标识对应的可访问接口；

确定所述访问请求当前的访问接口是否为所述应用标识对应的可访问接口，若是，则确定所述访问请求的访问接口验证通过。

8.根据权利要求1所述的方法，其特征在于，在接收访问请求之后，所述方法还包括：

监测当前请求流量，若所述当前请求流量满足限流条件，则调用预设的限流规则，对接收的各访问请求进行限流。

9.根据权利要求1所述的方法，其特征在于，在接收访问请求之后，所述方法还包括：

基于所述访问请求的IP地址和预先设置的IP地址黑名单进行验证；

若所述访问请求的IP地址在所述IP地址黑名单内，则拒绝所述访问请求。

10.根据权利要求9所述的方法，其特征在于，所述方法还包括：

获取访问日志，基于所述预先设置的IP地址黑名单对所述访问日志进行数据过滤；

统计过滤后的访问日志中，各IP地址的访问频率，将满足恶意访问频率的IP地址添加至所述预先设置的IP地址黑名单中。

11.根据权利要求10所述的方法，其特征在于，在基于所述预先设置的IP地址黑名单对所述访问日志进行数据过滤之后，所述方法还包括：

确定过滤后的访问日志中各访问请求的调用对象；

若所述调用对象为预先设置的非法调用对象，则将所述访问请求的IP地址添加至所述预先设置的IP地址黑名单中。

12.一种请求处理装置，其特征在于，包括：

权限验证模块，用于接收访问请求，基于预设权限信息对所述访问请求进行权限验证；其中，所述预设权限信息指云服务基于应用访问接口设置的各阈值信息，用于对客户端上传的访问请求进行安全过滤；

报文有效性验证模块，用于获取权限验证通过的访问请求中的验证数据以及请求数据，基于所述验证数据和所述请求数据进行报文有效性验证；

访问有效性验证模块，用于对于报文有效性验证通过的访问请求进行访问有效性验证；

报文处理模块，用于对访问有效性验证通过的访问请求中的请求报文转换为预设格

式,对所述预设格式的请求报文进行处理;

其中,所述权限验证模块,包括:

白名单获取单元,用于获取访问权限白名单,确定所述访问请求的url地址是否在所述访问权限白名单中;

第一权限验证单元,用于若所述访问请求的url地址在所述访问权限白名单中,则确定所述访问请求的权限验证为通过;

token信息提取单元,用于若所述访问请求的url地址不在所述访问权限白名单中,则提取所述访问请求的请求头中的token信息;

应用标识验证单元,用于基于所述token信息确定所述访问请求对应的应用标识,确定所述应用标识是否在所述访问权限白名单内;

第二权限验证单元,用于若所述应用标识在所述访问权限白名单内,则确定所述访问请求的权限验证为通过。

13.一种电子设备,其特征在于,包括:

一个或多个处理器;

