

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 11 月 26 日 (26.11.2020)



(10) 国际公布号
WO 2020/233012 A1

(51) 国际专利分类号:
G06F 9/54 (2006.01)

(21) 国际申请号: PCT/CN2019/117893

(22) 国际申请日: 2019 年 11 月 13 日 (13.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910418187.X 2019年5月20日 (20.05.2019) CN

(71) 申请人: 平安科技(深圳)有限公司(PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN];
中国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, Guangdong 518033 (CN)。

(72) 发明人: 郭巧佳(GUO, Qiaojia); 中国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, Guangdong 518033 (CN)。

(74) 代理人: 北京鸿元知识产权代理有限公司 (GRANDER IP LAW FIRM); 中国北京市朝阳区光华路 7 号汉威大厦东区 18A6 室, Beijing 100004 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: DISTRIBUTED SMART API ASYNCHRONOUS CALLBACK METHOD, DEVICE, CLIENT TERMINAL, SERVICE TERMINAL, AND STORAGE MEDIUM

(54) 发明名称: 分布式的智能API异步回调方法、装置、客户端、服务端及存储介质

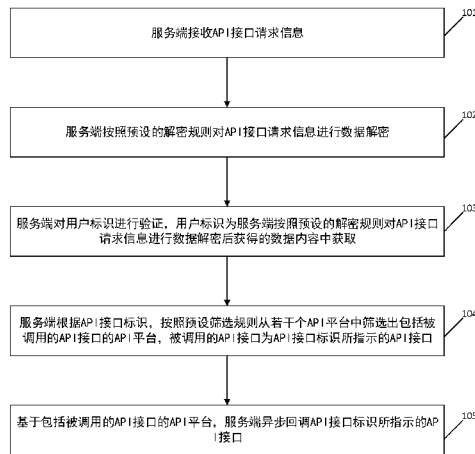


图 1

101 A service terminal receives API interface request information
102 The service terminal performs data decryption on the API interface request information according to a pre-determined decryption rule
103 The service terminal verifies a user identifier, the user identifier being acquired from data contents obtained after the service terminal has performed data decryption on the API interface request information according to the pre-determined decryption rule
104 The service terminal selects, from multiple API platforms, an API platform comprising a called API interface according to the API interface identifier and a pre-determined selection rule, the called API interface being an API interface indicated by the API interface identifier
105 The service terminal performs, on the basis of the API platform comprising the called API interface, asynchronous callback for the API interface indicated by the API interface identifier

(57) Abstract: The present application relates to the field of monitoring, and discloses a distributed smart API asynchronous callback method. The method comprises: a service terminal receiving API interface request information; performing data decryption on the API interface request information according to a pre-determined decryption rule, the decrypted API interface request information comprising an API interface identifier, a user identifier, and a data packet format; verifying the user identifier; selecting, from multiple API platforms, an API platform comprising a called API interface according to the API interface identifier and a pre-determined selection rule, the called API interface being an API interface indicated by the API interface identifier; and performing, on the basis of the API platform comprising the called API interface, asynchronous callback for the API interface indicated by the API interface identifier. The present application discloses a device, a client terminal, a service terminal, and a storage medium. The present application achieves high data security and function building flexibility.

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国(除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本申请涉及监控领域, 公开了一种分布式的智能API异步回调方法, 包括: 服务端接收API接口请求信息; 按照预设的解密规则对所述API接口请求信息进行数据解密, 解密后的API接口请求信息包括API接口标识、用户标识、数据报文格式; 对所述用户标识进行验证; 根据所述API接口标识, 按照预设筛选规则从若干个API平台中筛选出包括被调用的API接口的API平台, 被调用的API接口为API接口标识所指示的API接口; 基于所述包括被调用的API接口的API平台, 异步回调所述API接口标识所指示的API接口。本申请公开了一种装置、客户端、服务端和存储介质。本申请具有较高的数据安全性、功能搭建灵活性。

分布式的智能 API 异步回调方法、装置、客户端、服务端及存储介质

本申请要求申请号为 201910418187.X，申请日为 2019 年 5 月 20 日，
5 发明创造名称为“分布式的智能 API 异步回调方法及装置”的专利申请的
优先权。

技术领域

10 本申请涉及监控领域，尤其是一种通过软件进行业务节点监控技术，
具体公开了一种分布式的智能 API 异步回调方法、装置、客户端、服务端
和存储介质。

背景技术

15 面对急速变化的市场环境，通常企业会通过改变业务流程以适应这种
市场环境，由于企业的业务流程管理依赖管理系统来实现，进而企业经常
对管理系统的功能进行重新搭建，但是，在重新搭建管理系统的功能的过
程中，我们发现，在现有技术中，重新搭建管理系统功能的方式通常是重
写一个功能模块，且重写后的功能模块与管理系统中原有的其他模块依赖
20 度高，解耦度不高，进而导致管理系统的功能搭建不够灵活、搭建周期长、
搭建成本高。

申请内容

为了解决上述问题，本申请公开了一种智能 API 异步回调方法、装置、
客户端、服务端和存储介质。

25 本申请第一方面，提供一种分布式的智能 API 异步回调方法，该方法
包括：

服务端接收 API 接口请求信息；

按照预设的解密规则对所述 API 接口请求信息进行数据解密，解密后
的 API 接口请求信息包括 API 接口标识、用户标识、数据报文格式；

30 对所述用户标识进行验证；

根据所述 API 接口标识，按照预设筛选规则从多个 API 平台中筛选出
包括被调用的 API 接口的 API 平台，被调用的 API 接口为 API 接口标识所
指示的 API 接口；

35 基于所述包括被调用的 API 接口的 API 平台，异步回调所述 API 接口
标识所指示的 API 接口。

本申请第二方面，提供一种分布式的智能 API 异步回调装置，包括：
第一接收模块，接收 API 接口请求信息；

解密模块，按照预设的解密规则对所述 API 接口请求信息进行数据解

密，解密后的 API 接口请求信息包括 API 接口标识、用户标识和数据报文格式；

验证模块，对所述用户标识进行验证；

筛选模块，根据所述 API 接口标识，按照预设筛选规则从多个 API 平台中筛选出包括被调用的 API 接口的 API 平台，被调用的 API 接口为 API 接口标识所指示的 API 接口；

接口调用模块，基于所述包括被调用的 API 接口的 API 平台，异步回调所述 API 接口标识所指示的 API 接口。

本申请的第三方面，提供一种一种客户端，包括：

封装模块，用于封装 API 接口请求信息，接口请求信息中包含用户标识，和 API 接口标识，和 API 接口标识，和/或数据报文格式；

请求信息加密模块，用于按照预设加密规则对封装后的 API 接口请求信息进行加密；

发送模块，用于通过 POST 方式发送加密后的 API 接口请求信息；

第二接收模块，用于接收认证公钥；

监听模块，用于设置回调监听发送结果。

本申请第四方面，提供一种服务端，包括：

至少 1 个存储单元；

与所述至少 1 个存储单元耦合的处理单元；

其中，所述至少 1 个存储单元用于存储计算机指令；

所述处理单元用于调用所述计算机指令，以执行本申请第一方面公开的分布式的智能 API 异步回调方法。

本申请第五方面，提供一种计算机非易失性存储介质，所述计算机非易失性存储介质存储有计算机指令，所述计算机指令被调用时，用于执行本申请第一方面公开的分布式的智能 API 异步回调方法。

