(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
2023 年 5 月 4 日 (04.05.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/071460 A1

(51) 国际专利分类号:
H04L 67/2866 (2022.01)

(21) 国际申请号: PCT/CN2022/113751

(22) 国际申请日: 2022 年 8 月 19 日 (19.08.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111256545.5 2021年10月27日 (27.10.2021) CN

(71) 申请人: 北京字节跳动网络技术有限公司 (**BEIJING BYTEDANCE NETWORK TECHNOLOGY CO., LTD.**) [CN/CN]; 中国北京市石景山区实兴大街30号院3号楼2层B-0035房间, Beijing 100041 (CN)。

(72) 发明人: **陈兴修(CHEN, Xingxiu)**; 中国北京市海淀区知春路63号中国卫星通信大厦今日头条小邮局, Beijing 100086 (CN)。 **梁宇明(LIANG, Yuming)**; 中国北京市海淀区知春路63号中国卫星通信大厦今日头条小邮局, Beijing 100086 (CN)。 **叶剑烨(YE, Jianye)**; 中国北京市海淀区知春路63号中国卫星通信大厦今日头条小邮局, Beijing 100086 (CN)。 **郑宇(ZHENG, Yu)**; 中国北京市海淀区知春路63号中国卫星通信大厦今日头条小邮局, Beijing 100086 (CN)。 **蒋伟(JIANG, Wei)**; 中国北京市海淀区知春路63号中国卫星通信大厦今日头条小邮局, Beijing 100086 (CN)。 **魏澄(WEI, Cheng)**; 中国北京市海淀区知春路63号中国卫星通信大厦今日头条小邮局, Beijing 100086 (CN)。 **任锋(REN, Feng)**; 中国北京市海淀区知春路63号中国卫星通信大厦今日头条小邮局, Beijing 100086 (CN)。 **赵明冬(ZHAO, Mingdong)**; 中国北京市海淀区知春路63号中国卫星通信大厦今日头条小邮局, Beijing 100086 (CN)。

(54) **Title:** DATA EXCHANGE METHOD, SYSTEM AND APPARATUS, AND DEVICE

(54) **发明名称**: 用于数据交换的方法、系统、装置和设备

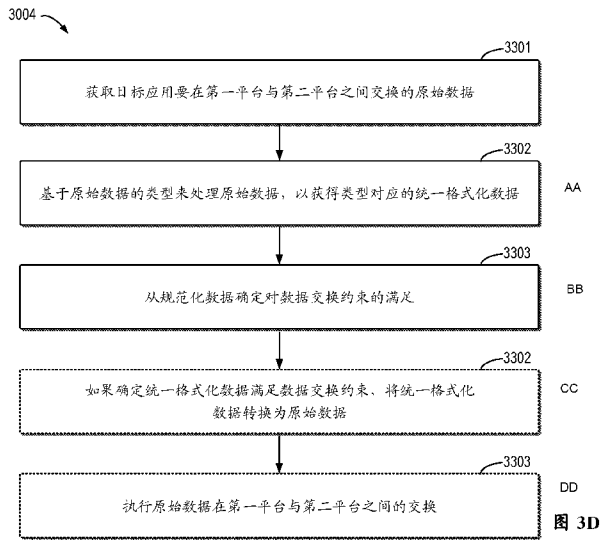

图 3D

3301 Acquire original data to be exchanged by a target application between a first platform and a second platform
AA Process the original data on the basis of the type of the original data, so as to obtain uniformly formatted data corresponding to the type
BB Determine, from normalized data, the satisfaction of a data exchange constraint
CC If it is determined that the uniformly formatted data satisfies the data exchange constraint, convert the uniformly formatted data into the original data
DD Execute the exchange of the original data between the first platform and the second platform

(57) **Abstract:** According to the embodiments of the present disclosure, provided are a data exchange method, system and apparatus, and an electronic device, a storage medium and a program product. The method described herein comprises: acquiring original data to be exchanged by a target application between a first platform and a second platform; processing the original data on the basis of the type of the original data, so as to obtain uniformly formatted data corresponding to the type; and determining, from the uniformly formatted data, the satisfaction of a data exchange constraint. On the basis of such means, by means of the embodiments of the present disclosure, the determination of a data exchange constraint can be simplified and facilitated, thereby accelerating a data exchange process.

WO 2023/071460 A1

[见续页]

(74) 代理人：北京市金杜律师事务所(KING & WOOD MALLESONS)；中国北京市朝阳区东三环中路1号环球金融中心办公楼东楼20层, Beijing 100020 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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：根据本公开的实施例，提供了一种用于数据交换的方法、系统、装置、电子设备、存储介质和程序产品。在此描述的方法包括：获取目标应用要在第一平台与第二平台之间交换的原始数据；基于原始数据的类型来处理原始数据，以获得类型对应的统一格式化数据；以及从统一格式化数据确定对数据交换约束的满足。基于这样的方式，本公开的实施例可以简化和促进关于数据交换约束的确定，加速数据交换过程。

用于数据交换的方法、系统、装置和设备

本申请要求于 2021 年 10 月 27 日提交中国国家知识产权局、申请号为 202111256545.5、申请名称为“用于数据交换的方法、系统、装置和设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本公开的各实现方式涉及计算机领域，更具体地，涉及用于数据交换的方法、系统、装置、设备、计算机存储介质和计算机程序产品。

背景技术

随着互联网技术的发展，各式各样的互联网应用已经成为人们生活中的重要部分。这样的应用每天将产生海量的数据，由此带来了各方面的诸如数据主权保护等数据安全问题。例如，一些国家可能禁止特定类型的用户数据被发送到海外的服务器。

对于一些全球化应用而言，这样的挑战是更为显著的。这样的全球化应用可能需要基于相同的技术架构来为多个不同区域的用户提供服务。然而，这些区域可能具有完全不同的数据安全约束，例如特定的数据主权保护要求，这导致数据安全保护的难度进一步加大。

发明内容

在本公开的第一方面，提供了一种数据交换方法。该方法包括：获取目标应用要在第一平台与第二平台之间交换的原始数据；基于原始数据的类型来处理原始数据，以获得类型对应的统一格式化数据；以及从统一格式化数据确定对数据交换约束的满足。

在本公开的第二方面，提供了一种数据交换系统。该数据交换系统包括：第一数据中心，被配置为获取目标应用要在第一平台与第二平台之间交换的原始数据，并且基于所述原始数据的类型来处理所述原始数据，以获得所述类型对应的统一格式化数据；以及第二数据中心，被配置为从所述第一数据中心获取所述统一格式化数据，并且从所述统一格式化数据确定对数据交换约束的满足。

在本公开的第三方面，提供了一种用于数据交换的装置。该装置包括：获取模块，被配置为获取目标应用要在第一平台与第二平台之间交换的原始数据；预处理模块，被配置为基于原始数据的类型来处理原始数据，以获得类型对应的统一格式化数据；以及约束满足确定模块，被配置为从统一格式化数据确定对数据交换约束的满足。

在本公开的第四方面，提供了一种电子设备。该设备包括：存储器和处理器；其中存储器用于存储一条或多条计算机指令，其中一条或多条计算机指令被处理器执行以实现根据本公开的第一方面的方法。