存储装置,用于存储一个或多个程序,

当所述一个或多个程序被所述一个或多个处理器执行,使得所述一个或多个处理器实现如权利要求1-11中任一所述的请求处理方法。

14.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-11中任一所述的请求处理方法。

一种请求处理方法、装置、存储介质及电子设备

技术领域

[0001] 本发明实施例涉及自动程序设计领域，尤其涉及一种请求处理方法、装置、存储介质及电子设备。

背景技术

[0002] 随着计算机技术的发展，应用程序对外提供开放接口的需求越来越多。

[0003] 但是各个内部微服务对接标准不统一，将导致API接口的可持续开发和可维护变得越来越难，对外开放接口的安全性、高可靠性、可维护性得不到保证。

发明内容

[0004] 本发明实施例提供一种请求处理方法、装置、存储介质及电子设备，以实现提高应用接口的安全性和可靠性。

[0005] 第一方面，本发明实施例提供了一种请求处理方法，该方法包括：

[0006] 接收访问请求，基于预设权限信息对所述访问请求进行权限验证；

[0007] 获取权限验证通过的访问请求中的验证数据以及请求数据，基于所述验证数据和所述请求数据进行报文有效性验证；

[0008] 对于报文有效性验证通过的访问请求进行访问有效性验证；

[0009] 对访问有效性验证通过的访问请求中的请求报文转换为预设格式，对所述预设格式的请求报文进行处理。

[0010] 可选的，所述基于预设权限信息对所述访问请求进行权限验证，包括：

[0011] 获取访问权限白名单，确定所述访问请求的url地址是否在所述访问权限白名单中；

[0012] 若是，则确实所述访问请求的权限验证为通过。

[0013] 可选的，所述方法还包括：

[0014] 若所述访问请求的url地址不在所述访问权限白名单中，则提取所述访问请求的请求头中的token信息；

[0015] 基于所述token信息确定所述访问请求对应的应用标识，确定所述应用标识是否在所述访问权限白名单内；

[0016] 若是，则确实所述访问请求的权限验证为通过。

[0017] 可选的，所述验证数据包括预设签名，所述请求数据包括请求报文，所述报文有效性验证包括签名验证；

[0018] 所述基于所述验证数据和所述请求数据进行报文有效性验证，包括：

[0019] 对所述访问请求的请求头中的请求报文进行解密，得到解密报文；

[0020] 基于所述解密报文生成验证签名，将所述验证签名与所述预设签名进行比对，若所述验证签名与所述预设签名比对成功，则确定所述请求数据的签名验证成功。

[0021] 可选的，所述基于所述解密报文生成验证签名，包括：

[0022] 获取所述访问请求的请求头中设置的随机数、时间戳、应用秘钥、应用标识中的至少一项；

[0023] 基于所述随机数、时间戳、应用秘钥、应用标识中的至少一项以及所述解密报文，根据预设拼接方式形成验证签名。

[0024] 可选的，所述验证数据还包括预设加密信息，所述报文有效性验证还包括加密验证；

[0025] 所述基于所述验证数据和所述请求数据进行报文有效性验证，包括：

[0026] 对所述解密报文进行至少一种预设加密方式的加密处理，得到验证加密信息，将所述验证加密信息与所述预设加密信息进行比对；

[0027] 若所述验证加密信息与所述预设加密信息比对成功，则确定所述请求数据的加密验证成功。

[0028] 可选的，所述验证数据还包括有效时间间隔；所述报文有效性验证还包括时间戳验证；

[0029] 所述基于所述验证数据和所述请求数据进行报文有效性验证，包括：

[0030] 确定所述访问请求中的时间戳以及当前时间戳是否满足有效时间间隔，若是，则确定所述访问请求时间戳验证通过。

[0031] 可选的，所述访问有效性验证包括失效日期验证；

[0032] 对于报文有效性验证通过的访问请求进行访问有效性验证，包括：

[0033] 获取所述请求头中token信息的失效期，基于当前时间戳和所述失效期确定所述token信息是否失效；

[0034] 若是，则向发送所述访问请求的客户端发送错误信息，以使所述客户端重新获取token信息；

[0035] 若否，则确定所述访问请求的失效日期验证通过。

[0036] 可选的，所述访问有效性验证还包括访问接口验证；

[0037] 对于报文有效性验证通过的访问请求进行访问有效性验证，包括：

[0038] 基于所述访问请求中的应用标识，确定所述应用标识对应的可访问接口；

[0039] 确定所述访问请求当前的访问接口是否为所述应用标识对应的可访问接口，若是，则确定所述访问请求的访问接口验证通过。

[0040] 可选的，在接收访问请求之后，所述方法还包括：

[0041] 监测当前请求流量，若所述当前请求流量满足限流条件，则调用预设的限流规则，对接收的各访问请求进行限流。

[0042] 可选的，在接收访问请求之后，所述方法还包括：

[0043] 基于所述访问请求的IP地址和预先设置的IP地址黑名单进行验证；

[0044] 若所述访问请求的IP地址在所述IP地址黑名单内，则拒绝所述访问请求。

[0045] 可选的，所述方法还包括：

[0046] 获取访问日志，基于所述预先设置的IP地址黑名单对所述访问日志进行数据过滤；

[0047] 统计过滤后的访问日志中，各IP地址的访问频率，将满足恶意访问频率的IP地址添加至所述预先设置的IP地址黑名单中。

[0048] 可选的，在基于所述预先设置的IP地址黑名单对所述访问日志进行数据过滤之后，所述方法还包括：

[0049] 确定过滤后的访问日志中各访问请求的调用对象；

[0050] 若所述调用对象为预先设置的非法调用对象，则将所述访问请求的IP地址添加至所述预先设置的IP地址黑名单中。

[0051] 可选的，在基于所述预先设置的IP地址黑名单对所述访问日志进行数据过滤之后，所述方法还包括：

[0052] 确定过滤后的访问日志中各访问请求的调用对象；

[0053] 若所述调用对象为预先设置的非法调用对象，则将所述访问请求的IP地址添加至所述预先设置的IP地址黑名单中。

[0054] 第二方面，本发明实施例还提供了一种请求处理装置，该装置包括：

[0055] 权限验证模块，用于接收访问请求，基于预设权限信息对所述访问请求进行权限验证；

[0056] 报文有效性验证模块，用于获取权限验证通过的访问请求中的验证数据以及请求数据，基于所述验证数据和所述请求数据进行报文有效性验证；

[0057] 访问有效性验证模块，用于对于报文有效性验证通过的访问请求进行访问有效性验证；

[0058] 报文处理模块，用于对访问有效性验证通过的访问请求中的请求报文转换为预设格式，对所述预设格式的请求报文进行处理。

[0059] 第三方面，本发明实施例还提供了一种电子设备，所述电子设备包括：

[0060] 一个或多个处理器；

[0061] 存储装置，用于存储一个或多个程序，

[0062] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如本发明任意实施例提供的请求处理方法。

[0063] 第四方面，本发明实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现本发明任意实施例提供的请求处理方法。

[0064] 本发明实施例的技术方案具体包括：接收客户端发送的访问请求，并且基于预设权限信息对该访问请求进行权限验证，过滤没有权限的访问请求，以实现对客户端的访问请求进行初步过滤，保证了访问的安全性；获取权限验证通过的访问请求中的验证数据以及请求数据，并基于验证数据和请求数据进行报文有效性验证，过滤掉报文无效的访问请求，进一步保证了访问的安全性；对报文有效性验证通过的访问请求进行访问有效性验证，确保当前进行访问请求访问的访问接口的正确性，再次的保证了访问请求的安全性；对访问有效性验证通过的访问请求中的请求报文转换为预设格式，对该预设格式的请求报文进行处理，保证了访问请求的请求内容的规范性；本发明实施例的技术方案通过对访问请求进行逐步验证，以及对通过各项验证的访问请求进行预设格式的处理，实现了提高应用接口的安全性和可靠性。

附图说明

[0065] 为了更加清楚地说明本发明示例性实施例的技术方案，下面对描述实施例中所需

要用到的附图做一简单介绍。显然，所介绍的附图只是本发明所要描述的一部分实施例的附图，而不是全部的附图，对于本领域普通技术人员，在不付出创造性劳动的前提下，还可以根据这些附图得到其他的附图。

[0066] 图1是本发明实施例一提供的请求处理方法的流程示意图；

[0067] 图2是本发明实施例三提供的请求处理装置的结构示意图；

[0068] 图3为本发明实施例四提供的电子设备的结构示意图。

具体实施方式

[0069] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结构。

[0070] 实施例一

[0071] 图1为本发明实施例一提供的一种请求处理方法的流程图，本实施例可适用于对客户端发送的访问请求能行处理的情况。该方法可以由请求处理装置来执行，该装置可以由软件和/或硬件的方式来实现。如图1所示，该方法具体包括以下步骤：

[0072] S110、接收访问请求，基于预设权限信息对客户端访问请求进行权限验证。

[0073] 在本发明实施例中，访问请求是客户端基于互联网区交易向云服务发送访问请求，以使云服务对该访问请求中的请求内容进行处理。预设权限信息为云服务基于应用访问接口设置的各阈值信息，用于对客户端上传的访问请求进行安全过滤。权限验证即对该访问请求进行是否有权限进入该云服务的初步验证，具体的，该权限验证在web层进行处理。