可见，本申请能够异步回调分布式设置的 API 接口，以调用分布式设置的 API 接口所提供的功能，进而实现快速功能模块的快速搭建，同时本申请能够对请求数据及 API 接口返回的数据进行加密，进而实现数据传输安全性较高。

附图说明

图 1 是本申请实施例一公开的一种分布式的智能 API 异步回调方法的流程示意图；

图 2 是本申请实施例二公开的一种分布式的智能 API 异步回调方法的流程示意图；

图 3 是本申请实施例三公开的一种分布式的智能 API 异步回调装置的结构示意图；

图 4 是本申请实施例四公开的一种分布式的智能 API 异步回调装置的结构示意图。

图 5 是本申请公开的一种分布式的智能 API 异步回调装置的结构示意图。

具体实施方式

本申请的说明书和权利要求书及上述附图中的术语“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、装置、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他步骤或单元。

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出现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。

面对急速变化的市场环境，通常企业会通过改变业务流程以适应这种市场环境，由于企业的业务流程管理依赖管理系统来实现，进而企业经常对管理系统的功能进行重新搭建，但是，在重新搭建管理系统的功能的过程中，我们发现，在现有技术中，重新搭建管理系统功能的方式通常是重写一个功能模块，且重写后的功能模块与管理系统中原有的其他模块依赖度高，解耦度不高，进而导致管理系统的功能搭建不够灵活、搭建周期长、搭建成本高。针对这种场景，本申请公开了一种分布式的智能 API 异步回调方法及装置。

下面结合本申请的具体实施例对本申请的一种分布式的智能 API 异步回调方法及装置进行详细说明。

实施例一

请参阅图 1，图 1 是本申请实施例一公开的一种分布式的智能 API 异步回调方法的流程示意图，该方法在服务端执行。如图 1 所示，本申请实施例一的一种分布式的智能 API 异步回调方法包括：

101、服务端接收 API 接口请求信息。

作为一种可选的实施方式，在本申请实施例中，服务端在收到请求端发出的 API 接口请求信息之前，本申请实施例的分布式的智能 API 异步回调方法还包括：

服务端接收公钥请求，生成认证公钥和认证密钥；

服务端发送认证公钥。

102、服务端按照预设的解密规则对 API 接口请求信息进行数据解密。

服务端接收到 API 接口请求信息后，对 API 接口请求信息进行数据解密，以解析出包含用户标识，及 API 接口标识，及请求数据内容，及数据

报文格式。

作为一种可选的实施方式，在本申请实施例中，服务端使用认证密钥对 API 接口请求信息进行验证。

在本申请实施例中，可选的，服务端将 API 接口请求信息中的数据报文格式与服务端默认设定的数据报文格式进行比对，若 API 接口请求信息中的数据报文格式与服务端默认设定的数据报文格式不一致，则服务端按照服务端默认设定的数据报文格式对 API 接口请求信息进行格式转换。

示例性地，若 API 接口请求信息的数据报文格式为 XML 格式，服务端默认设定的数据报文格式为 JSON 数据格式，经服务端比对，两者不一致，则服务端对 API 接口请求信息进行结点解读，解读方式主要为通过深度优先遍历的方式遍历 API 接口请求信息的数据报文中所有的节点。在此，结点下包含多个数值，本申请实例定义为根节点，否则定义为子节点。

在本申请实施例中，遍历 API 接口请求信息的数据报文中所有的节点的过程为：

以根-节点-节点、或者根-节点-根-节点再到下一个根-节点-节点的方式遍历所有的节点，直到最后一个节点，结束遍历过程。

在本申请实施例中，遍历 API 接口请求信息的数据报文所有的节点的同时，进行 API 接口请求信息的数据转换，以将 API 接口请求信息以名为一个 JSON 数据表示。例如，假设一个 API 接口请求信息的数据报文为：

```
<login>
  <userId>test</userId>
  <password>test123</password>
</login>
<content>
  <data>
    <extdata>welcome test</extdata>
  </data>
</content>
```

对 API 接口请求信息的数据进行数据转换后，生成两个 JSON 数据，即 login 和 content，其中 content 中存在嵌套，如下所示：

```
login {userId: test;password: test123} ;
content {data: {extdata: 1;welcome: test} } 。
```

103、服务端对用户标识进行验证，用户标识为服务端按照预设的解密规则对 API 接口请求信息进行数据解密后获得的数据内容中获取。

在本申请实施例中，可选的，用户标识包括用户身份标识及用户权限标识。

相对应地，服务端对用户标识进行验证可以包括：

服务端对用户身份标识进行验证；

服务端对用户权限标识进行验证。

在本申请实施例中，进一步可选的，服务端对用户身份标识进行验证可以包括：

将用户身份标识与用户身份数据库进行比对，若用户身份数据库包含用户身份标识，则服务端返回用户身份验证成功信息，若用户身份数据库不包含用户身份标识，则服务端返回用户身份验证失败信息，使得当用户终端接收到用户身份验证失败信息重新提交 API 接口请求信息。

在本申请实施例中，进一步可选的，服务端对用户权限标识进行验证可以包括：

将用户权限标识与用户权限数据库进行比对，若用户权限数据库包含用户权限标识，则服务端返回用户权限验证成功信息，若用户权限数据库不包含用户权限标识，则服务端返回用户权限验证失败信息。

在本申请实施例中，进一步可选的，用户身份数据库及用户权限数据库可以是 mysql, orcal, sqlserver 等关系型数据库中的任意一种，由于 mysql 为轻量级数据库，且具备更便利的移植性，从而便于扩展和维护，本申请实施例选择 mysql 作为用户身份数据库。

104、服务端根据 API 接口标识，按照预设筛选规则从若干个 API 平台中筛选出包括被调用的 API 接口的 API 平台，被调用的 API 接口为 API 接口标识所指示的 API 接口。

在本申请实施例中，可选的，服务端根据 API 接口标识，按照预设筛选规则从若干个 API 平台中筛选出包括被调用的 API 接口的 API 平台包括：

服务端根据 API 接口标识，从若干个 API 平台中筛选出当前访问量最小的 API 平台。

105、基于包括被调用的 API 接口的 API 平台，服务端异步回调 API 接口标识所指示的 API 接口。

在本申请实施例中，可选的，按照预设的数据格式返回请求结果。例如，按照 JSON 格式返回请求结果。

在本申请实施例中，可选的，按照预设的数据格式返回请求结果中的预设的数据格式可以下步骤确定：

在本申请实施例中，可选的，API 接口请求信息还包括业务任务数据，以及，基于包括被调用的 API 接口的 API 平台，服务端异步回调 API 接口标识所指示的 API 接口之后，方法还包括：

发送回调结果，回调结果为 API 接口标识所指示的 API 接口根据业务任务数据生成。

在本申请实施例中，可选的，服务端发送回调结果之前，方法还包括：服务端按照 API 接口请求信息中的数据报文格式对回调结果进行数据格式转换；

服务端按照回调结果加密规则对回调结果进行加密。

在本申请实施例中，可选的，回调结果加密规则可以是 RSA 加密算法，因 RSA 加密算法破解困难，其保密性是得到业界公认的，虽然其安全性尚

未有明确的论证，但实际运用中，尚未有破解 RSA 加密算法的示例发生，故其具有较高的数据安全性。

在本申请实施例中，可选的，回调结果加密规则可以是 Base64 加密算法

需要说明的是，请求结果可以根据调用方的具体业务需求确定，本申请对请求结果的具体内容不作限定。

可见，本申请实施例能够根据功能相似性，将不同平台中具有相同功能的功能模块进行整合，进而生成一个对外开放的通用接口，进而当调用请求方需要调用部署在不同平台上的功能模块时，调用请求方只需调用该通用接口，并提供相关的字段标识，即可完成多平台之间的 API 接口调用，另一方面，本申请实施例能够根据回调请求中的数据格式，返回数据格式与回调请求中的数据格式一致的回掉结果，即本申请实施例具有灵活的报文转换功能。再一方面，本申请实施例能够对数据进行加密，使得数据的传输具有较高的安全性。