在本公开的第五方面，提供了一种计算机可读存储介质，其上存储有一条或多条计算机指令，其中一条或多条计算机指令被处理器执行实现根据本公开的第一方面的方法。

在本公开的第六方面，提供了一种计算机程序产品，其包括一条或多条计算机指令，其中一条或多条计算机指令被处理器执行实现根据本公开的第一方面的方法。

附图说明

结合附图并参考以下详细说明，本公开各实施例的上述和其他特征、优点及方面将变得更加明显。在附图中，相同或相似的附图标注表示相同或相似的元素，其中：

图 1 示出了根据本公开实施例的数据安全保护系统的示意性框图；

图 2 示出了根据本公开的一些实施例的计算安全子系统的示意性框图；

图 3A 示出了根据本公开的一些实施例的在其中部署数据交换子系统的示例部署环境；

图 3B 示出了根据本公开的一些实施例的在 TTP 方的内部数据中心（IDC）和非 TTP 所处的境外内部数据中心（RoW IDC）中 DES 的实现；

图 3C 示出了根据本公开的一些实施例的 DE 的示例架构的框图；

图 3D 示出了根据本公开的一些实施例的数据交换过程的流程图；

图 3E 示出了根据本公开的一些实施例的在 DES 处实现的各类数据处理的示例数据流的流程图；

图 3F 示出了根据本公开的一些实施例的涉及 MQ 通道的数据交换架构的示意框图；

图 3G 示出了根据本公开的一些实施例的涉及 HDFS 通道的数据交换架构的示意框图；

图 3H 示出了根据本公开的一些实施例的数据从 TTP IDC 复制到境外 IDC 的目标对象存储（TOS）通道的示意图；

图 3I 示出了根据本公开的一些实施例的数据从境外 IDC 复制到 TTP IDC 的 TOS 通道的示意图；

图 3J 示出了根据本公开的一些实施例的在 TOS 通道中的消息序列图；

图 3K 示出了根据本公开的一些实施例的涉及服务调用通道的数据交换架构的示意框图；

图 3L 示出了根据本公开的一些实施例的在服务调用通道中从非 TTP 到 TTP 的数据交换示例；

图 3M 示出了根据本公开的一些实施例的在服务调用通道中从 TTP 到非 TTP 的数据交换示例；

图 4A 示出了根据本公开的一些实施例的管理移动端应用的网络流量的方法的流程图；

图 4B 示出了根据本公开的一些实施例的针对原生类型的网络流量的分析和限制过程的示意图；

图 4C 示出了根据本公开一些实施例的针对网页视图类型的网络流量的分析和限制过程的示意图；

图 4D 示出了根据本公开一些实施例的针对第三方 SDK 类型的网络流量的分析和限制过程的示意图；

图 4E 示出了根据本公开的一些实施例的安全沙盒子系统的模块图；

图 5 示出了根据本公开的一些实施例的管理推荐策略的示例过程的流程图；

图 6 示出了根据本公开的一些实施例的用于数据交换的装置的示例框图；以及

图 7 示出了可以用来实施本公开的实施例的示例设备的框图。

具体实施方式

下面将参照附图更详细地描述本公开的实施例。虽然附图中显示了本公开的某些实施例，然而应当理解的是，本公开可以通过各种形式来实现，而且不应该被解释为限于这里阐述的

实施例，相反提供这些实施例是为了更加透彻和完整地理解本公开。应当理解的是，本公开的附图及实施例仅用于示例性作用，并非用于限制本公开的保护范围。

在本公开的实施例的描述中，术语“包括”及其类似用语应当理解为开放性包含，即“包括但不限于”。术语“基于”应当理解为“至少部分地基于”。术语“一个实施例”或“该实施例”应当理解为“至少一个实施例”。术语“第一”、“第二”等等可以指代不同的或相同的对象。下文还可能包括其他明确的和隐含的定义。

以下参考附图来说明本公开的基本原理和若干示例实现。

数据安全保护系统整体架构

根据本公开的实施例，提供了一种数据安全保护系统。图 1 示出了根据本公开实施例的数据安全保护系统 1000 的示意性框图。如图 1 所示，数据安全保护系统 1000 包括多个子系统，以用于从不同维度来保护用户在使用目标应用的过程产生的相关数据的安全。

通常而言，为了支持目标应用的运行，一方面，用户需要例如可以在通过适当的电子设备来运行目标应用 1080。另一方面，还需要在适当的计算环境（例如，云计算环境）中部署目标应用平台 1030，以例如运行用于支持目标应用 1080 的正常运行的各种类型的服务。

在一些实施例中，数据安全保护系统 1000 可以首先从运行代码的安全性的角度来保证目标应用 1090 的在运行过程中所产生的数据的安全。如图 1 所示，数据安全保护系统 1000 可以包括安全计算子系统 1060，其可以用于保证与目标应用 1080 对应的代码的安全性，以及保证与目标应用平台 1030 所对应的代码的安全性。

经计算子系统 1060 编译获得的服务运行文件例如可以被部署到目标应用平台 1030 中，经计算子系统 1060 编译获得的目标应用的安装文件（例如，apk 文件）例如可以被发布至应用商城 1120。关于安全计算子系统 1060 的具体实现将在下文结合图 2 详细讨论。

在一些实施例中，如图 1 所示，安全计算子系统 1060 可以是基于云基础设施 1070。在一些实施例中，云基础设施 1070 例如可以是由受信合作伙伴所提供。在本公开中，“受信合作伙伴”也可以称为受信技术合作方（Trusted Technology Partner，TTP），其例如可以包括在特定区域（例如，特定国家或法域）内技术上受信的任何个人、企业或组织。

在一些实施例中，如图 1 所示，数据安全保护系统 1000 可以包括由 TTP 所提供的受信安全环境 1010。与传统的应用平台部署不同，目标应用平台 1030 可以被被部署在受信安全环境 1010 中，以提高目标应用平台 1030 所产生数据的安全性，以及其运行机制的透明性和可信程度。

在一些实施例中，目标应用 1080 可以通过推荐算法来为用户提供内容推荐服务。这样的内容推荐例如可以包括但不限于：多媒体内容推荐、用户推荐、商品推荐等等。考虑到目前越来越多的推荐系统利用机器学习来实现推荐功能，这使得仅从代码程度来管理推荐机制可能难以保证推荐的公平性。

如图 1 所示，数据安全保护系统 1000 还可以包括推荐管理子系统 1050，其例如可以通过对目标应用平台 1030 所运行的推荐算法进行测试，以确保目标应用 1080 中的推荐机制的公平性。关于推荐管理子系统 1050 的具体实现，将在下文详细描述。

在一些实施例中，考虑到目标应用平台 1030 在运行服务以支持目标应用 1080 的正常运行时，目标应用平台 1030 可能需要与其当前部署的目标区域（例如，特定国家或法域）外的应用或数据中心（也称为境外应用或境外数据中心）进行交互。

通常而言，目标区域通常会通过法律或规章而对本区域内产生的数据与境外的通信进行约束。目标区域内产生的特定类型的数据可能被禁止被传递到境外。为了保证目标应用平台1030在与境外通信过程的合规性，数据安全保护子系统可以包括数据交换子系统1040。类似地，数据交换子系统1040可以被部署在受信安全环境1010中，以保证其运行的透明性和可信程度。

在一些实施例中，如图1所示，数据交换子系统1040可以包括多个数据通道，以用于不同类型的数据传输。例如，目标应用平台1030中产生的多媒体数据例如可以通过数据交换子系统1040中的相应数据通道，并经由第三方提供的内容分发网络1130来与海外应用1140和/或海外数据中心1150通信。

作为另一示例，对于一些目标应用平台1030中产生的特定内部数据，其可以通过相应的数据通道并例如可以通过直连光缆来与海外数据中心1150和海外开发部门1160通信。关于数据交换子系统1040的具体实现将在下文结合图3A至图3M详细描述。

进一步地，为了保证目标应用平台1030出口和入口通信的安全性，在一些实施例中，数据安全子系统1000还可以包括应用防火墙子系统1020。应用防火墙子系统1020例如可以被部署在受信安全环境1010中，其例如可以用于监控从目标应用1080到目标应用平台1030的数据通信，从目标应用平台1030到目标应用1080的数据通信，和/或从目标应用平台1030到第三方应用110的数据通信等。

以此方式，数据安全保护平台1000不仅可以通过数据交换子系统1040来保证目标应用平台1030与境外的数据通信的安全性和合规性，还能够通过应用防护墙子系统1020来保证目标应用平台1030与境内的各对象（例如，目标应用1080或第三方应用1110等）通信的安全性和合规性。

在一些实施例中，对于目标应用1080而言，为了保证其运行的合规性和可信程度，数据安全保护系统1000还可以包括例如由TTP管理的安全沙盒子系统1090，其使得目标应用1080的应用业务逻辑1100所涉及的不同类型的网络通信能够受到安全沙盒子系统1090的保护。由此方式，数据安全保护系统1000可以避免目标应用1080例如通过后门程序等方式来发起不合规的数据通信。关于安全沙盒子系统1090的详细实现将在下文结合图4A至图4E详细描述。

由此，基于本公开的数据安全保护系统1000，TTP可以在从目标应用的开发到运行的整个生命周期期间对代码安全性、数据安全性等各个方面进行管理和监控，从而保证与目标应用相关联的数据的安全性，并且保证其运行的合规性。

安全计算子系统

以下将参考图2来详细描述安全计算子系统1060。图2示出了根据本公开实施例的安全计算子系统1060的示意性框图。

如图2所示，安全计算子系统1060例如可以包括安全代码环境2010，其例如可以由TTP所提供。以下将结合提交新的开发代码2140来描述安全计算子系统1060的工作过程。

如图2所示，当开发者有需要部署的新的开发代码2140时，其例如可以通过由TTP提供的同步网关2150来向安全代码环境2010提交开发代码2140。相应地，开发代码2140将被同步至由安全代码环境2010中的代码库2160。

在一些实施例中，当开发者需要利用新的开发代码2140来进行编译时，开发者例如可以

通过同步网关 2150 来向制品构建系统 2080 来发送构建请求。

备选地，当代码库 2160 接收到新的开发代码 2140 时，代码库 2160 也可以自动地向制品构建系统 2080 发送代码合并事件，以触发制品构建系统 2080 以启动制品（artifact，例如可执行代码）的构建过程。