[0074] 具体的，云服务预先设置权限信息，并在接收到客户端发送的访问请求时，基于该预设权限信息对该访问请求进行权限验证，以保证云服务访问接口的安全性。

[0075] 可选的，于预设权限信息对客户端访问请求进行权限验证的方法可以是：获取访问权限白名单，确定客户端访问请求的url地址是否在客户端访问权限白名单中；若是，则确实客户端访问请求的权限验证为通过。其中，白名单为预先设置在redis数据包中的具有访问权限的名单，该redis数据库中包括有各有权限的url地址以及有访问权限的客户端的应用标识。

[0076] 具体的，获取访问请求中的url地址，基于云服务的openresty的access_by_lua_file模块将访问请求中的url地址与预设白名单中的url地址进行比对验证；若该url地址比对成功，则说明书该访问请求是具有访问权项的访问请求，即该访问请求的权限验证为通过。为了避免因为访问请求的地址没有更换而错误拦截有访问权限的访问请求的情况，进一步的，获取访问请求的请求头的token，并根据该token确定其对应的应用标识；将其应用标识与白名单中的各应用标识进行比对，若比对一致，则说明该应用标识对应的访问请求验证为通过。

[0077] S120、获取权限验证通过的访问请求中的验证数据以及请求数据，基于客户端验证数据和客户端请求数据进行报文有效性验证。

[0078] 在本发明实施例中，验证数据为云服务预先设置的验证数据，用于对通过权限验证的访问请求进行报文有效性验证的数据。请求数据为接收到的通过权限验证的访问请求

的请求数据。报文有效性验证为对具有访问权限的访问请求进行的该访问请求的请求报文是否为有效报文的验证，具体的，该报文有效性验证在api网关层进行验证。

[0079] 可选的，当验证数据包括预设签名时，请求数据包括请求报文时，该报文有效性验证包括签名验证；相应的，基于验证数据和请求数据进行报文有效性验证的方法可以是：对客户端访问请求的请求头中的请求报文进行解密，得到解密报文；基于客户端解密报文生成验证签名，将客户端验证签名与客户端预设签名进行比对，若客户端验证签名与客户端预设签名比对成功，则确定客户端请求数据的签名验证成功。

[0080] 具体的，采用预设的解密方式对通过权限验证的访问请求的请求头的中的请求报文进行解密得到解密报文，例如基于应用标识获得该访问请求的方法秘钥(ase key)以及应用秘钥(app secret)，并基于该方法秘钥和应用秘钥对该请求报文进行解密得到解密报文。具体的，生成的解密报文包括访问请求的请求头中设置的随机数、时间戳、应用秘钥、应用标识中的至少一项。可选的，基于客户端解密报文生成验证签名的方法可以是基于客户端随机数、时间戳、应用秘钥、应用标识中的至少一项以及客户端解密报文，根据预设拼接方式形成验证签名。示例性的，验证签名可以是：app secret+time stamp+aes key+encrpt data+nonce+app secret。预设签名可以是预先设置的signture签名。将基于解密报文生成的验证签名作为请求数据，将预先设置的预设签名作为验证数据，将验证数据与请求数据进行比对；当两个数据比对结果一致时，则确定客户端请求数据的签名验证成功。

[0081] 在上述实施例的基础上，该验证数据还包括预设加密信息，请求数据包括请求加密信息，则该报文有效性验证还包括加密验证；相应的，基于验证数据和请求数据进行报文有效性验证的方法可以是：对客户端解密报文进行至少一种预设加密方式的加密处理，得到验证加密信息，将客户端验证加密信息与客户端预设加密信息进行比对；若客户端验证加密信息与客户端预设加密信息比对成功，则确定客户端请求数据的加密验证成功。

[0082] 其中，预设加密方式的加密处理可以是Base64加密方式、MD5加密方式、钥匙串加密方式、对称加密算法以及非对称加密算法等加密方式。其中，即可以选择上述加密方式中任一作为预设加密方式，也可以选择两种及以上加密方式作为预设加密方式对解密报文进行加密处理得到验证加密信息。预先设置Content-MD5为预设加密信息。将验证加密信息作为请求数据，将预设加密信息作为验证数据，将该验证数据和请求数据进行比对；当比对结果一致，则确定客户端请求数据的加密验证成功。

[0083] 在上述实施例的基础上，验证数据还包括有效时间间隔，请求数据还包括访问请求的时间数据，则该报文有效性验证还包括时间戳验证；相应的，基于验证数据和请求数据进行报文有效性验证的方法可以是：确定客户端访问请求中的时间戳以及当前时间戳是否满足有效时间间隔，若是，则确定客户端访问请求时间戳验证通过。

[0084] 具体的，确定访问请求中访问的时间数据，并将该请求时间数据距离验证时的时间间隔作为请求数据；预先确定访问请求的有效时间间隔作为验证数据；将两个时间间隔进行比对，若请求数据的时间间隔小于验证数据的时间间隔，则确定客户端请求数据的时间戳验证成功。

[0085] 当然，上述基于请求数据和验证数据对该访问请求的报文有效性验证只是作为可选实施例，也可以基于实际情况对验证数据、请求数据以及报文有效性的验证方法进行具体设置，本实施例对此不加以限制。

[0086] S130、对于报文有效性验证通过的访问请求进行访问有效性验证。

[0087] 在本发明实施例中，客户端的访问请求可以发送给云服务的多个访问接口；云服务的多个访问接口可以接收多个客户端发送的访问请求，预先在云服务端上设置该访问接口可以接收的访问请求，即访问有效性验证则是对当前访问请求是否为当前访问接口允许访问的访问请求之一。

[0088] 可选的，对报文有效性验证通过的访问请求进行访问有效性验证的方法可以是：获取客户端请求头中token信息的失效期，基于当前时间戳和客户端失效期确定客户端token信息是否失效；若是，则向发送客户端访问请求的客户端发送错误信息，以使客户端客户端重新获取token信息；若否，则确定客户端访问请求的失效日期验证通过。其中，token信息的失效期可以是云服务预先设置的当前token时效的时间点。错误信息可以是证明当前token过期的消息。

[0089] 具体的，获取到该访问请求的请求头中的token信息中携带的访问时间戳，并将该时间戳与预设的token失效期(access_token)中的时间点进行比对。如果时间戳在失效期时间点之前，则说明该时间戳未失效，即确定客户端访问请求的失效日期验证通过；如果时间戳在失效期时间点之后，则说明该时间戳失效，即确定客户端访问请求的失效日期验证未通过，需要向发送访问请求的服务端反馈需重新获取token的错误信息，以使客户端客户端重新获取token信息。