实施例二

请参阅图 2，图 2 是本申请实施例二公开的一种分布式的智能 API 异步回调方法的流程示意图，该方法在客户端执行。如图 2 所示，本申请实施例二的一种分布式的智能 API 异步回调方法包括：

201、客户端封装 API 接口请求信息，接口请求信息中包含用户标识，和 API 接口标识，和数据报文格式。

202、客户端按照预设加密规则对封装后的 API 接口请求信息进行加密。

在本申请实施例中，可选的，预设加密规则可以是 RSA 加密算法，因 RSA 加密算法破解困难，其保密性是得到业界公认的，虽然其安全性尚未有明确的论证，但实际运用中，尚未有破解 RSA 加密算法的示例发生，故其具有较高的数据安全性。

在本申请实施例中，可选的，预设加密规则可以是 Base64 加密算法。

作为一种可选的实施方式，在本申请实施例中，客户端按照预设加密规则对封装后的 API 接口请求信息进行加密之前，本申请实施例二的一种分布式的智能 API 异步回调方法还包括：

客户端发送公钥请求并接收认证公钥。

203、客户端通过 POST 方式发送加密后的 API 接口请求信息。

客户端在发起请求时，需要封装承载在请求协议上的 API 接口请求信息，该 API 接口请求信息包含用户标识、API 接口标识、API 接口标识、数据报文格式，其中，可选的，数据报文格式为可选的，如不填写，则数据报文格式默认为 JSON 格式。进一步可选，在本申请实施例中，数据报文格式为 JSON 格式。

需要说明的是，客户端不局限于 APP、网页、桌面运用等，只要支持 http 传输协议的任何平台都可以，本申请实施例对此不作限定。

需要说明的是,关于 POST 请求方式和 GET 请求方式请参考现有技术中的描述,本申请实施例对此不在赘述。

在本申请实施例中,可选的,客户端通过 POST 方式发送加密后的 API 接口请求信息之后,一种分布式的智能 API 异步回调方法还包括:

5 设置回调监听发送结果。

在本申请实施例中,可选的,客户端通过 GET 方式发送加密后的 API 接口请求信息。

204、客户端接收回调结果。

在本申请实施例中,可选的,客户端接收回调结果之后,客户端对回调结果进行解密。

在本申请实施例中,可选的,采用 RSA 算法对回调结果进行解密。

可见,本申请实施例,通过访问通用接口,即可调用部署在不同平台上的 API 接口,且本申请实施例能够对回调请求中的数据进行加密,故本申请实施例具有较高的灵活性、数据安全性。

实施例三

请参阅图 3,图 3 是本申请实施例三公开的一种分布式的智能 API 异步回调装置的结构示意图,其中,该智能 API 异步回调装置可用于执行本申请实施一公开的一种分布式的智能 API 异步回调方法。如图 3 所示,该智能 API 异步回调装置包括:

第一接收模块 301,用于接收 API 接口请求信息。

解密模块 302,用于按照预设的解密规则对 API 接口请求信息进行数据解密,解密后的 API 接口请求信息包括 API 接口标识、用户标识、数据报文格式。

25 该智能 API 异步回调装置还包括:

验证模块 303,用于对用户标识进行验证。

作为一个可选的实施方式,在本申请实施例中,用户标识包括用户身份标识及用户权限标识;以及,验证模块 303 对用户标识进行验证具体为:

对用户身份标识进行验证;

30 对用户权限标识进行验证。

在本申请实施例中,可选的,验证模块 303 对用户身份标识进行验证更具体为:

将用户身份标识与用户身份数据库进行比对,若用户身份数据库包含用户身份标识,则返回用户身份验证成功信息,若用户身份数据库不包含用户身份标识,则返回用户身份验证失败信息。

在本申请实施例中,可选的,验证模块 303 对对用户权限标识进行验证更具体为:

将用户权限标识与用户权限数据库进行比对,若用户权限数据库包含用户权限标识,则返回用户权限验证成功信息,若用户权限数据库不包含

用户权限标识，则返回用户权限验证失败信息。

在本申请实施例中，进一步可选的，用户身份数据库及用户权限数据库可以是 mysql, orcal, sqlserver 等关系型数据库中的任意一种，由于 mysql 为轻量级数据库，且具备更便利的移植性，从而便于扩展和维护，
5 本申请实施例选择 mysql 作为用户身份数据库。

作为一个可选的实施方式，在本申请实施例中，验证模块 303 还用于使用认证密钥对 API 接口请求信息进行验证。

在第一接收模块 301 接收到 API 接口请求信息之后，验证模块 303 对 API 接口请求信息进行数据解密，以解析出包含用户标识，及 API 接口标识，及请求数据内容，及数据报文格式。
10

该智能 API 异步回调装置还包括：

筛选模块 304，用于根据 API 接口标识，按照预设筛选规则从若干个 API 平台中筛选出包括被调用的 API 接口的 API 平台，被调用的 API 接口为 API 接口标识所指示的 API 接口。

15 该智能 API 异步回调装置还包括：

接口调用模块 305，用于基于包括被调用的 API 接口的 API 平台，异步回调 API 接口标识所指示的 API 接口。

作为一个可选的实施方式，在本申请实施例中，第一接收模块还用于接收公钥请求，进一步的，装置还包括公钥密钥生成模块 306 和发送模块 307，其中，
20

公钥密钥生成模块 306，用于根据公钥请求生成认证公钥和认证密钥；发送模块 307，用于发送认证公钥。

作为一个可选的实施方式，在本申请实施例中，装置还包括转换模块 308，转换模块 308 用于将 API 接口请求信息中的数据报文格式与默认设定的数据报文格式进行比对，若 API 接口请求信息中的数据报文格式与默认设定的数据报文格式不一致，则按照默认设定的数据报文格式对 API 接口请求信息进行格式转换。
25

示例性地，若 API 接口请求信息的数据报文格式为 XML 格式，服务端默认设定的数据报文格式为 JSON 数据格式，经转换模块 308 比对，两者不一致，则服务端对 API 接口请求信息进行结点解读，解读方式主要为通过深度优先遍历的方式遍历 API 接口请求信息的数据报文中所有的节点。在此，结点下包含多个数值，本申请实例定义为根节点，否则定义为子节点。
30

在本申请实施例中，遍历 API 接口请求信息的数据报文中所有的节点的过程为：

35 以根-节点-节点、或者根-节点-根-节点再到下一个根-节点-节点的方式遍历所有的节点，直到最后一个节点，结束遍历过程。

在本申请实施例中，遍历 API 接口请求信息的数据报文所有的节点的同时，进行 API 接口请求信息的数据转换，以将 API 接口请求信息以名为一个 JSON 数据表示。例如，假设一个 API 接口请求信息的数据报文为：

```

<login>
  <userId>test</userId>
  <password>test123</password>
</login>
5 <content>
  <data>
    <extdata>welcome test</extdata>
  </data>
</content>