当构建过程被启动后，代码拉取模块 2090 可以从代码库 2160 获取用于构建的代码文件。在一些实施例中，用于构建的代码文件例如可以是由开发者所指定的，或者是由制品构建系统 2080 所自动地确定的。

进一步地，编译模块 2100 可以对由代码拉取模块 2090 从代码库 2160 中所拉取的代码进行编译，以例如编译为中间代码。

在一些实施例中，考虑到代码编译过程中往往还会利用引入一些第三方代码。安全计算子系统 1060 也需要保证所引入的第三方代码的安全性。

如图 2 所示，安全计算子系统 1060 可以包括第三方独立网关 2030，以用于检查并确认所需要引入的第三方库 2020 的安全性。应当理解，这样的第三方库例如也可能是经编译的链接库或者是源代码本身。

通过安全性检查的第三方库 2020 可以被添加到制品库 2040 中。如图 2 所示，在制品的构建过程中，编译模块 2100 还可以从制品库 2040 中获取编译当前制品所依赖的其他制品，例如历史已经编译生成的制品，或者基于第三方库 2020 生成的制品等。

进一步地，编译模块 2100 例如可以将从代码库 2160 所拉取的代码和从制品库 2040 所获取的依赖制品，并将其编译生成中间代码，以由安全代码扫描模块 2110 执行代码安全性检测。

应当理解，由 TTP 管理的安全代码扫描模块 2110 可以执行任何适当的代码扫描过程来执行安全性检查，这样的扫描规则对于开发者来说是未知的，由此可以保证用于编译得到最终制品的代码的安全性。

在一些实施例中，上传模块 2120 可以根据安全代码扫描模块 2110 的结果来执行相应的上传。如果安全代码扫描模块 2110 确定编译获得的中间代码是安全的，则上传模块 2120 可以将进一步编译得到的可执行文件上传至制品库 2040。

进一步地，如果安全代码扫描模块 2110 确定编译获得的中间代码是安全的，上传模块 2120 还可以将可执行文件的签名信息上传至制品签名管理模块 2060。

相反，如果安全代码扫描模块 2110 确定当前中间代码具有相应风险，则上传模块 2120 可以将相关风险上传至问题追踪系统 2070，以例如形成风险分析报告。相应地，所编译得到的可执行文件将被禁止上传至制品库 2040。

在一些实施例中，代码库 2160 中的开发代码 2140 例如还可以在一个受信环境中被提供，以例如进行人工核查。如果确定开发代码 2140 存在风险，则该结果同样可以被上报至问题追踪系统 2070。

在一些实施例中，如果安全代码扫描模块 2110 确定当前中间代码具有相应风险，则上传模块 2120 还可以通知回调模块 2130，以在代码库 2160 中将相应代码标记为风险代码。

在一些实施例中，由 TTP 维护的问题追踪系统 2070 例如可以将所接收的风险上报信息发送至开发代码 2140 的开发者或者维护者，以提醒其当前开发代码 2140 无法通过安全检查，因此无法被部署。

在一些实施例中，如果开发代码 2140 通过安全性检查，其可以被编译成可执行文件，并进一步被添加到制品库 2040，以例如经由部署网关 2050 而被部署。

在一些实施例中，在部署从制品库 2040 获取的制品（即，可执行文件）之前，部署网关 2050 可以通过制品签名管理系统 2060 来验证制品的签名是否有效。当制品的签名有效性被确认后，部署网关 2050 可以将基于开发代码 2140 所生成的制品部署到网络中。

在一些实施例中，制品例如可以是在客户设备处执行的应用程序，则部署网关 2050 例如可以将所生成的安装文件（例如，apk 文件）发布至相应的应用商店，以供用户下载。由此，本公开的实施例可以保证用户能够下载并安装的安装文件总是由安全代码环境 2010 经由部署网关 2050 所发布的。

在一些实施例中，制品例如可以是用于部署到目标应用平台 1030 中的服务程序。具体而言，目标应用的维护方可能向部署平台发起将特定制品部署到目标应用平台 1030 中的请求。相应地，在该请求通过审核后，目标应用平台 1030 可以从制品库 2040 获取待部署的特定制品，并且对该特定制品的签名进行认证。在该制品的签名通过认证后，该制品例如可以通过以虚拟机或容器的方式被部署到目标应用平台 1030 中。

由此，基于所讨论的安全计算子系统，本公开的实施例能够从代码上传、代码编写、代码编译、第三方库引用等各个环节来有效地监控从代码转换为真正部署使用的应用程序或服务程序的过程。基于这样的方式，本公开的实施例能够有效地避免在源代码中引入的各种安全漏洞或合规风险。

数据交换子系统

应用的运行会涉及在不同国家、地区管辖的应用平台之间进行数据交互。例如，在图 1 所示的示例中，期望在目标应用平台 1030 与同一应用在境外运行的目标应用平台之间交互数据，以提供应用的全球数据交互。如前所述，数据交换子系统（DES）1040 可以支持目标应用的公共数据和满足规则的其他数据在不同平台之间进行同步，并且确保所交换的数据的安全性和合规性。总体上，DES 1040 被配置为检测在不同平台之间的数据是否满足数据交换约束。数据交换约束可以包括为了满足国家或地区的法律和法规等设置的约束，由于企业、组织和/或用户保护的其他方面的要求而需要设置的约束，等等。

例如，在具有特定数据主权保护要求的国家或地区，可能要由 TTP 进行涉及数据主权保护的检查。因此，在涉及跨平台的数据交换的很多情况下都需要保护数据交换的安全性和合规性。特别是在设置 TTP 机房后，外界与 TTP 机房存储的数据交换会受到约束，希望与 TTP 方交互的数据会经过数据主权保护的检查。在这样的示例中，数据交换约束可以包括与特定国家或地区的数据主权保护要求相关的规则。

这类的交互数据可以划分为两个方面，一个方面包括平台之间的互通类数据，另一方面包括平台的运维人员对平台的访问或操作等运维类数据。互通类数据主要用于在两个平台之间进行同步，确保应用的功能完整性，这类数据需要经过 DES 系统以进行安全性和合规性的检查。互通类数据例如包括在线业务数据，离线数据等。运维类数据的检查是要确保运维人员在运维控制面上的操作也是合规的。

图 3A 示出了根据本公开的一些实施例的在其中部署 DES 1040 的示例部署环境 3001。

在图 3A 中，TTP 方 3027 指的是在特定国家或地区中需要受到 TTP 监督和约束的环境。TTP 方 3027 可以涉及用于运行、管理、维护目标应用的各种组件，例如包括业务系统 3028、运营平台 3029、在线存储 3030、离线存储 3031 等。TTP 方 3027 还包括运维平台 3032，运维人员会需要访问运维平台 3032，以实现对目标应用的访问、管理或维护等。

类似地，非 TTP 方 3020 指的是在特定国家或地区之外的一个或多个其他国家或地区所属的环境，其不受到 TTP 方 3027 所处国家或地区的数据交换约束。非 TTP 方 3020 可以涉及用于运行、管理、维护目标应用的各种组件，例如包括业务系统 3020、运营平台 3021、在线存储 3022、离线存储 3023 等。非 TTP 方 3020 还包括运维平台 3024，运维人员会需要访问运维平台 3024，以实现对本地应用或应用平台的访问、管理或维护等。

境内用户流量会流通过 TTP 方 3027 的一些组件，境外用户流量会流通过非 TTP 方 3020 的一些组件。在本文中，“境内用户流量”指的是在该特定国家或地区管辖的应用平台上产生的用户流量，“境外用户流量”指的是在该特定国家或地区之外的一个或多个其他国家或地区管辖的应用平台上产生的用户流量。

在图 3A 的环境中，互通类数据包括在 TTP 方与非 TTP 方之间交换的境内用户流量与境外用户流量。互通类数据会经过 DES 1040，以便进行数据安全性和合规性等方面的检查。此外，还可以设置运营网关 3026，以用于对运维类数据执行数据安全性和合规性等方面的检查。

如下文将详细讨论的，在 DES 1040 中，可以根据数据的类型设置不同的数据通道，以在相应的通道中执行对要交换的数据的检查。图 3A 示意性示出了一些通道，包括目标对象存储（TOS）通道，消息队列（MQ）通道，离线聚合数据通道，日志（LOG）通道，服务调用通道等。

对于数据交换的双方，可以均有各自的 DES 来实现数据保护，例如用于对流入数据和/或流出数据的保护。

图 3B 进一步示出了在 TTP 方的内部数据中心（IDC）和非 TTP 所处的境外内部数据中心（RoW IDC）中 DES 1040 的实现。

在图 3B 中，TTP IDC 3056 指的是针对在特定国家或地区运行的目标应用的 IDC，其受到 TTP 的数据保护检测，境外 IDC 3059 指的是在特定国家或地区之外的一个或多个其他国家或地区中运行目标应用的 IDC，其可能受到其他国家或地区的数据保护约束。