[0090] 在上述实施例的基础上，对报文有效性验证通过的访问请求进行访问有效性验证的方法还可以是：基于客户端访问请求中的应用标识，确定客户端应用标识对应的可访问接口；确定客户端访问请求当前的访问接口是否为客户端应用标识对应的可访问接口，若是，则确定客户端访问请求的访问接口验证通过。

[0091] 具体的，获取云服务预设的当前访问接口的允许访问的访问列表，该访问列表存储有允许访问的客户端的各应用的应用标识。获取访问请求的请求报文中的service Id对应的应用标识(app ID)，并将该应用标识与访问列表中存储的各应用标识进行比对；若比对结果一致，则说明当前访问请求为允许当前访问接口访问的标识，确定客户端访问请求的访问接口验证通过。

[0092] S140、对访问有效性验证通过的访问请求中的请求报文转换为预设格式，对客户端预设格式的请求报文进行处理。

[0093] 在本发明实施例中，获取通过访问有效性的访问请求中的请求报文，并将该请求报文转换为预设格式，以使待处理的请求报文为统一格式，并根据请求报文的报文内容对该预设格式的请求报文进行处理，有利于后续对多个访问请求中的请求报文进行维护。

[0094] 在上述实施例的基础上，当交易访问频繁时，过多的访问请求会对当前访问接口造成处理压力，为了缓解当前访问接口的处理压力，需要对各访问请求进行限流处理。可选的，对访问请求进行限流处理的方法可以是：监测当前请求流量，若客户端当前请求流量满足限流条件，则调用预设的限流规则，对接收的各访问请求进行限流。

[0095] 具体的，云服务中引入Sentinel，Sentinel控制台提供一个轻量级的控制台，该控制台提供机器发现、单机资源实时监控、集群资源汇总以及规则管理的功能；进一步的，云服务还引入Sentinel相关JAR包，安装Sentinel控制台，在控制台根据交易访问添加相应限流策略，如QPS限流，线程数限流；当达到预先配置的限流条件时，流控生效；即需要在

Sentinel能看见各个接口访问情况，并做出相应流控规则调整。

[0096] 在上述实施例的基础上，在接收访问请求之后，基于客户端访问请求的IP地址和预先设置的IP地址黑名单进行验证；若客户端访问请求的IP地址在客户端IP地址黑名单内，则拒绝客户端访问请求。

[0097] 具体的，获取当前访问请求的IP地址，并将该IP地址和预设的IP地址黑名单进行比对验证；若当前访问请求的IP地址与预设IP地址黑名单中的IP地址比对成功，则说明当前IP地址为非法访问，则拒绝该访问请求，以实现降低因恶意访问给当前访问接口造成的处理压力。

[0098] 在上述实施例的基础上，确定IP地址黑名单的方法还可以是：获取访问日志，基于客户端预先设置的IP地址黑名单对客户端访问日志进行数据过滤；统计过滤后的访问日志中，各IP地址的访问频率，将满足恶意访问频率的IP地址添加至客户端预先设置的IP地址黑名单中。

[0099] 具体的，获取当前访问接口的访问日志以及预先设置的IP地址黑名单列表，并基于该黑明单列表统计访问当前访问接口的各访问请求的IP地址；获取各IP地址的访问频率，将满足恶意访问频率的IP地址作为IP地址黑名单，并基于该IP地址更新原有的IP地址黑明单列表，以便于及时发现非法访问的IP地址，降低因为恶意访问给当前访问接口的处理压力。

[0100] 在上述实施例的基础上，确定IP地址黑名单的方法还可以是：在基于客户端预先设置的IP地址黑名单对客户端访问日志进行数据过滤之后，确定过滤后的访问日志中各访问请求的调用对象；若客户端调用对象为预先设置的非法调用对象，则将客户端访问请求的IP地址添加至客户端预先设置的IP地址黑名单中。

[0101] 本发明实施例的技术方案具体包括：接收客户端发送的访问请求，并且基于预设权限信息对该访问请求进行权限验证，过滤没有权限的访问请求，以实现对客户端的访问请求进行初步过滤，保证了访问的安全性；获取权限验证通过的访问请求中的验证数据以及请求数据，并基于验证数据和请求数据进行报文有效性验证，过滤掉报文无效的访问请求，进一步保证了访问的安全性；对报文有效性验证通过的访问请求进行访问有效性验证，确保当前进行访问请求访问的访问接口的正确性，再次的保证了访问请求的安全性；对访问有效性验证通过的访问请求中的请求报文转换为预设格式，对该预设格式的请求报文进行处理，保证了访问请求的请求内容的规范性；本发明实施例的技术方案通过对访问请求进行逐步验证，以及对通过各项验证的访问请求进行预设格式的处理，实现了提高应用接口的安全性和可靠性。

[0102] 实施例二

[0103] 本实施例在上述各实施例的基础上，增加了客户端中的应用向云服务发送访问请求的交互过程，其中与上述各实施例相同或相应的术语的解释在此不再赘述。

[0104] 在本发明实施例中，该交互过程具体包括：

[0105] 应用(app)在客户端安装后第一次打开，app使用保存在app中的默认秘钥对传输的数据(设备唯一标识符device Id、设备类型(安卓/IOS/POS)，设备型号等)加密，获取app ID及app secret客户端将app ID和app secret加密存储到系统本地。进一步的，客户端发起初始化在检查手机本地系统中没有加密存储的app ID和app secret情况下发起，即设备

未初始化。API网关层会将app ID,app secret,device ID以及设备其他信息存储到数据库中,以便于后期的信息查询。

[0106] 可选的,设备初始化后发起交易,或者客户端正常启动发起交易,获取客户端内存中的存放的token,如果token不存在,则发起获取token的交易,如果token存在,按约定的时间戳(token timestamp)判定token有效期,将token放到请求头的access_token字段中,以判断当前客户端内存放的token是否有效。

[0107] 可选的,使用aes Key进行AES算法对请求数据进行加密,发起交易。交易前通过约定的Token有效性规则,验证Token是否有效(临界值允许发往私有云,公有云基于服务端有效期判断为最终依据)。