```

10 对 API 接口请求信息的数据进行数据转换后,生成两个 JSON 数据,即 login 和 content,其中 content 中存在嵌套,如下所示:

```

login {userId: test;password: test123} ;
content {data: {extdata: 1;welcome: test} } 。

```

15 作为一个可选的实施方式,在本申请实施例中,筛选模块 304 具体用于:根据 API 接口标识,从若干个 API 平台中筛选出当前访问量最小的 API 平台。

作为一个可选的实施方式,在本申请实施例中,API 接口请求信息还包括业务任务数据;以及,发送模块 307 还用于发送回调结果,回调结果为 API 接口标识所指示的 API 接口根据业务任务数据生成。

20 作为一个可选的实施方式,在本申请实施例中,转换模块 308 还用于按照 API 接口请求信息中的数据报文格式对回调结果进行数据格式转换;以及,装置还包括加密模块 309,加密模块 309 用于:

按照回调结果加密规则对回调结果进行加密。

25 在本申请实施例中,可选的,回调结果加密规则可以是 RSA 加密算法,因 RSA 加密算法破解困难,其保密性是得到业界公认的,虽然其安全性尚未有明确的论证,但实际运用中,尚未有破解 RSA 加密算法的示例发生,故其具有较高的数据安全性。

在本申请实施例中,可选的,回调结果加密规则可以是 Base64 加密算法

30 需要说明的是,请求结果可以根据调用方的具体业务需求确定,本申请对请求结果的具体内容不作限定。

35 可见,本申请实施例能够根据功能相似性,将不同平台中具有相同功能的功能模块进行整合,进而生成一个对外开放的通用接口,进而当调用请求方需要调用部署在不同平台上的功能模块时,调用请求方只需调用该通用接口,并提供相关的字段标识,即可完成多平台之间的 API 接口调用,另一方面,本申请实施例能够根据回调请求中的数据格式,返回数据格式与回调请求中的数据格式一致的回掉结果,即本申请实施例具有灵活的报文转换功能。再一方面,本申请实施例能够对数据进行加密,使得数据的传输具有较高的安全性。

实施例四

请参阅图 4，图 4 是本申请实施例四公开的客户端的结构示意图，其中，该客户端可以用于执行本申请实施例二公开的一种分布式的智能 API 异步回调方法。如图 4 所示，该客户端包括：

封装模块 401，用于封装 API 接口请求信息，接口请求信息中包含用户标识，和 API 接口标识，和 API 接口标识，和/或数据报文格式。

客户端在发起请求时，需要封装承载在请求协议上的 API 接口请求信息，该 API 接口请求信息包含用户标识、API 接口标识、API 接口标识、数据报文格式，其中，可选的，数据报文格式为可选的，如不填写，则数据报文格式默认为 JSON 格式。进一步可选，在本申请实施例中，数据报文格式为 JSON 格式。

需要说明的是，客户端不局限于 APP、网页、桌面运用等，只要支持 http 传输协议的任何平台都可以，本申请实施例对此不作限定。

需要说明的是，关于 POST 请求方式和 GET 请求方式请参考现有技术中的描述，本申请实施例对此不在赘述

该客户端还包括：

请求信息加密模块 402，用于按照预设加密规则对封装后的 API 接口请求信息进行加密。

在本申请实施例中，可选的，预设加密规则可以是 RSA 加密算法，因 RSA 加密算法破解困难，其保密性是得到业界公认的，虽然其安全性尚未有明确的论证，但实际运用中，尚未有破解 RSA 加密算法的示例发生，故其具有较高的数据安全性。

在本申请实施例中，可选的，预设加密规则可以是 Base64 加密算法。

作为一种可选的实施方式，在本申请实施例中，客户端还包括：

发送模块 403，用于通过 POST 方式发送加密后的 API 接口请求信息。

作为一种可选的实施方式，在本申请实施例中，发送模块 403 还用于发送公钥请求；以及，客户端还包括第二接收模块 404，第二接收模块 404 用于接收认证公钥。

在本申请实施例中，可选的，客户端还包括：

监听模块 405，用于设置回调监听发送结果。

在本申请实施例中，可选的，第二接收模块 404 还用于接收回调结果。

在本申请实施例中，可选的，客户端还包括：

回调结果解密模块 406，用于对回调结果进行解密。

在本申请实施例中，可选的，客户端通过 GET 方式发送加密后的 API 接口请求信息。

在本申请实施例中，可选的，采用 RSA 算法对回调结果进行解密。

可见，本申请实施例，通过访问通用接口，即可调用部署在不同平台上的 API 接口，且本申请实施例能够对回调请求中的数据进行加密，故本

申请实施例具有较高的灵活性、数据安全性。

实施例五

请参阅图 5，图 5 是本申请实施例五公开的一种服务端。如图 5 所示，
5 服务端 50 包括：

至少 1 个存储单元 501；

与至少 1 个存储单元耦合的处理单元 502；

其中，至少 1 个存储单元用于存储计算机指令；

10 处理单元用于调用计算机指令，以执行本申请第一方面公开的分布式的智能 API 异步回调方法。

本申请实施例能够根据功能相似性，将不同平台中具有相同功能的功能模块进行整合，进而生成一个对外开放的通用接口，进而当调用请求方需要调用部署在不同平台上的功能模块时，调用请求方只需调用该通用接口，并提供相关的字段标识，即可完成多平台之间的 API 接口调用，另一方面，本申请实施例能够根据回调请求中的数据格式，返回数据格式与回调请求中的数据格式一致的回掉结果，即本申请实施例具有灵活的报文转换功能。再一方面，本申请实施例能够对数据进行加密，使得数据的传输具有较高的安全性。

实施例六

20 本申请实施例六公开了一种计算机可读存储介质，其存储用于电子数据交换的计算机程序，其中，该计算机程序使得计算机执行实施例一、实施例二中任意一个实施例所描述的分布式的智能 API 异步回调方法中的步骤。

25 本申请实施例能够根据功能相似性，将不同平台中具有相同功能的功能模块进行整合，进而生成一个对外开放的通用接口，进而当调用请求方需要调用部署在不同平台上的功能模块时，调用请求方只需调用该通用接口，并提供相关的字段标识，即可完成多平台之间的 API 接口调用，另一方面，本申请实施例能够根据回调请求中的数据格式，返回数据格式与回调请求中的数据格式一致的回掉结果，即本申请实施例具有灵活的报文转换功能。再一方面，本申请实施例能够对数据进行加密，使得数据的传输具有较高的安全性。

实施例七

35 本申请实施例公开了一种计算机程序产品，该计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质，且该计算机程序可操作来使计算机执行实施例一、实施例二中任意一个实施例所描述的分布式的智能 API 异步回调方法中的步骤。

本申请实施例能够根据功能相似性，将不同平台中具有相同功能的功

能模块进行整合，进而生成一个对外开放的通用接口，进而当调用请求方需要调用部署在不同平台上的功能模块时，调用请求方只需调用该通用接口，并提供相关的字段标识，即可完成多平台之间的 API 接口调用，另一方面，本申请实施例能够根据回调请求中的数据格式，返回数据格式与回调请求中的数据格式一致的回掉结果，即本申请实施例具有灵活的报文转换功能。再一方面，本申请实施例能够对数据进行加密，使得数据的传输具有较高的安全性。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中沒有详述的部分，可以参见其他实施例的相关描述。