如图 3B 所示，DES 1040A 被实现在 TTP IDC 3056 中，用于检测外部流入和/或内部流出的数据。DES 1040B 被实现在境外 IDC 3059 中，用于检测外部流入和/或内部流出的数据。DES 1040A 和 DES 1040B 可以被认为是 DES 1040 的具体部署实例。

从 TTP IDC 3056 角度来看，从外部流入的数据或内部流出的数据可以包括多种类型的数据，下文将举例描述。

如图 3B 所示，对于 TTP IDC 3056，外部流入的数据可以包括用户请求，例如来自特定国家或地区境内的用户通过境内运行的目标应用 3058 发起的主动请求。如本文中其他部分将描述的，在一些实施例中，用户请求还可以经过移动沙盒和/或 TTP IDC 3056 中的防火墙网关 3057 等被进行安全性保护。用户请求会到达 TTP IDC 3056 中的境内应用平台 3041 进一步处理。在一些示例中，境内应用平台 3041 可以包括各种服务、供应商网关、存储等等组件。此外，如果用户请求是要被传送到 TTP IDC 3056 以外的数据中心，该用户请求会被传递到 DES 1040A 进行数据保护。

在一些实施例中，对于 TTP IDC 3056，外部流入的数据还可以包括由供应商 3055 发起的供应商请求，例如请求境内应用平台的特定服务。例如，第三方供应商可能会调用境内应用平台的应用程序接口（API），例如 OpenAPI。由于不能确认第三方供应商是否属于境内用户，供应商请求会经由 TTP IDC 3056 中的第三方网关 3040 被送到境内应用平台 3041 中的供应商网关进行检查，以确定是否是境内用户。如果发起请求的供应商是境内用户，那么供应

商请求可以被正常响应。如果发起请求的供应商是境外用户，那么供应商请求会经过 DES 1040A 被传送。

在一些实施例中，对于 TTP IDC 3056，外部流入的数据还可以包括从境外 IDC 3059 同步到 TTP IDC 3056 的数据。例如，如果对于境外流入数据需要进行数据安全审核时，境外流入数据也需要经过 DES 1040A 的处理。

在一些实施例中，对于 TTP IDC 3056，外部流入的数据还可以包括运维人员对 TTP IDC 3056 的运维操作，例如对 TTP IDC 3056 的变更。这样操作可以包括代码类变更，配置类变更，日志维护等。代码类变更例如可以包括新功能的上线、bin 文件发布等。代码类变更可以由本国际或地区的应用平台的境内运维人员执行。配置类变更可以包括对目标应用的一些设置的启用或禁用，调度的流量配置等。在一些情况下，对于跨国运营的应用平台，可以由境外平台运维人员执行配置类变更。当然，这仅取决于不同应用的管理要求。日志维护指的是对 TTP IDC 3056 中的日志 3044 进行维护。

在一些实施例中，境内运维人员或境外运维人员可以网络隔离的条件下对 TTP IDC 3056 执行运维操作，以进一步确保数据主权保护。如图 3B 所示，境内运维人员在网络隔离的情况下发起运维操作，运维操作会经由负载均衡器 3045 进行分配，以分布到 TTP IDC 3056 中的代码 3042 处，运维平台 3043 处或日志 3044 处。除网络隔离之外，境外运维人员的运维操作会经由运营网关 3046 来进一步进行安全检查，然后被分布到 TTP IDC 3056 中的代码 3042 处，运维平台 3043 处或日志 3044 处。

在一些实施例中，对于 TTP IDC 3056，内部流出的数据可以包括在应用平台的运行过程中从境内应用平台 3041 发起的第三方请求，以用于请求第三方服务 3054，例如在公共网络中的第三方服务。第三方请求也需要由 DES 1040A 进行数据保护。

在一些实施例中，对于 TTP IDC 3056，内部流出的数据还可以包括从 TTP IDC 3056 同步到境外 IDC 3059 的数据。例如，在目标应用运行中，可能会需要将存储在 TTP IDC 3056 中的用户内容同步到境外 IDC 3059。根据数据主权保护的一些规定，这类数据可能是 DES 1040A 需要审核的重点数据。

在一些实施例中，对于 TTP IDC 3056，内部流出的数据还可以包括代码同步数据。例如，在一些情况下，出于数据主权保护等方面的检查要求，可能会要求对目标应用或应用平台的代码审核。为了在满足数据主权保护要求的前提下不泄露代码，可能会将代码同步到安全隔离环境 3051 以供审核。安全隔离环境 3051 例如可以是不联网的机房，受监控的机房等物理环境，或者具有安全保护的虚拟计算环境，等等。

从境外 IDC 3059 的角度，其中部署的 DES 1040B 也会对类似的外部流入数据和内部流出数据进行安全保护。例如，用户通过境外运行的目标应用 3058 产生的用户请求，在经由负载均衡器 3047 到达境外应用平台 3048（其可以包括各类服务和存储）后，也可以经过 DES 1040B 保护。在运维方面，境外运维人员也可以在网络隔离的情况下经由水晶（crystal）网关 3049 对境外应用平台 3048 执行运维操作。这类运维操作也可以经由 DES 1040B 进行数据保护。

对于在 DES 1040A 或 1040B 中进行保护的数据，取决于类型不同，用于执行数据主权保护的方案以及为了实现数据主权保护所需要执行的处理也可能不同。

在本公开的实施例中，在 DES 1040（例如，DES 1040A 或 1040B）中，可以按数据的类型来对数据进行预处理，以将数据的格式统一格式化，从而简化和促进后续关于数据主权保

护的检查，加速数据交换过程。

由此，DES 1040 中可以按数据类型划分为不同处理部分。例如，按数据来源，DES 1040A 中可以包括境内用户数据通道，用于处理特定国家或地区境内用户相关的数据；境外用户数据通道，用于处理境外用户相关的数据；工程技术数据通道，用于处理工程类、运维类数据，诸如代码、参数等各类研发数据、运维数据等。进一步地，取决于数据产生、传输、接收、存储等处理技术，各个通道中的数据还可以被进一步划分。如下文将描述的，按技术划分，不同通道中的数据可以被划分为消息队列（MQ）数据，离线聚合数据，目标对象存储（TOS）数据，服务调用数据中的一项或多项，或者其他类型的数据。

对于在数据主权保护审核中通过的数据，可以从统一格式化格式的数据转换回原始格式的数据，并提供到相应的目的地。根据本公开的方案，由于数据来源不同，不同类型的数据在数据格式、处理技术等方面都各有不同，通过统一格式化的预处理和后处理，可以降低后续在数据主权保护的审核阶段的复杂度。此外，随着数据来源的更新和技术扩展/变化等，可以只需要改变数据的预处理和后处理，而不会对数据交换约束确定阶段的处理进行复杂改动。由此，数据交换架构具有极大的灵活性和可扩展性。

下文将参考附图来详细描述一些具体实施例。

DES 的整体架构和数据流

图 3C 示出了根据本公开的一些实施例的 DES 1040 的示例架构的框图。在图 3C 的示例中，DES 1040 被示出为对目标应用在境内应用平台 3041 与外部应用平台（统称为境外应用平台 3048）之间同步数据，并执行数据交换约束的确定。

如图 3C 所示，DES 1040 可以包括 DES 适配器 3061，DES 中心和 DES 适配器 3070。DES 中心可以包括针对不同类型数据通道的 DES 中心，例如针对境内用户数据的 DES 中心 3065A，针对境外用户数据的 DES 中心 3065B，以及针对工程技术数据的 DES 中心 3065C 等。DES 中心 3065A、3065B 和 3065C 具有不同同步能力。在下文中，有时为了便于描述，DES 中心 3065A、3065B 和 3065C 可以被统称为 DES 中心 3065。

DES 适配器 3061 与境内应用平台 3041 相连，用于从境内应用平台 3041 接收要同步并且要经由 DES 1040 检测的数据，以及将从境外应用平台 3048 接收到并且经过 DES 1040 检测的数据发送给境内应用平台 3041。DES 适配器 3070 与境外应用平台 3048 相连，用于将境内应用平台 3041 接收到并且经过 DES 1040 检测的数据发送给境外应用平台 3048，并且从境外应用平台 3048 接收要同步并且要经由 DES 1040 检测的数据。DES 适配器 3061 和 DES 适配器 3070 均与 DES 中心 3065 互连，以向 DES 中心 3065 传送数据。

各个 DES 中心 3065 被配置为利用数据交换约束来检测数据，以确保在两个应用平台之间交换的数据的安全性和合规性。通常，满足数据交换约束的数据会通过 DES 1040 被传递到相应的目的地，而不满足数据交换约束的数据可能会被 DES 1040 驳回。