[0108] 可选的,云服务的网关接入后首先检查http请求头中是否有access_token存在,如果不存在作为设备初始化操作,如果存在作为普通交易,先检查token是否有效期,如果失效,直接更新token、aes Key及时间戳(tokenTimestamp),并将错误信息返回至客户端,客户端接收到特定错误码后,更新系统本地机密存储中的aes Key,同时更新客户端内存中的token,再次将原交易数据进行发送。

[0109] 可选的,如果Token本地检查有效,原生外壳在点击特定菜单(一级菜单,涉及主界面的菜单和底部的消息,我的等功能)时候,发起交易服务端查询当前菜单是否需要登录及登录有效期。

[0110] 可选的,如果检查需要登陆,但未登录,直接返回前端特定错误码,跳转到登录界面;APP外壳进行ANYOFFICE登录(如果userToken存在,正常情况打开APP的时候已经自动进行了ANYOFFICE登录),UASS登录和通知公有云接入网关登录状态。

[0111] 可选的,通知登录状态中,如果服务端验证到设备deviceid有变更,返回前端进行设备重新绑定操作,服务端更新绑定信息,重新返回Token和AESKey,成功后返回当着已登录返回主界面,失败或报错可主动返回,则到登录界面。设备重新绑定需要手机验证码,原绑定设备信息反显。

[0112] 可选的,API网关的接入普通交易,检查Token有效性,失效则返回特定错误码和新的Token及AESKey;同时判断交易是否需要登录,否则返回特定错误码跳转登录界面。

[0113] 可选的,每次需要登录状态的交易动作,会联动更新user_token的有效期,及只有在连续在特定时间周期内没有做需要登录的交易,才会导致user_token有效期失效,并需要重新登录。

[0114] 本发明实施例的技术方案具体包括:接收客户端发送的访问请求,并且基于预设权限信息对该访问请求进行权限验证,过滤没有权限的访问请求,以实现对客户端的访问请求进行初步过滤,保证了访问的安全性;获取权限验证通过的访问请求中的验证数据以及请求数据,并基于验证数据和请求数据进行报文有效性验证,过滤掉报文无效的访问请求,进一步保证了访问的安全性;对报文有效性验证通过的访问请求进行访问有效性验证,确保当前进行访问请求访问的访问接口的正确性,再次的保证了访问请求的安全性;对访问有效性验证通过的访问请求中的请求报文转换为预设格式,对该预设格式的请求报文进行处理,保证了访问请求的请求内容的规范性;本发明实施例的技术方案通过对访问请求进行逐步验证,以及对通过各项验证的访问请求进行预设格式的处理,实现了提高应用接口的安全性和可靠性。

[0115] 以下是本发明实施例提供的请求处理装置的实施例，该装置与上述各实施例的请求处理方法属于同一个发明构思，在请求处理装置的实施例中未详尽描述的细节内容，可以参考上述请求处理方法的实施例。

[0116] 实施例三

[0117] 图2为本发明实施例三提供的请求处理装置的结构示意图，本实施例可适用于对客户端发送的访问请求能行处理的情况。该请求处理装置的具体结构如下：权限验证模块310、报文有效性验证模块320、访问有效性验证模块330和报文处理模块340；其中，

[0118] 权限验证模块310，用于接收访问请求，基于预设权限信息对所述访问请求进行权限验证。

[0119] 报文有效性验证模块320，用于获取权限验证通过的访问请求中的验证数据以及请求数据，基于所述验证数据和所述请求数据进行报文有效性验证。

[0120] 访问有效性验证模块330，用于对于报文有效性验证通过的访问请求进行访问有效性验证。

[0121] 报文处理模块340，用于对访问有效性验证通过的访问请求中的请求报文转换为预设格式，对所述预设格式的请求报文进行处理。

[0122] 本发明实施例的技术方案具体包括：接收客户端发送的访问请求，并且基于预设权限信息对该访问请求进行权限验证，过滤没有权限的访问请求，以实现对客户端的访问请求进行初步过滤，保证了访问的安全性；获取权限验证通过的访问请求中的验证数据以及请求数据，并基于验证数据和请求数据进行报文有效性验证，过滤掉报文无效的访问请求，进一步保证了访问的安全性；对报文有效性验证通过的访问请求进行访问有效性验证，确保当前进行访问请求访问的访问接口的正确性，再次的保证了访问请求的安全性；对访问有效性验证通过的访问请求中的请求报文转换为预设格式，对该预设格式的请求报文进行处理，保证了访问请求的请求内容的规范性；本发明实施例的技术方案通过对访问请求进行逐步验证，以及对通过各项验证的访问请求进行预设格式的处理，实现了提高应用接口的安全性和可靠性。

[0123] 在上述实施例技术方案的基础上，权限验证模块310，包括：

[0124] 白名单获取单元，用于获取访问权限白名单，确定所述访问请求的url地址是否在所述访问权限白名单中。

[0125] 第一权限验证单元，用于若是，则确实所述访问请求的权限验证为通过。

[0126] 在上述实施例技术方案的基础上，权限验证模块310，还包括：

[0127] token信息提取单元，用于若所述访问请求的url地址不在所述访问权限白名单中，则提取所述访问请求的请求头中的token信息。

[0128] 应用标识验证单元，用于基于所述token信息确定所述访问请求对应的应用标识，确定所述应用标识是否在所述访问权限白名单内。

[0129] 第二权限验证单元，用于若是，则确实所述访问请求的权限验证为通过。

[0130] 在上述实施例技术方案的基础上，所述验证数据包括预设签名，所述请求数据包括请求报文，所述报文有效性验证包括签名验证。

[0131] 相应的，报文有效性验证模块320，包括：

[0132] 解密报文获取单元，用于对所述访问请求的请求头中的请求报文进行解密，得到

解密报文。

[0133] 签名验证单元，用于基于所述解密报文生成验证签名，将所述验证签名与所述预设签名进行比对，若所述验证签名与所述预设签名比对成功，则确定所述请求数据的签名验证成功。