作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储器中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储器中，包括若干指令用以使得一台计算机设备（可为个人计算机、服务端或者网络设备）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储器包括：U 盘、只读存储器（ROM, Read-Only Memory）、随机存取存储器（RAM, Random Access Memory）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读取存储器中，存储器可以包括：闪存盘、只读存储器（英文：Read-Only Memory，简称：ROM）、随机存取器（英文：Random Access Memory，简称：RAM）、磁盘或光盘等。

以上对本申请实施例进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求 书

1. 一种分布式的智能 API 异步回调方法，应用于服务端，其特征在于，所述方法执行以下步骤：

步骤 101，接收 API 接口请求信息；

步骤 102，按照预设的解密规则对所述 API 接口请求信息进行数据解密，解密后的 API 接口请求信息包括 API 接口标识、用户标识和数据报文格式；

步骤 103，对所述用户标识进行验证；

步骤 104，根据所述 API 接口标识，按照预设筛选规则从多个 API 平台中筛选出包括被调用的 API 接口的 API 平台，被调用的 API 接口为 API 接口标识所指示的 API 接口；

步骤 105，基于所述包括被调用的 API 接口的 API 平台，异步回调所述 API 接口标识所指示的 API 接口。

2. 如权利要求 1 所述的分布式的智能 API 异步回调方法，其特征在于，所述步骤 101 之前，所述方法还包括：

接收公钥请求，并根据所述公钥请求生成认证公钥和认证密钥；

发送所述认证公钥。

3. 如权利要求 2 所述的分布式的智能 API 异步回调方法，其特征在于，在所述步骤 101 与所述步骤 102 之间，所述方法还包括：

使用所述认证密钥对所述 API 接口请求信息进行验证。

4. 如权利要求 1 所述的分布式的智能 API 异步回调方法，其特征在于，在步骤 102 和步骤 103 之间，所述方法还包括：

将所述 API 接口请求信息中的所述数据报文格式与服务端默认设定的数据报文格式进行比对；

若所述 API 接口请求信息中的所述数据报文格式与默认设定的数据报文格式不一致，则按照默认设定的数据报文格式对所述 API 接口请求信息进行格式转换。

5. 如权利要求 1 所述的分布式的智能 API 异步回调方法，其特征在于，根据所述 API 接口标识，按照所述预设筛选规则从所述多个 API 平台中筛选出所述包括被调用的 API 接口的 API 平台包括：

根据所述 API 接口标识，从所述多个 API 平台中筛选出当前访问量最小的 API 平台。

6. 如权利要求 1 所述的分布式的智能 API 异步回调方法，其特征在于，所述 API 接口请求信息还包括业务任务数据；

以及，所述基于所述包括被调用的 API 接口的 API 平台，异步回调所述 API 接口标识所指示的 API 接口之后，所述方法还包括：

发送回调结果，所述回调结果为所述 API 接口标识所指示的 API 接口根据所述业务任务数据生成。

7. 如权利要求 6 所述的分布式的智能 API 异步回调方法,其特征在于,所述发送回调结果之前,所述方法还包括:

按照所述 API 接口请求信息中的所述数据报文格式对所述回调结果进行数据格式转换;

按照回调结果加密规则对所述回调结果进行加密。

8. 一种分布式的智能 API 异步回调装置,其特征在于,包括:

第一接收模块,接收 API 接口请求信息;

解密模块,按照预设的解密规则对所述 API 接口请求信息进行数据解密,解密后的 API 接口请求信息包括 API 接口标识、用户标识和数据报文格式;

验证模块,对所述用户标识进行验证;

筛选模块,根据所述 API 接口标识,按照预设筛选规则从多个 API 平台中筛选出包括被调用的 API 接口的 API 平台,被调用的 API 接口为 API 接口标识所指示的 API 接口;

接口调用模块,基于所述包括被调用的 API 接口的 API 平台,异步回调所述 API 接口标识所指示的 API 接口。

9. 如权利要求 8 所述的分布式的智能 API 异步回调装置,其特征在于,还包括:

公钥密钥生成模块,用于根据公钥请求生成认证公钥和认证密钥;

发送模块,用于发送认证公钥。

10. 如权利要求 9 所述的分布式的智能 API 异步回调装置,其特征在于,所述验证模块使用所述认证密钥对所述 API 接口请求信息进行验证。

11. 如权利要求 8 所述的分布式的智能 API 异步回调装置,其特征在于,还包括:

转换模块,将所述 API 接口请求信息中的所述数据报文格式与服务端默认设定的数据报文格式进行比对,若所述 API 接口请求信息中的所述数据报文格式与默认设定的数据报文格式不一致,则按照默认设定的数据报文格式对所述 API 接口请求信息进行格式转换。

12. 如权利要求 8 所述的分布式的智能 API 异步回调装置,其特征在于,所述筛选模块根据所述 API 接口标识,从所述多个 API 平台中筛选出当前访问量最小的 API 平台。

13. 如权利要求 9 所述的分布式的智能 API 异步回调装置,其特征在于,所述第一接收模块接收 API 接口请求信息还包括业务任务数据,所述发送模块发送回调结果,所述回调结果为所述 API 接口标识所指示的 API 接口根据所述业务任务数据生成。

14. 如权利要求 11 所述的分布式的智能 API 异步回调装置,其特征在于,所述转换模块按照所述 API 接口请求信息中的所述数据报文格式对所述回调结果进行数据格式转换。

15. 如权利要求 14 所述的分布式的智能 API 异步回调装置,其特征

在于,还包括加密模块,按照回调结果加密规则对所述回调结果进行加密。

16. 一种客户端,其特征在于,包括:

封装模块,用于封装 API 接口请求信息,接口请求信息中包含用户标识,和 API 接口标识,和 API 接口标识,和/或数据报文格式;

请求信息加密模块,用于按照预设加密规则对封装后的 API 接口请求信息进行加密;

发送模块,用于通过 POST 方式发送加密后的 API 接口请求信息;

第二接收模块,用于接收认证公钥;

监听模块,用于设置回调监听发送结果。

17. 根据权利要求 16 所述的客户端,其特征在于,还包括:

回调结果解密模块,用于对回调结果进行解密。

18. 一种服务端,其特征在于,包括:

至少 1 个存储单元;

与所述至少 1 个存储单元耦合的处理单元;

其中,所述至少 1 个存储单元用于存储计算机指令;

所述处理单元用于调用所述计算机指令,以执行以下步骤:

步骤 101,接收 API 接口请求信息;

步骤 102,按照预设的解密规则对所述 API 接口请求信息进行数据解密,解密后的 API 接口请求信息包括 API 接口标识、用户标识和数据报文格式;

步骤 103,对所述用户标识进行验证;

步骤 104,根据所述 API 接口标识,按照预设筛选规则从多个 API 平台中筛选出包括被调用的 API 接口的 API 平台,被调用的 API 接口为 API 接口标识所指示的 API 接口;

步骤 105,基于所述包括被调用的 API 接口的 API 平台,异步回调所述 API 接口标识所指示的 API 接口。

19. 如权利要求 18 所述的服务端,其特征在于,所述处理单元用于调用所述计算机指令,以执行以下步骤:

在按照所述预设的解密规则对所述 API 接口请求信息进行数据解密与对所述用户标识进行验证之间,所述步骤还包括:

将所述 API 接口请求信息中的所述数据报文格式与服务端默认设定的数据报文格式进行比对;

若所述 API 接口请求信息中的所述数据报文格式与默认设定的数据报文格式不一致,则按照默认设定的数据报文格式对所述 API 接口请求信息进行格式转换。

20. 一种计算机非易失性存储介质,其特征在于,所述计算机非易失性存储介质存储有计算机指令,所述计算机指令被调用时,用于执行权利要求 1-7 任一项所述的分布式的智能 API 异步回调方法。

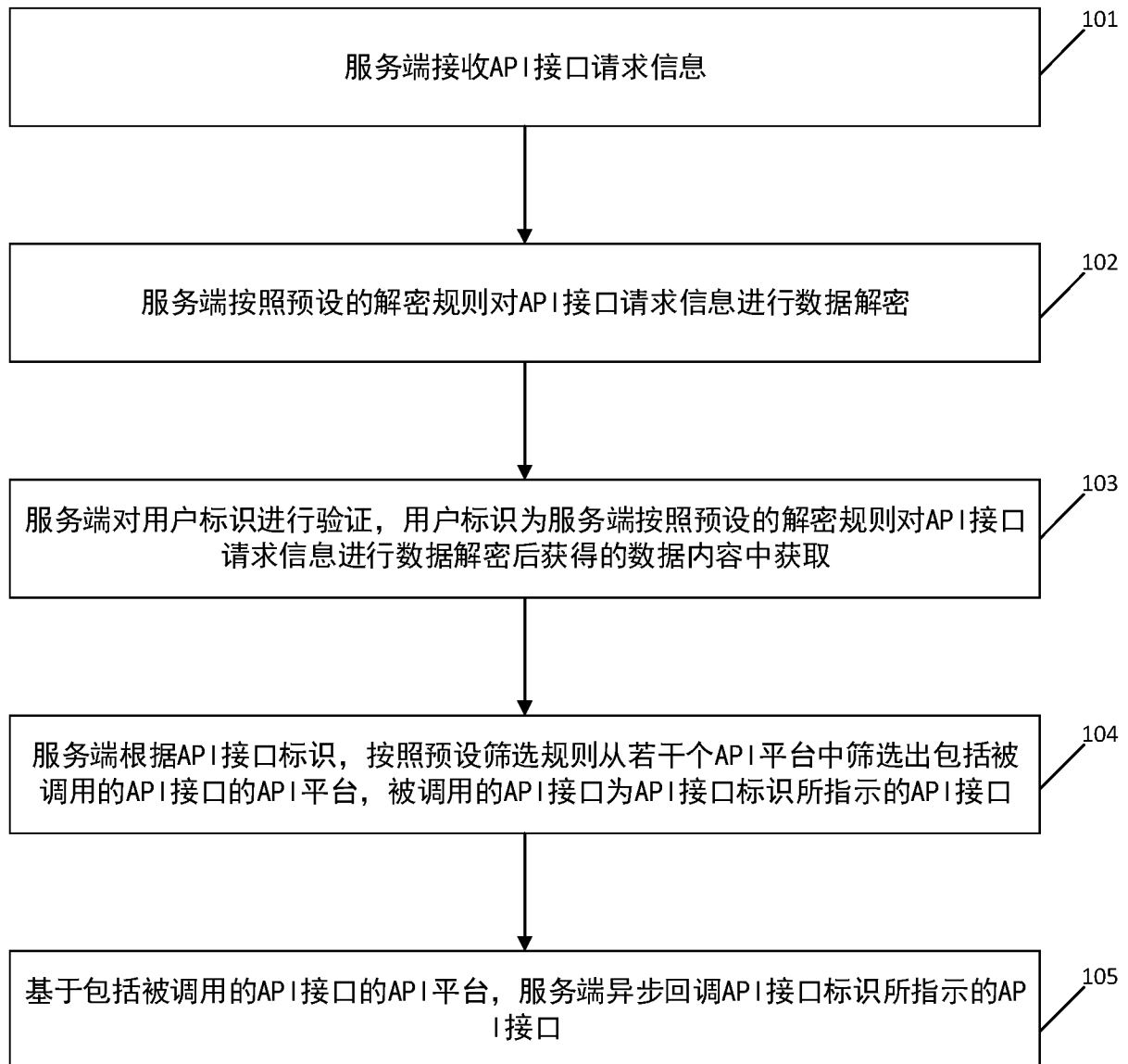


图 1

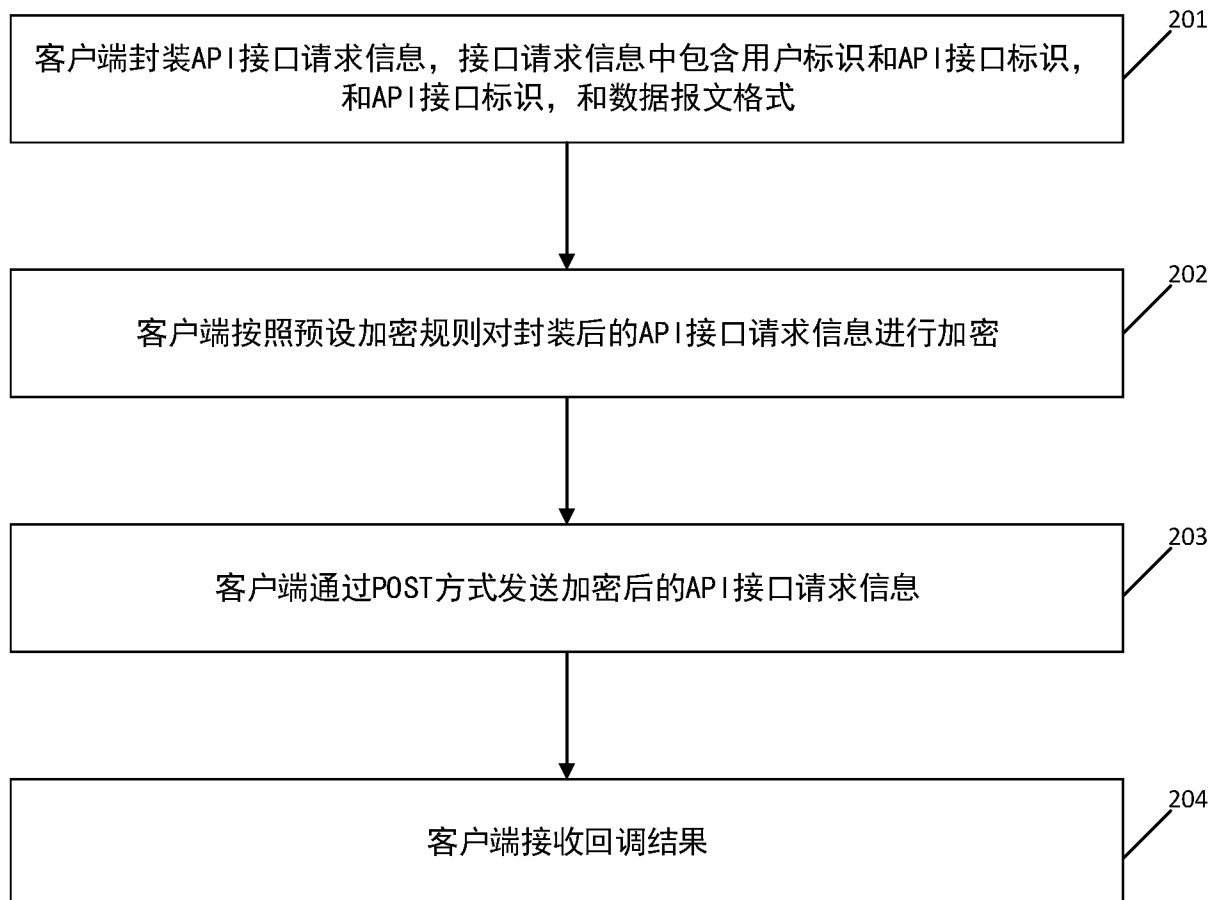


图 2

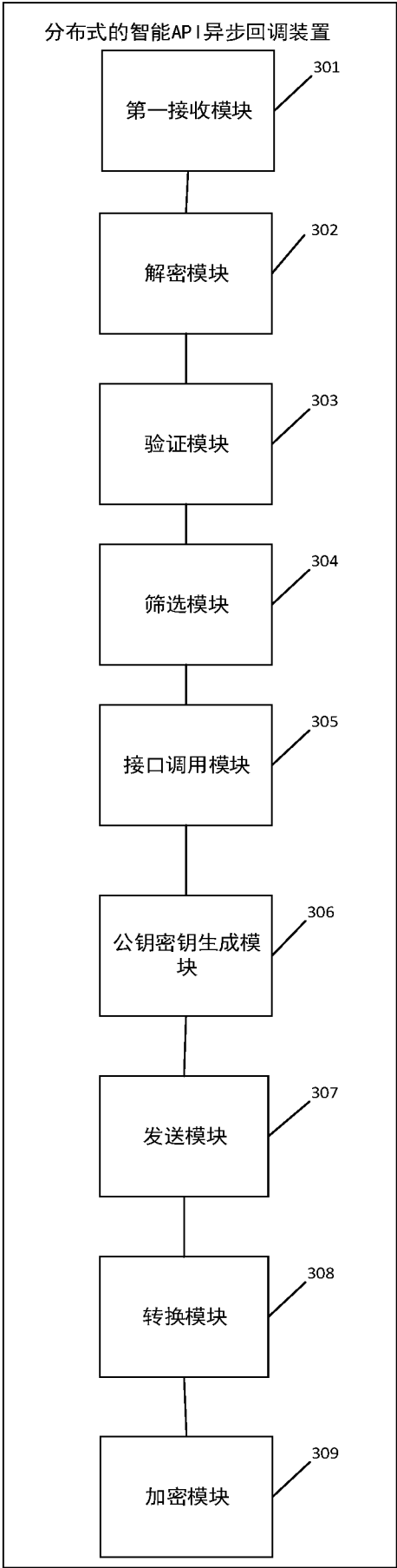


图 3

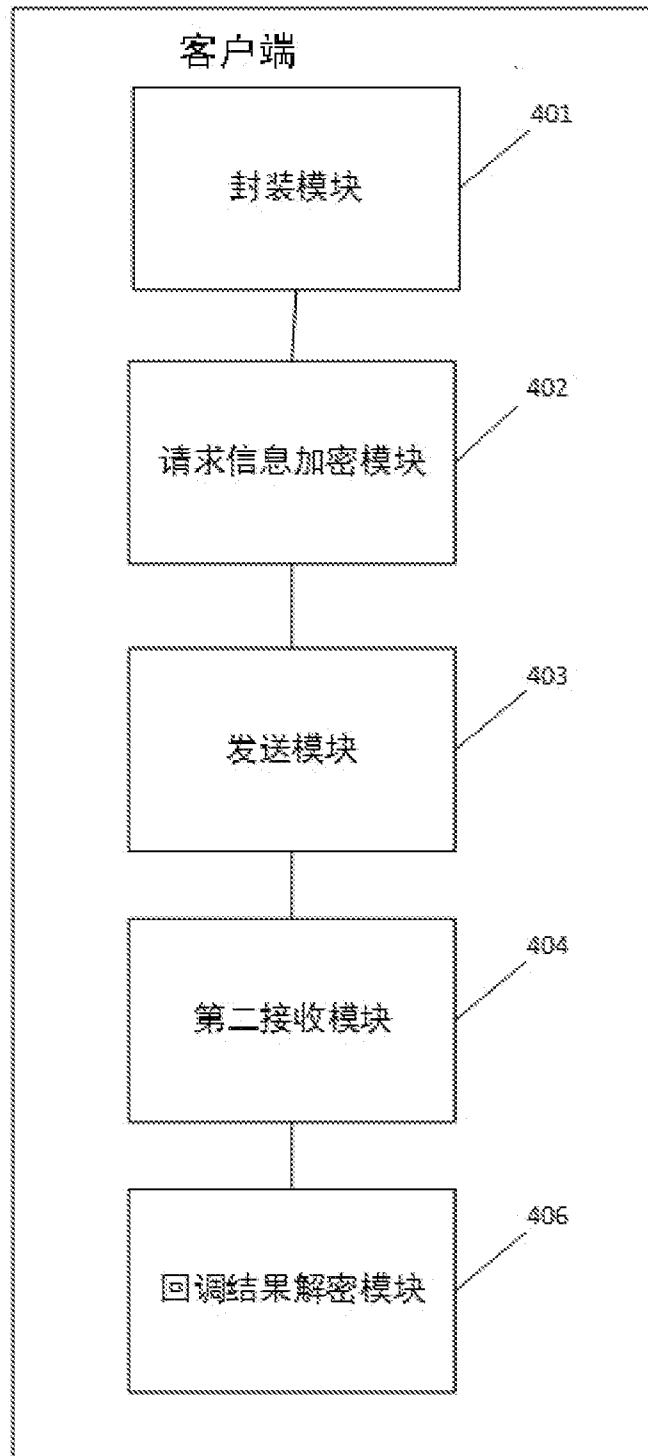


图 4

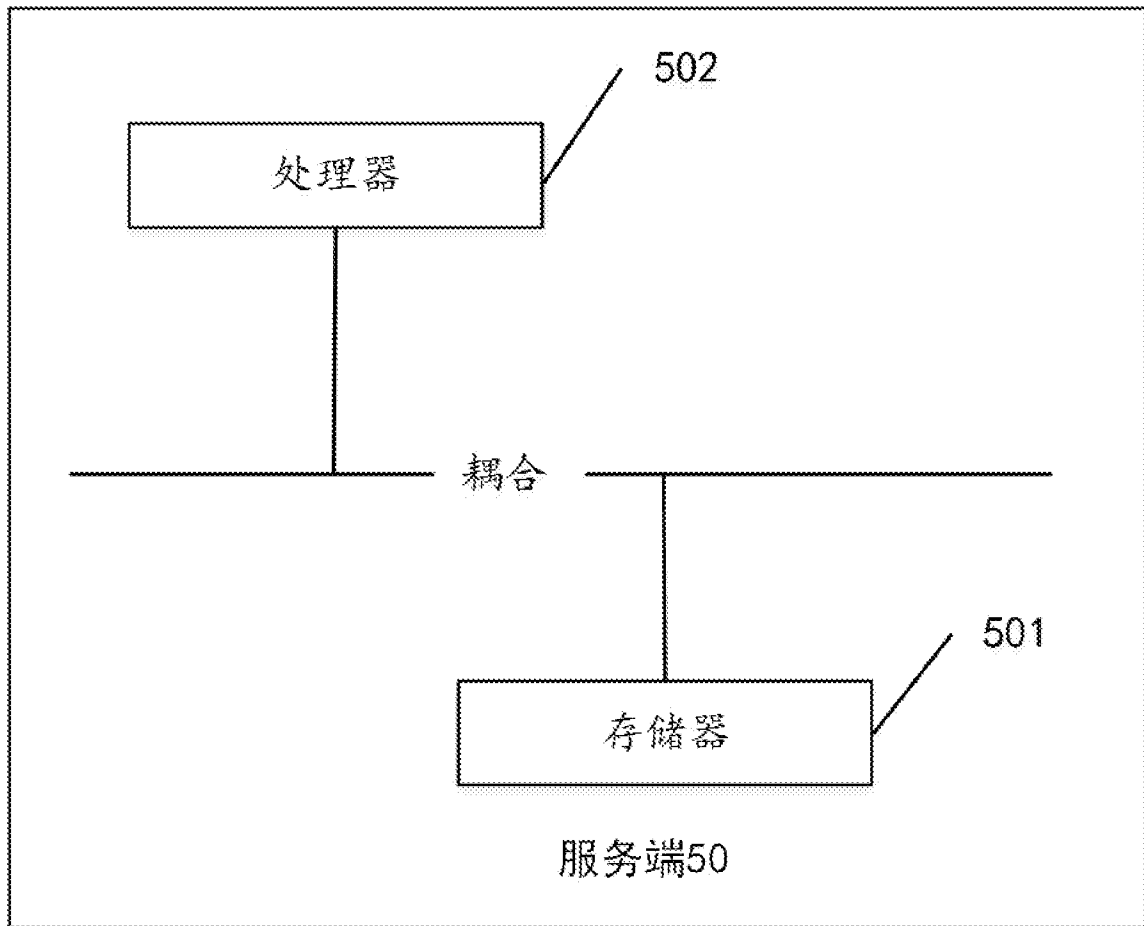


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/117893

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/54(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC, GOOGLE: API, 应用程序接口, 接口, 平台, 多, 不同, 通用, 标准, 标识, 格式, 加密, 解密, 验证, 身份, 用户, 指示, 密钥, 公钥, 比对, 比较, 选择, 筛选, 规则, 调用, 转换, 变换, interface, platform, different, multiple, two, format, standard, identif+, user, compar+, check+, select+, rule, transfer+, convert+, key, encrypt, decrypt, secrect, public, private, validat+, authentic+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110287037 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 27 September 2019 (2019-09-27) claims 1-10, description, paragraphs 121-193	1-20
Y	CN 102792269 A (MICROSOFT CORPORATION) 21 November 2012 (2012-11-21) description, paragraphs 30-48, 67-69	1-20
Y	CN 106101258 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 09 November 2016 (2016-11-09) description, paragraphs 33-93	1-20
Y	CN 107291567 A (SHANDONG INSPUR TONGRUAN INFORMATION TECHNOLOGY CO., LTD.) 24 October 2017 (2017-10-24) description, paragraphs 84-87, 115-117	1-20
A	CN 108830099 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 16 November 2018 (2018-11-16) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance
 “E” earlier application or patent but published on or after the international filing date