DES 适配器 3061 和 3070 可以被配置为对要传入 DES 中心 3065 的数据执行预处理和后处理，以使 DES 中心 3065 在各个数据类型对应的统一格式化数据基础上进行关于数据交换约束是否被满足的确定。

在一些实施例中，DES 1040 中的 DES 适配器 3061 和 DES 中心 3065 可以与境内应用平台 3041 一起被实现在 TTP IDC 3056 中，DES 适配器 3070 可以与境外应用平台 3048 一起被实现在境外 IDC 3059 中。

在一些实施例中，可以隔离 DES 1040 中的不同组件，以进一步确保更有效的数据隔离。这样的数据隔离可以通过将不同组件部署在不同数据中心来实现。在一些实施例中，可以通过应用虚拟私有数据中心（VPC）技术来实现数据隔离。例如，如图 3C 所示，DES 适配器 3061 可以被实现在 VPC1 中，各个 DES 中心可以被实现在 VPC2 中，DES 适配器 3070 可以被实现在 VPC3 中。DES 中心 3065 中的数据安全性和合规性的确定可以由 TTP 执行。在数据隔离的情况下，VPC1 和 VPC3 不具有直接通信连接，但 VPC1 和 VPC3 分别与 VPC2 具有直接通信连接，可以彼此通信数据/信息。通过 VPC 技术所带来的数据隔离，部署在 VPC2 的 DES 中心 3065 可以是 TTP 信任的区域（称为 TTP 受信区域）。

在一些实施例中，DES 适配器 3061 可以包括 DES 入口 3062，其可以实现控制面的处理，例如由运维人员申请建立和管理数据通道，注册规则等，并且可以由 TTP 查看通道中的数据。DES 适配器 3061 还可以包括 DES 代理（proxy）3063，其可以实现数据面的处理，例如数据验证、数据过滤、数据转换、数据采样、日志检测，等等。类似地，在一些实施例中，DES 适配器 3070 可以控制面的 DES 入口 3072 和数据面的 DES 代理 3073。

在一些实施例中，对于境内用户数据通道，DES 中心 3065A 可以包括 DES 注册中心，用于注册数据交换约束、配置数据等等。DES 中心 3065A 还可以包括进一步细分的通道，包括针对服务调用数据的服务调用通道，针对 MQ 数据的 MQ 通道，针对离线聚合数据的 HDFS 通道（其中，HDFS 称为 Hadoop 分布式文件系统）以及针对 TOS 数据的 TOS 通道。离线聚合数据例如包括高度并行集成虚拟环境（HIVE）类型的数据。

服务调用数据例如可以包括利用各种网络协议或调用协议，例如 HTTP 协议或 RPC 协议来进行远程服务调用的数据。MQ 数据可以包括支持 MQ 协议以及类似协议的数据，例如包括各类数据库（例如，MySQL，Redis 数据库）中存储的数据。离线聚合数据可以包括基于 HDFS 技术的文件系统中的数据，以及基于其他技术的文件系统中的数据。TOS 数据包括对象文件，例如视频、音频、图像、文档、以及其他媒体文件。

在一些实施例中，虽然图 3C 中未示出，对于境外用户数据通道的 DES 中心 3065B 和对于工程技术数据通道的 DES 中心 3065C，也可以包括与 DES 中心 3065A 类似的组件。

图 3D 示出了根据本公开的一些实施例的数据交换过程 300 的流程图。过程 3004 可以被实现在 DES 1040 中。

如图 3D 所示，在框 3301，DES 1040 获取目标应用要在第一平台（例如，境内应用平台 3041）与第二平台（例如，境外应用平台 3048）之间交换的原始数据。取决于交换的方向，原始数据可以来自第一平台，并可以由 DES 1040 中的 DES 适配器 3061 接收到。或者，原始数据可以来自第二平台，并可以由 DES 1040 中的 DES 适配器 3070 接收到。

在框 3302，DES 1040 基于原始数据的类型来处理原始数据，以获得该类型对应的统一格式化数据。原始数据的处理（此处的处理也可称为预处理）可以根据原始数据的类型来确定。原始数据的类型例如可以包括 MQ 数据、离线聚合数据、TOS 数据或服务调用数据等。进一步地，在一些情况下，原始数据的处理也可以按数据来源的不同来确定。例如，根据数据来源，原始数据可以被划分为境内用户数据，境外用户数据或工程技术数据。不同类型的数据对应的格式不同，并且可以应用不同方式来产生对应的统一格式化数据。

在一些实施例中，由于数据源所使用的技术不同，同一类型的数据可能在不同格式下被提供，这增加了对技术处理的要求。因此，可以指定一个统一格式。在预处理阶段，可以通过格式转换将原始数据的格式转换为该类型下的指定格式，以获得统一格式化数据。

例如，对于 MQ 数据，可以将不同格式的 MQ 数据进行解析，以便分析由不同格式封装的消息中的内容。对于离线聚合数据和 TOS 数据，可以响应于从不同格式下的文件系统或数据系统调用这些数据的不同请求，转换为通过统一 API 来实现的文件调用请求。对于服务调用，可以将不同协议下生成的服务调用请求转换为统一协议中的服务调用请求。

对于不同类型的数据的具体预处理方式，下文将更详细描述。

在框 3303，DES 1040 从统一格式化数据确定对数据交换约束的满足。例如，DES 1040 中的 DES 中心 3065，特别是对应数据类型的 DES 中心 3065 可以执行对数据交换约束的满足与否的检查。经过统一格式化的预处理，DES 中心 3065 不需要应用各种不同技术来解析原始数据，从而更方便地利用规则来执行数据安全性和合规性的检查。

在框 3304，如果确定统一格式化数据满足数据交换约束，DES 1040 将统一格式化数据转换为原始数据。在满足数据交换约束的情况下，数据被允许在平台之间同步。为了确保数据正确同步，DES 1040 会进一步处理中间生成的统一格式化数据（即，执行后处理阶段），以将统一格式化数据转换为原始数据，其具有原始的格式。

在框 3305，DES 1040 执行原始数据在第一平台与第二平台之间的交换。由此，可以实现在满足安全性和合规性情况下的数据交换。

在一些实施例中，如上文简单提及的，可以在不同平台之间创建与不同类型的原始数据分别对应的多个数据通道，不同类型的原始数据将会被传递到对应的数据通道中进行处理。每个数据通道可以包括适合处理该类型的原始数据的预处理组件、后处理组件和关于数据交换约束的确认组件。附加地或备选地，每个数据通道可以被注册有要被应用到该特定类型的原始数据的数据交换约束。通过这样的方式，可以实现对不同类型的数据的预处理、数据交换约束的确认和后处理方面的分离。

与不同类型的数据对应的数据通道可以被灵活地创建、更新和删除。这样，如果数据的预处理和后处理方式发生变化，或者针对数据的特定类型的数据交换约束需要更新，都可以在相应数据通道中执行，而不会影响到其他数据通道。此外，根据业务需要，如果要在第一平台与第二平台之间交换的新类型的原始数据并且该新类型的数据也要执行关于数据主权保护的检查，那么可以灵活地在第一平台与第二平台之间创建新的数据通道用于处理新类型的原始数据。

图 3E 示出了根据本公开的一些实施例的在 DES 1040 处实现的各类数据处理的示例数据流 3005 的流程图。数据流 3005 涉及控制面的数据流和数据面的数据流。

在控制面，可以由运维人员在 DES 1040 中配置一个或多个类型的数据的通道，并可以实现对通道的更新和维护等。如图 3E 所示，境内运维人员可以经由 DES 入口 3062 请求配置特定数据类型和用于处理特定数据类型的通道，并将指示特定数据类型的数据目录 3081 和对特定数据类似的数据定义 3082 注册到 DES 注册中心 3066。数据定义 3082 可以指定在 DES 1040 中对不同类型的数据进行处理的通道信息，并且可以包括关于对相应类型的数据的预处理方案、后处理方案等。

类似的，境外运维人员也可以经由 DES 入口 3072 请求配置特定数据类型和用于处理特定数据类型的通道。境外运维人员也可以将指示特定数据类型的数据目录 3084 和对特定数据类似的数据定义 3085 注册到 DES 注册中心 3066。数据定义 3085 可以指定在 DES 1040 中对不同类型的数据进行处理的通道信息，并且可以包括关于对相应类型的数据的预处理方案、后处理方案等。

在数据面，不同类型的数据在 DES 1040 中会经过各自的通道。如图 3E 所示，对于服务调用数据，在 TTP IDC 侧的客户端或服务器 3086 与境外 IDC 侧的客户端或服务器 3090 之间交换服务调用请求。为了使服务调用请求满足数据主权保护要求，服务调用请求在 DES 1040 中的服务调用通道被处理。