[0134] 在上述实施例技术方案的基础上，签名验证单元，包括：

[0135] 请求头数据获取子单元，用于获取所述访问请求的请求头中设置的随机数、时间戳、应用秘钥、应用标识中的至少一项。

[0136] 验证签名生成子单元，用于基于所述随机数、时间戳、应用秘钥、应用标识中的至少一项以及所述解密报文，根据预设拼接方式形成验证签名。

[0137] 在上述实施例技术方案的基础上，所述验证数据还包括预设加密信息，所述报文有效性验证还包括加密验证。

[0138] 相应的，报文有效性验证模块320，包括：

[0139] 验证加密信息获取单元，用于对所述解密报文进行至少一种预设加密方式的加密处理，得到验证加密信息，将所述验证加密信息与所述预设加密信息进行比对。

[0140] 加密验证单元，用于若所述验证加密信息与所述预设加密信息比对成功，则确定所述请求数据的加密验证成功。

[0141] 在上述实施例技术方案的基础上，所述验证数据还包括有效时间间隔；所述报文有效性验证还包括时间戳验证。

[0142] 相应的，报文有效性验证模块320，包括：

[0143] 时间戳验证单元，用于确定所述访问请求中的时间戳以及当前时间戳是否满足有效时间间隔，若是，则确定所述访问请求时间戳验证通过。

[0144] 在上述实施例技术方案的基础上，所述访问有效性验证包括失效日期验证；

[0145] 相应的，访问有效性验证模块330，包括：

[0146] 失效期获取单元，用于获取所述请求头中token信息的失效期，基于当前时间戳和所述失效期确定所述token信息是否失效。

[0147] 第一失效期判断单元，用于失效期获取单元，用于若是，则向发送所述访问请求的客户端发送错误信息，以使所述客户端重新获取token信息。

[0148] 第二失效期判断单元，用于若否，则确定所述访问请求的失效日期验证通过。

[0149] 在上述实施例技术方案的基础上，所述访问有效性验证还包括访问接口验证。

[0150] 相应的，访问有效性验证模块330，包括：

[0151] 可访问接口获取单元，用于基于所述访问请求中的应用标识，确定所述应用标识对应的可访问接口。

[0152] 访问接口验证单元，用于确定所述访问请求当前的访问接口是否为所述应用标识对应的可访问接口，若是，则确定所述访问请求的访问接口验证通过。

[0153] 在上述实施例技术方案的基础上，该装置还包括：

[0154] 限流单元，用于在接收访问请求之后，监测当前请求流量，若所述当前请求流量满足限流条件，则调用预设的限流规则，对接收的各访问请求进行限流。

[0155] 在上述实施例技术方案的基础上，该装置还包括：

[0156] 黑名单验证单元，用于在接收访问请求之后，基于所述访问请求的IP地址和预先

设置的IP地址黑名单进行验证。

[0157] 访问请求判断单元，用于若所述访问请求的IP地址在所述IP地址黑名单内，则拒绝所述访问请求。

[0158] 在上述实施例技术方案的基础上，该装置还包括：

[0159] 数据过滤单元，用于获取访问日志，基于所述预先设置的IP地址黑名单对所述访问日志进行数据过滤。

[0160] IP地址黑名单添加单元，用于统计过滤后的访问日志中，各IP地址的访问频率，将满足恶意访问频率的IP地址添加至所述预先设置的IP地址黑名单中。

[0161] 在上述实施例技术方案的基础上，该装置还包括：

[0162] 调用对象确定单元，用于在基于所述预先设置的IP地址黑名单对所述访问日志进行数据过滤之后，确定过滤后的访问日志中各访问请求的调用对象。

[0163] IP地址黑名单添加单元，用于若所述调用对象为预先设置的非法调用对象，则将所述访问请求的IP地址添加至所述预先设置的IP地址黑名单中。

[0164] 本发明实施例所提供的请求处理装置可执行本发明任意实施例所提供的请求处理方法，具备执行方法相应的功能模块和有益效果。

[0165] 值得注意的是，上述请求处理装置的实施例中，所包括的各个单元和模块只是按照功能逻辑进行划分的，但并不局限于上述的划分，只要能够实现相应的功能即可；另外，各功能单元的具体名称也只是为了便于相互区分，并不用于限制本发明的保护范围。

[0166] 实施例四

[0167] 图3为本发明实施例四提供的一种电子设备的结构示意图。图3示出了适于用来实现本发明实施方式的示例性电子设备12的框图。图3显示的电子设备12仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0168] 如图3所示，电子设备12以通用计算电子设备的形式表现。电子设备12的组件可以包括但不限于：一个或者多个处理器或者处理单元16，系统存储器28，连接不同系统组件(包括系统存储器28和处理单元16)的总线18。

[0169] 总线18表示几类总线结构中的一种或多种，包括存储器总线或者存储器控制器，外围总线，图形加速端口，处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说，这些体系结构包括但不限于工业标准体系结构(ISA)总线，微通道体系结构(MAC)总线，增强型ISA总线、视频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0170] 电子设备12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被电子设备12访问的可用介质，包括易失性和非易失性介质，可移动的和不可移动的介质。

[0171] 系统存储器28可以包括易失性存储器形式的计算机系统可读介质，例如随机存取存储器(RAM)30和/或高速缓存存储器32。电子设备12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例，存储系统34可以用于读写不可移动的、非易失性磁介质(图3未显示，通常称为“硬盘驱动器”)。尽管图3中未示出，可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器，以及对可移动非易失性光盘(例如CD-ROM，DVD-ROM或者其它光介质)读写的光盘驱动器。在这些情况下，每个驱动器可以通过一个或者多个数据介质接口与总线18相连。系统存储器28可以包括至少一个程序产品，该程序产品具有一组(例如至少一个)程序模块，这些程序模块被配置以执行本发明

各实施例的功能。

[0172] 具有一组(至少一个)程序模块42的程序/实用工具40,可以存储在例如系统存储器28中,这样的程序模块42包括但不限于操作系统、一个或者多个应用程序、其它程序模块以及程序数据,这些示例中的每一个或某种组合中可能包括网络环境的实现。程序模块42通常执行本发明所描述的实施例中的功能和/或方法。