 “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 “O” document referring to an oral disclosure, use, exhibition or other means
 “P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 “&” document member of the same patent family

Date of the actual completion of the international search

16 January 2020

Date of mailing of the international search report

23 January 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/117893**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 108881448 A (HANGZHOU BEIGOU TECHNOLOGY CO., LTD.) 23 November 2018 (2018-11-23) entire document	1-20
A	CN 109391689 A (ZHENGZHOU YUNHAI INFORMATION TECHNOLOGY CO., LTD.) 26 February 2019 (2019-02-26) entire document	1-20
A	US 2014165199 A1 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) 12 June 2014 (2014-06-12) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/117893

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110287037	A	27 September 2019	None			
CN	102792269	A	21 November 2012	WO	2011112964	A2	15 September 2011
				AU	2011226658	A1	20 September 2012
				EP	2545447	A2	16 January 2013
				US	2011225074	A1	15 September 2011
CN	106101258	A	09 November 2016	None			
CN	107291567	A	24 October 2017	None			
CN	108830099	A	16 November 2018	WO	2019210579	A1	07 November 2019
CN	108881448	A	23 November 2018	None			
CN	109391689	A	26 February 2019	None			
US	2014165199	A1	12 June 2014	CN	102779255	A	14 November 2012
				EP	2852913	A1	01 April 2015
				WO	2014012441	A1	23 January 2014

国际检索报告

国际申请号

PCT/CN2019/117893