在图 3E 的示例中，服务调用通道可以至少包括 DES 代理 3063 中的预处理模块 3087、DES 中心 3065 中的 HTTP 代理 3088，以及 DES 代理 3073 中的路由模块 3089。来自 TTP IDC 侧的客户端或服务器 3086 的服务调用请求被传送到预处理模块 3087。预处理模块 3087 利用来自数据定义 3082 中所规定的数据预处理方案来处理服务调用请求，并将统一格式化后的服务调用请求发送给 HTTP 代理 3088。

在这个示例中，假设服务调用请求被统一格式化为符合统一协议，即 HTTP 协议的请求。因此，HTTP 代理 3088 可以在确定统一格式化后的服务调用请求满足数据交换约束后，将统一格式化后的服务调用请求通过路由模块 3089 提供到另一侧的客户端或服务器 3090。在被提供到客户端或服务器 3090 之前，统一格式化后的服务调用请求被转换回到符合原始协议的服务调用请求。

对于 MQ 数据，这个类型的原始数据在 DES 1040 中的 MQ 通道被处理。在图 3E 的示例中，MQ 通道可以至少包括 DES 代理 3063 中的预处理模块 3092、DES 中心 3065 中的 MQ 传送器 3094，以及 DES 代理 3073 中的路由模块 3097。

针对 MQ 类型的原始数据 3091 被传送到预处理模块 3092。预处理模块 3092 利用来自数据定义 3082 中所规定的数据预处理方案来处理原始数据 3091，得到统一格式化数据 3093。统一格式化数据 3093 由 MQ 传送器 3094 提取，例如经由第三方软件开发工具包（SDK）提取。在经过数据交换约束的检查后，由 SDK 将满足规则的统一格式化数据 3096 推送到境外 IDC。不满足数据交换约束的统一格式化数据 3095 被驳回。路由模块 3097 将满足规则的统一格式化数据 3096 路由到对应的目的地，在被传输到目的地之前统一格式化数据 3093 被转换回对应的原始数据 3098。

对于离线聚合数据和 TOS 数据，原始数据分别会在 DES 1040 中的 HDFS 通道和 TOS 通道被处理。为简化，图 3E 示出了一个通道的示例，但可以理解，HDFS 通道和 TOS 通道可以包括图示的组件。在图 3E 的示例中，HDFS 通道或 TOS 通道可以至少包括 DES 代理 3063 中的预处理模块 3100、DES 中心 3065 中的文件传送器 3103，以及 DES 代理 3073 中的路由模块 3105。

由于离线聚合数据类型或 TOS 类型的数据被存储在文件系统或其他存储系统中，预处理模块 3100 可以向文件传送管理器 3102 发起调用文件传送 API 的请求，以获得针对离线聚合数据类型或 TOS 类型的原始数据 3099 被传送到预处理模块 3100。预处理模块 3100 可以利用来自数据定义 3082 中所规定的数据预处理方案来处理原始数据 3099，得到统一格式化数据 3101。

与 MQ 类型的数据处理类似，统一格式化数据 3101 由文件传送器 3103 提取，例如经由 SDK 提取。在经过数据交换约束的检查后，由 SDK 将满足规则的统一格式化数据 3104 推送到境外 IDC。不满足数据交换约束的统一格式化数据会被驳回，无法被传送到境外 IDC。路由模块 3105 将满足规则的统一格式化数据 3104 路由到对应的目的地，在被传输到目的地之前统一格式化数据 3094 被转换回对应的原始数据 3106。

应当理解，图 3E 仅示出了在 DES 1040 中对从 TTP IDC 到境外 IDC 的流出数据的处理。

对于相反方向的数据流，在 DES 1040 中也可以通过类似的流程处理，并且 DES 1040 也可以保留对应的组件用于支持相应的处理，特别是在 DES 适配器中的组件。

下文将针对 DES 1040 中不同类型的数据的一些示例实现进行详细讨论。

针对 MQ 的数据交换的示例实现

图 3F 示出了根据本公开的一些实施例的涉及 MQ 通道的数据交换架构 3006 的示意框图。数据交换架构 3006 可以被实现在 DES 1040 中，用于针对 MQ 类型的数据执行数据安全保护。在图 3F 的示例中，示出了从 TTP IDC 到境外 IDC 方向的数据交换。

如图 3F 所示，TTP IDC 中的源数据库 3110 产生要传送的 MQ 数据的实体。MQ 数据可以包括改变数据或者商业定制事件等消息，不同消息可以具有不同的格式。源数据库 3110 产生的 MQ 数据被放入源消息队列 3112 中。

在图 3F 的示例中，在 DES 适配器 3061 中除 DES 入口 3062 外，还包括 DES 前适配器 3120。DES 前适配器 3120 可以被实现为 DES 代理 3063 的一部分，以用于对从 TTP IDC 到境外 IDC 方向的 MQ 数据进行预处理。DES 前适配器 3120 可以被配置为将不同格式的 MQ 数据处理为具有统一格式的统一格式化 MQ 数据，并将统一格式化 MQ 数据提供给 MQ 传送器 3094，以执行关乎数据交换约束是否满足的确定。

MQ 数据（或消息）也可以包括由不同协议生成的数据，每个协议下的数据具有定制格式，因此需要不同的预处理。如图 3F 所示，DES 前适配器 3120 可以包括解析器 3122，其被配置为对不同类型的原始 MQ 数据进行解析，以将不同类型的原始 MQ 数据转换统一格式的统一格式化 MQ 数据。如图 3F 所示，DES 前适配器 3120 可以包括 MySQL 解析器，用于解析通过 MySQL 协议生成的数据，例如变化数据捕获（CDC）数据；Redis 解析器，用于解析通过 Redis 协议生成的数据，例如 CDC 数据；文档解析器，用于解析文档数据库中的数据，特别是 CDC 数据；图解析数据，用于解析图（graph）数据库的数据，特别是 CDC 数据；MQ 解析器，用于解析通过消息队列发送的不同类型的业务事件数据，等等。可以理解，解析器 3122 是可灵活缩放的，其中可以设置更多、更少或其他的解析器，用于解析相应类型的 MQ 数据。

解析后得到的统一格式化 MQ 数据也可以是消息队列的形式，可以被放入统一格式化消息的队列 3124 中。在 TTP IDC 的 VPC2 中，负责 MQ 数据的 MQ 传送器 3094 可以通过 SDK 从统一格式化消息的队列 3124 提取解析后的统一格式化 MQ 数据用于进行数据安全性和合规性检查。不满足数据的统一格式化 MQ 数据被 MQ 传送器 3094 驳回，并被记录在驳回日志 3126 中。满足数据交换约束的统一格式化 MQ 数据经由 SDK 被推送到 DES 适配器 3070 中的 DES 后适配器 3130。

DES 后适配器 3130 可以被实现为 DES 代理 3073 的一部分，以用于对从 TTP IDC 到境外 IDC 方向的统一格式化 MQ 数据进行后处理，以将数据传送到目的地。满足数据交换约束的统一格式化 MQ 数据经由 SDK 被推送到 DES 后适配器 3130。

DES 后适配器 3130 可以包括数据回放器 3132，用于对统一格式化 MQ 数据执行后处理。具体地，DES 后适配器 3130 可以被配置为将统一格式化 MQ 数据转换为原始 MQ 数据。因此，DES 后适配器 3130 可以包括与不同类型的 MQ 数据相对应的回放器（replayer），用于执行从统一格式到各自的定制格式的转换。如图 3F 所示，DES 后适配器 3130 可以包括 MySQL 回放器，用于将统一格式化 MQ 数据转换为符合 MySQL 协议的 MQ 数据；Redis 回放器，用

于将统一格式化 MQ 数据转换为符合 Redis 协议的 MQ 数据；文档回放器，用于将统一格式化 MQ 数据转换为图形式的原始数据；MQ 回放器，用于将统一格式化数据转换为符合 MQ 协议的原始数据，等等。

转换后的原始 MQ 数据被放入 DES 后适配器 3130 中的统一格式化消息的队列 3134，并从中可以被同步到目标消息队列 3135。目标消息队列 3135 用于存放从源消息队列 3112 经由 DES 1040 间接同步过来的 MQ 数据。目标数据库 3136 可以从目标消息队列 3135 获得期望的 MQ 数据。

图 3F 中仅示出了从 TTP IDC 到境外 IDC 方向的数据交换所涉及的组件。对于图 3F 的示例中，示出了从境外 IDC 到 TTP IDC 方向的数据交换，DES 1040 中可以包括类似的组件用于处理这个方向的数据交换，例如 DES 适配器 3070 可以包括具有与 DES 前适配器 3120 类似功能的 DES 前适配器，并且 DES 适配器 3061 可以包括具有与 DES 后适配器 3130 类似功能的 DES 后适配器。为简化目的，这个方向的处理不再详细展开。

可以理解，图 3F 中示出的在 DES 中用于处理 MQ 数据交换的组件仅是示例。在其他示例中，取决于需要，不同功能模块还可以按其他方式被细分、合并等，并且还可以包括更多、更少或不同的功能模块。