[0173] 电子设备12也可以与一个或多个外部设备14(例如键盘、指向设备、显示器24等)通信,还可与一个或者多个使得用户能与该电子设备12交互的设备通信,和/或与使得该电子设备12能与一个或多个其它计算设备进行通信的任何设备(例如网卡,调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口22进行。并且,电子设备12还可以通过网络适配器20与一个或者多个网络(例如局域网(LAN),广域网(WAN)和/或公共网络,例如因特网)通信。如图3所示,网络适配器20通过总线18与电子设备12的其它模块通信。应当明白,尽管图3中未示出,可以结合电子设备12使用其它硬件和/或软件模块,包括但不限于:微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0174] 处理单元16通过运行存储在系统存储器28中的程序,从而执行各种功能应用以及样本数据获取,例如实现本发实施例所提供的一种请求处理方法步骤,请求处理方法包括:

[0175] 接收访问请求,基于预设权限信息对所述访问请求进行权限验证;

[0176] 获取权限验证通过的访问请求中的验证数据以及请求数据,基于所述验证数据和所述请求数据进行报文有效性验证;

[0177] 对于报文有效性验证通过的访问请求进行访问有效性验证;

[0178] 对访问有效性验证通过的访问请求中的请求报文转换为预设格式,对所述预设格式的请求报文进行处理。

[0179] 当然,本领域技术人员可以理解,处理器还可以实现本发明任意实施例所提供的样本数据获取方法的技术方案。

[0180] 实施例五

[0181] 本实施例五提供了一种计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现例如实现本发实施例所提供的一种请求处理方法步骤,请求处理方法包括:

[0182] 接收访问请求,基于预设权限信息对所述访问请求进行权限验证;

[0183] 获取权限验证通过的访问请求中的验证数据以及请求数据,基于所述验证数据和所述请求数据进行报文有效性验证;

[0184] 对于报文有效性验证通过的访问请求进行访问有效性验证;

[0185] 对访问有效性验证通过的访问请求中的请求报文转换为预设格式,对所述预设格式的请求报文进行处理。

[0186] 本发明实施例的计算机存储介质,可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是但不限于:电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、

可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0187] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0188] 计算机可读介质上包含的程序代码可以用任何适当的介质传输,包括但不限于:无线、电线、光缆、RF等等,或者上述的任意合适的组合。

[0189] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计算机程序代码,所述程序设计语言包括面向对象的程序设计语言,诸如Java、Smalltalk、C++,还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络,包括局域网(LAN)或广域网(WAN),连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0190] 本领域普通技术人员应该明白,上述的本发明的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个计算装置上,或者分布在多个计算装置所组成的网络上,可选地,他们可以用计算机装置可执行的程序代码来实现,从而可以将它们存储在存储装置中由计算装置来执行,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样,本发明不限制于任何特定的硬件和软件的结合。

[0191] 注意,上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解,本发明不限于这里所述的特定实施例,对本领域技术人员来说能够进行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此,虽然通过以上实施例对本发明进行了较为详细的说明,但是本发明不仅仅限于以上实施例,在不脱离本发明构思的情况下,还可以包括更多其他等效实施例,而本发明的范围由所附的权利要求范围决定。

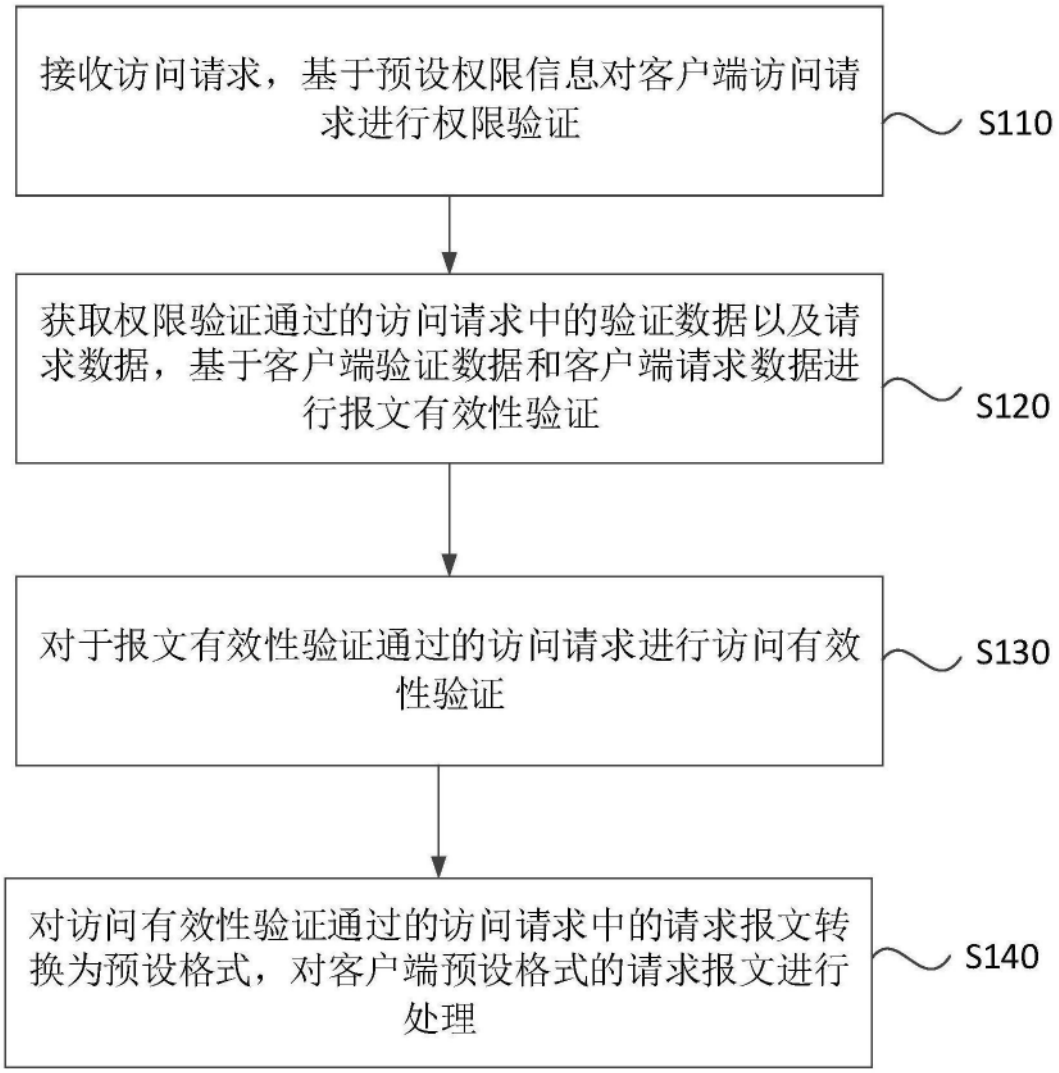

接收访问请求，基于预设权限信息对客户端访问请求进行权限验证
S110
获取权限验证通过的访问请求中的验证数据以及请求数据，基于客户端验证数据和客户端请求数据进行报文有效性验证
S120
对于报文有效性验证通过的访问请求进行访问有效性验证
S130
对访问有效性验证通过的访问请求中的请求报文转换为预设格式，对客户端预设格式的请求报文进行处理
S140