A. 主题的分类 G06F 9/54 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) G06F 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNKI, CNPAT, WPI, EPDOC, GOOGLE:API, 应用程序接口, 接口, 平台, 多, 不同, 通用, 标准, 标识, 格式, 加密, 解密, 验证, 身份, 用户, 指示, 密钥, 公钥, 比对, 比较, 选择, 筛选, 规则, 调用, 转换, 变换, interface, platform, different, multiple, two, format, standard, identif+, user, compar+, check+, select+, rule, transfer+, convert+, key, encrypt, decrypt, secrect, public, private, validat+, authentic+		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 110287037 A (平安科技深圳有限公司) 2019年 9月 27日 (2019 - 09 - 27) 权利要求1-10, 说明书121-193段	1-20
Y	CN 102792269 A (微软公司) 2012年 11月 21日 (2012 - 11 - 21) 说明书30-48、67-69段	1-20
Y	CN 106101258 A (腾讯科技深圳有限公司) 2016年 11月 9日 (2016 - 11 - 09) 说明书33-93段	1-20
Y	CN 107291567 A (山东浪潮通软信息科技有限公司) 2017年 10月 24日 (2017 - 10 - 24) 说明书84-87、115-117段	1-20
A	CN 108830099 A (平安科技深圳有限公司) 2018年 11月 16日 (2018 - 11 - 16) 全文	1-20
A	CN 108881448 A (杭州贝购科技有限公司) 2018年 11月 23日 (2018 - 11 - 23) 全文	1-20
A	CN 109391689 A (郑州云海信息技术有限公司) 2019年 2月 26日 (2019 - 02 - 26) 全文	1-20
☒ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2020年 1月 16日		国际检索报告邮寄日期 2020年 1月 23日
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 孟佳 电话号码 86-10-53961713

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	US 2014165199 A1 (TENCENT TECHNOLOGYSHENZHEN COMPANY LIMITED) 2014年 6月 12日 (2014 - 06 - 12) 全文	1-20

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/117893

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	110287037	A	2019年 9月 27日	无			
CN	102792269	A	2012年 11月 21日	WO	2011112964	A2	2011年 9月 15日
				AU	2011226658	A1	2012年 9月 20日
				EP	2545447	A2	2013年 1月 16日
				US	2011225074	A1	2011年 9月 15日
CN	106101258	A	2016年 11月 9日	无			
CN	107291567	A	2017年 10月 24日	无			
CN	108830099	A	2018年 11月 16日	WO	2019210579	A1	2019年 11月 7日
CN	108881448	A	2018年 11月 23日	无			
CN	109391689	A	2019年 2月 26日	无			
US	2014165199	A1	2014年 6月 12日	CN	102779255	A	2012年 11月 14日
				EP	2852913	A1	2015年 4月 1日
				WO	2014012441	A1	2014年 1月 23日