针对离线聚合数据的数据交换的示例实现

图 3G 示出了根据本公开的一些实施例的涉及 HDFS 通道的数据交换架构 3500 的示意框图。数据交换架构 3500 可以被实现在 DES 1040 中，用于针对离线聚合数据执行数据安全保护。在图 3G 的示例中，示出了在 TTP IDC 侧的 HDFS 3502 与境外 IDC 侧的 HDFS 3504 之间的离线聚合数据交换。在 HDFS 3502 与 HDFS 3504 中的一些离线聚合数据可能需要彼此同步。

如图 3G 所示，在数据交换架构 3500 中，TTP IDC 侧的数据传送检测器 3510 负责检测 HDFS 3502 中是否存储了需要被传送到另一侧的 HDFS 3504 的离线聚合数据。在发现要传送的离线聚合数据的情况下，数据传送递交器 3520 可以向文件传送器 3550 递交数据传送的请求。在被递交到文件传送器之间，数据预处理模块 3530 被配置为对数据执行预处理，以将离线聚合数据处理为统一格式化数据。

在文件传送器 3550 中，数据传送服务器 3556 被配置为基于利用数据交换约束来控制数据传送服务。如果数据传送服务器 3556 确定来自 HDFS 3502 的预处理后的统一格式化数据符合数据交换约束，那么可以调用传送工作 3558，以将统一格式化数据通过传送工作 3558 下的传送任务 3562 传送到境外 IDC。在一些实施例中，传送工作 3558 还可以可选地包括数据验证任务 3560，其可以被配置为根据需要执行数据验证。统一格式化数据经过 HDFS 网关 3564，并可以被执行后处理后，得到原始的离线聚合数据，并被存入 HDFS 3504。

类似的，在数据交换架构 3500 中，境外 IDC 侧的数据传送检测器 3570 负责检测 HDFS 3504 中是否存储了需要被传送到 TTP IDC 侧的 HDFS 3502 的离线聚合数据。在发现要传送的离线聚合数据的情况下，数据传送递交器 3572 可以向文件传送器 3550 递交数据传送的请求。在被递交到文件传送器之间，数据预处理模块 3570 被配置为对数据执行预处理，以将离线聚合数据处理为统一格式化数据。

在文件传送器 3550 中，如果数据传送服务器 3556 确定来自 HDFS 3504 的预处理后的统一格式化数据符合数据交换约束，那么可以调用传送工作 3554，以将统一格式化数据通过传

送工作 3554 下的传送任务 3552 传送到 TTP IDC。统一格式化数据经过后处理后，得到原始离线聚合数据，并被存入 HDFS 3502。

可以理解，图 3G 中示出的在 DES 中用于处理离线聚合数据交换的组件仅是示例。在其他示例中，取决于需要，不同功能模块还可以按其他方式被细分、合并等，并且还可以包括更多、更少或不同的功能模块。

针对对象存储的数据交换的示例实现

总体而言，TOS 通道可以确定对象文件是否满足数据交换约束、以及在约束满足的情况下将对象文件从源 IDC（例如，TTP IDC 或境外 IDC）复制到目的地 IDC（例如，境外 IDC 或 TTP IDC）。对象文件例如是视频、音频、图像、文档、或者其他媒体文件。

在一些实施例中，可以通过 API 从对象存储复制对象文件，执行数据交换约束的确定，并且利用 API 将对象文件推送到目的地端的对象存储。在对象文件的数据交换中，通过与对象文件对应的复制请求来确定对数据交换约束的满足。下文将参考图 3H 至图 3J 来描述 TOS 通道的细节。

图 3H 示出了根据本公开的一些实施例的数据从 TTP IDC 复制到境外 IDC 的目标对象存储（TOS）通道 3600 的示意图。在该示例中，要交换的数据是对象文件，其被存储在 TTP IDC 中的对象存储 3606，并且期望要被交换到境外 IDC 的对象存储 3607。

在图 3H 中，TTP IDC 中的 API 3605 被配置为将复制请求推送给工作节点 3605，并且从工作节点 3605 接收从另一侧的境外 IDC 交换过来的复制结果。如图所示，在数据流开始 3601 时，针对要交换的对象文件的复制请求由 API（也可称为 DES-TOS API）3602 传送给工作节点 3605。该复制请求可以指示要交换的对象文件相关的信息，例如对象文件的格式（视频、音频、文本等）、对象文件的标识符、以及其他文件元数据等。该复制请求具有统一格式。

受信区域 VPC2 内的工作节点 3605 被配置为响应于针对对象文件的复制请求，执行关于数据交换约束的确定。具体地，工作节点 3605 可以从统一格式化的复制请求中确定要交换的对象文件是否满足数据交换约束。

在一些实施例中，在 TTP IDC 侧，可以在初始阶段或者后续需要的时候发起数据交换约束的注册。在约束注册开始 3622 时，可以通过 TTP IDC 中的 DES 入口 3620，向 TTP 受信任区域中的 DES 注册中心 3624 注册要使用的数据交换约束。数据交换约束的注册可以通过调用 API 3602 来实现。工作节点 3605 可以通过 DES 注册中心 3624 来访问当前要使用的数据交换约束。

在一些实施例中，数据交换约束可以指示允许交换的对象文件的白名单或者不允许交换的对象文件的黑名单，在每个名单中可以按对象文件的格式、标识符等来标识允许或不允许交换的文件对象。

在执行数据交换约束，工作节点 3605 允许满足数据交换约束的复制请求的执行。如果复制请求允许被执行，工作节点 3605 访问 TTP IDC 中的对象存储 3606 以将对象文件复制到境外 IDC 中的对象存储 3607。对于非法请求（即不满足数据交换约束的复制请求），它们将被拒绝，从而无法被执行。工作节点 3605 可以将复制的对象文件经由境外 IDC 中的 API 3610 来写入对象存储 3607。这样，数据流结束 3611。

图 3I 示出了根据本公开的一些实施例的数据从境外 IDC 复制到 TTP IDC 的 TOS 通道 3650 的示意图。在该示例中，要交换的对象文件其被存储在境外 TTP IDC 中的对象存储 3607，

并且期望要被交换到 TTP IDC 的对象存储 3606。

在图 3I 中，境外 IDC 中的 API 3610 被配置为将复制请求推送给工作节点 3605，并且从工作节点 3605 接收从另一侧的 TTP IDC 交换过来的复制结果。如图 3I 所示，在数据流开始 3651 时，针对要交换的对象文件的复制请求由 API 3610 传送给工作节点 3605。该复制请求可以指示要交换的对象文件相关的信息，例如对象文件的格式（视频、音频、文本等）、对象文件的标识符、以及其他文件元数据等。该复制请求具有统一格式。受信区域 VPC2 内的工作节点 3605 可以从统一格式化的复制请求中确定要交换的对象文件是否满足数据交换约束。

在一些实施例中，在境外 IDC 侧，可以在初始阶段或者后续需要的时候发起数据交换约束的注册。在约束注册开始 3632 时，可以通过境外 IDC 中的 DES 入口 3630，向 TTP 受信任区域中的 DES 注册中心 3624 注册要使用的数据交换约束。数据交换约束的注册可以通过调用 API 3610 来实现。工作节点 3605 可以通过 DES 注册中心 3624 来访问当前要使用的数据交换约束。

在执行数据交换约束，工作节点 3605 允许满足数据交换约束的复制请求的执行。如果复制请求允许被执行，工作节点 3605 访问境外 IDC 中的对象存储 3607 以将对象文件复制到 TTP IDC 中的对象存储 3606。对于非法请求（即不满足数据交换约束的复制请求），它们将被拒绝，从而无法被执行。工作节点 3605 可以将复制的对象文件经由 TTP IDC 中的 API 3602 来写入对象存储 3606。这样，数据流结束 3652。

可以理解，图 3H 和图 3I 中示出的在 DES 中用于处理 TOS 数据交换的组件仅是示例。在其他示例中，取决于需要，不同功能模块还可以按其他方式被细分、合并等，并且还可以包括更多、更少或不同的功能模块。

图 3J 示出了根据本公开的一些实施例的在 TOS 通道中的消息序列 3012。图 3J 中的消息序列 3012 涉及 TTP 3701、运维人员 3702、平台工作人员 3703、DES 入口 3704、API 3705、工作节点 3605 和对象存储 3708。

取决于数据交换的方向，图 3J 中的 DES 入口 3704、API 3705 和对象存储 3708 可以是图 3H 和图 3I 中任一中的对应组件。例如，在图 3H 所示的从 TTP IDC 复制到境外 IDC 的 TOS 通道 3600 中，DES 入口 3704 包括图 3H 所示的 DES 入口 3620，API 3705 包括图 3H 中的 API 3602，对象存储 3708 包括图 3H 中的对象存储 3606。在从境外 IDC 复制到 TTP IDC 的 TOS 通道 3650 中，DES 入口 3704 包括图 3I 所示的 DES 入口 3630，API 3705 包括图 3I 中的 API 3610，对象存储 3708 包括图 3I 中的对象存储 3607。