图1

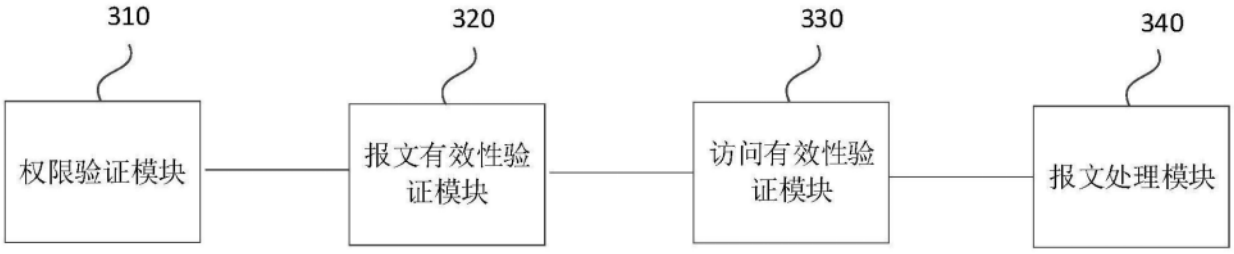

310
权限验证模块
320
报文有效性验证模块
330
访问有效性验证模块
340
报文处理模块

图2

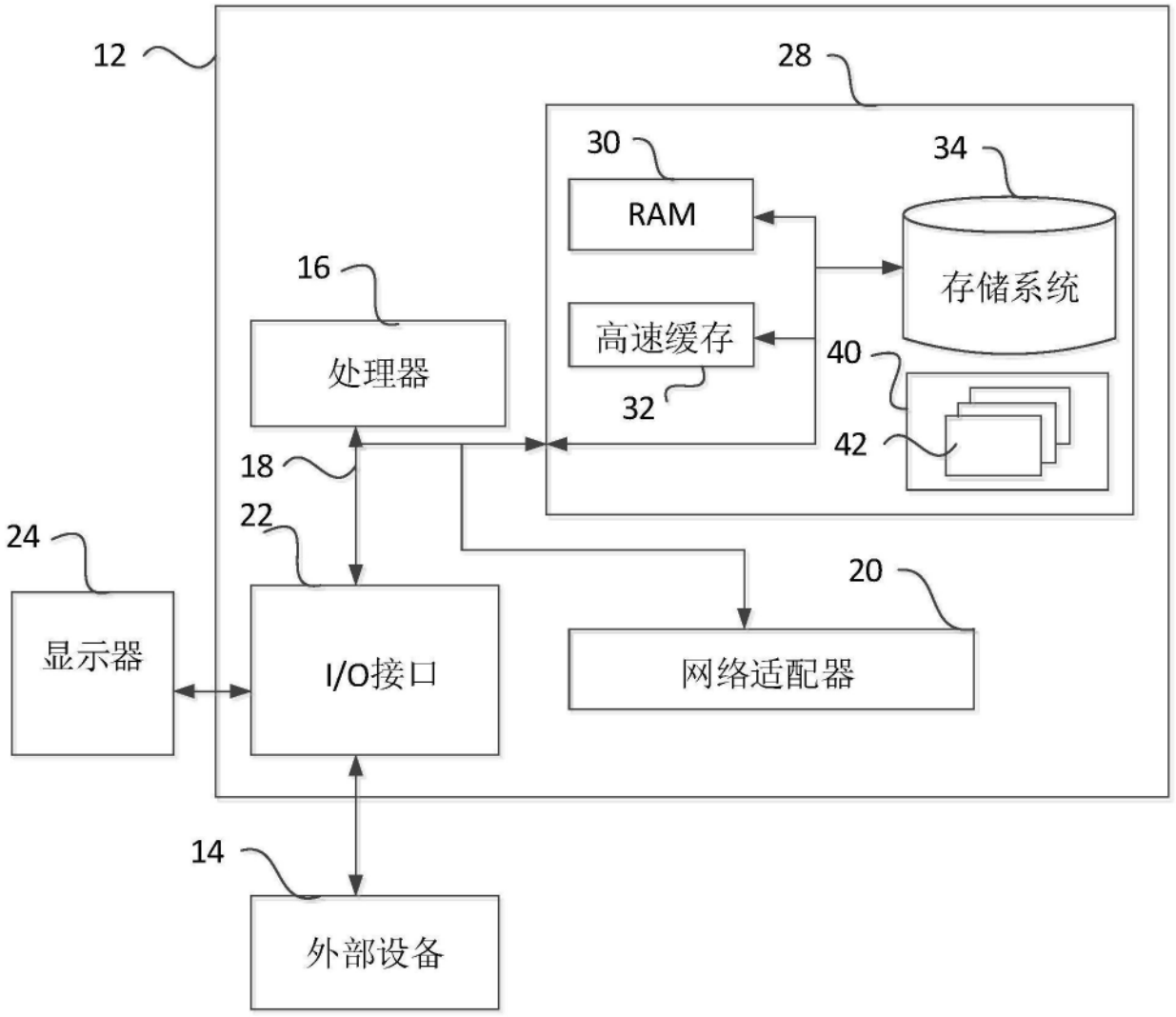

12
28
30
RAM
34
存储系统
16
处理器
高速缓存
32
40
42
18
22
24
显示器
I/O接口
20
网络适配器
14
外部设备

图3