在消息序列 3012 中，运维人员 3702 向 DES 入口 3704 注册 3711 数据交换约束，其可以约束对象文件在不同 IDC 的对象存储 3606 和 3607 之间的复制。在完成注册后，DES 入口 3704 可以向运维人员发送 3714 响应。DES 入口 3704 向 API 3705 注册 3712 关于数据交换约束的容器信息，并且在注册完成后 API 3705 可以向 DES 入口 3704 发送 3713 响应。经由 DES 入口 3704 注册的规则可以被高速缓存 3715 到 API 3705，并且也可以被高速缓存 3716 到工作节点 3605。

平台工作人员 3703 可以向 API 3705 发起 3717 对对象文件的复制请求。API 3705 可以执行认证 3718。工作节点 3605 可以从 API 3705 拉取 3719 复制请求，并且对要复制的对象文件执行 3720 数据交换约束的确定。如果允许复制对象文件，工作节点 3605 执行 3721 文件复制，以从对象存储 3706 复制对应的对象文件。无论不满足数据交换确定的结果如何，工作节点 3605 会向 API 3705 返回 3722 反馈。在允许复制对象文件的情况下，反馈包括所复制的对象

文件。在不允许复制对象文件的情况下，反馈用于指示复制请求被拒绝。

在一些实施例中，平台工作人员 3703 可以回调 3723 API 3705，从 API 3705 可以向平台工作人员 3703 返回 3724 复制请求 ID。在一些实施例中，TTP 3701 可以通过 DES 入口 3704 来查看 3725 历史对象文件复制的情况，以确认在过去一段时间内对象文件的交换是否符合数据交换约束的要求。DES 入口 3704 可以返回 3726 所要查看的结果。

针对服务调用的数据交换保护的示例实现

图 3K 示出了根据本公开的一些实施例的涉及服务调用通道的数据交换架构 3800 的示意框图。数据交换架构 3800 可以被实现在 DES 1040 中，用于针对服务调用类型的数据执行数据安全保护。在图 3L 的示例中，示出了在 TTP IDC 侧的目标平台服务 3802 与境外 IDC 侧的境外（非 TTP）平台服务 3804 之间的服务调用数据交换。例如，目标平台服务 3802 上的服务可能需要调用境外平台服务 3804 上的服务，反之，境外平台服务 3804 的服务也可能需要调用目标平台服务 3802 上的服务。

不同服务平台可能会应用多种不同的服务调用协议，例如 HTTP 协议或 Thrift RPC 协议。在本公开的一些实施例中，希望在 VPC 受信区域中执行数据主权保护时可以处理统一格式化数据，例如 HTTP 协议数据。

在图 3K 中，在控制面，非 TTP 控制面用于通道注册、通道架构更新、检测；TTP/TTP 控制面用于通道请求批准、通道禁止、通道检测等。在数据面，HTTP 负载均衡器 3810 是来自 TTP Cloud 的 L7 均衡产品，其是确保所有 DES-RPC 通道流量通过 VPC 受信区域的关键组件。HTTP 通道是 DES-RPC 通道中支持 HTTP 协议的通道。Thrift RPC 通道是 DES-RPC 通道中支持 Thrift RPC 协议的通道。在被发送到 TTP 的 HTTP 负载均衡器之前，Thrift RPC 通道将被包裹在 HTTP 通道中。

在通道注册阶段，DES-RPC 通道利用通道信息和数据定义来声明。通道信息可以包括通道的类型，例如 Thrift RPC 或 HTTP。通道信息还可以包括 RPC 调用元组。调用元组可以包括 src dc、src 服务、dst dc、dst 服务、rpc 方法/http 路径。

数据定义可以取决于数据的流动方向。对于从非 TTP 到 TTP 的数据流动，将使用具有合规注释的 Thrift IDL 来声明响应。对于从 TTP 到非 TTP 的数据流动，将使用带有合规注释的 Thrift IDL 来声明请求。在一些实施例中，在 DES-RPC 通道通过合规性注册时，DES-RPC 通道才是可用的。

可以理解，图 3K 中示出的在 DES 中用于处理服务调用数据交换的组件仅是示例。在其他示例中，取决于需要，不同功能模块还可以按其他方式被细分、合并等，并且还可以包括更多、更少或不同的功能模块。

图 3L 示出了根据本公开的一些实施例的在图 3K 所示的服务调用通道中从非 TTP 到 TTP 的数据交换示例。如图 3L 所示，由境外区域的服务 A 3901 发起的调用将由 HTTP 代理 3902 或 Thrift 代理 3903 转发到 TTP 的 HTTP 负载均衡器 3905。服务 A 3901 可以是图 3M 所示的境外平台服务的一个示例。对于 HTTP 请求，调用将由 HTTP 代理 3902 转发到 HTTP 负载均衡器 3905。对于 Thrift 请求，调用将由 Thrift 代理 3903 转发到 HTTP 负载均衡器 3905。

境外 IDC 中对应服务代理，比如说 HTTP 代理 3902 或者 Thrift 代理 3903 到 VPC 受信区域 HTTP 负载均衡器 3905 的服务发现建议通过 DNS 来实现，对应请求转发到 TTP IDC 区域的代理的服务发现则建议使用定制/通用的服务发现。

HTTP 负载均衡器 3905 可以包括合规插件 3906。对于非法的请求，合规插件 3906 将返回错误。对于 Thrift rpc 调用，请求将被 HTTP 包裹以生成新的 HTTP 请求。新的 HTTP 请求的主体为 Thrift 二进制文件。

在 VPC 受信区域中，TTP 的 HTTP 负载均衡器 3905 将请求分别转发到 TTP 的 HTTP 代理 3907 和 Thrift 代理 3908，然后 HTTP 代理 3907 和 Thrift 代理 3908 分别将请求转发到作为目标服务的服务 B 3908 和服务 C 3910。对于 Thrift rpc 调用，Thrift 代理 3908 会在发送请求之前从所生成的新的 HTTP 请求中恢复原始 Thrift 请求。

TTP 的 HTTP 代理 3907 和 Thrift 代理 3908 将在向 TTP 的 HTTP 负载均衡器 3905 发送响应之前对响应进行检查。对于未通过合规性检查的响应，将返回错误。此外，对于 Thrift rpc 调用，Thrift 响应将被 HTTP 包裹以生成新的 HTTP 响应。新的 HTTP 响应的主体为 Thrift 二进制文件。

图 3M 示出了根据本公开的一些实施例的在图 3K 所示的服务调用通道中从 TTP 到非 TTP 的数据交换示例。如图 3M 所示，由 TTP 的服务 A 3951 发起的调用将由 TTP 的 HTTP 代理 3952 和 Thrift 代理 3953 转发到 TTP 的 HTTP 负载均衡器 3955。对于 HTTP 请求，调用将由 HTTP 代理 3952 转发到 HTTP 负载均衡器 3955。对于 Thrift 请求，调用将由 Thrift 代理 3953 转发到 HTTP 负载均衡器 3955。

对于非法的请求，将返回错误。对于未通过合规性检查的响应，将返回错误。对于 Thrift rpc 调用，请求将被 HTTP 包裹以生成新的 HTTP 请求。新的 HTTP 请求的主体为 Thrift 二进制文件。

TTP 的 HTTP 负载均衡器 3955 将请求转发到非 TTP（也即，境外区域）的 HTTP 代理 3957 和 Thrift 代理 3958。然后 HTTP 代理 3957 和 Thrift 代理 3958 将请求转发到境外区域的服务 B 3959 和服务 C 3960。

对于 Thrift rpc 调用，Thrift 代理会在发送之前从所生成的新的 HTTP 请求中恢复原始 Thrift 请求。

非 TTP 的 HTTP 代理 3957 和 Thrift 代理 3958 将向 TTP 的 HTTP 负载均衡器 3955 发送响应。对于 Thrift rpc 调用，Thrift 响应将被 HTTP 包裹以生成新的 HTTP 响应。新的 HTTP 响应的主体为 Thrift 二进制文件。

安全沙盒子系统

客户端应用需要与服务器通信以传输数据。客户端应用的网络流量可以传输大量的用户数据。因此，需要一种能够管理客户端应用的网络流量的方法，以使得用户数据不会经由客户端应用的网络流量被传输到未经允许的服务器。例如，在数据主权保护的场景下，该方法可以防止用户数据被传输到非数据主权国家的服务器。

然而，客户端应用的网络流量的类型十分丰富。客户端应用可以包括移动端应用和电脑（PC 端）应用。客户端应用的网络流量可以包括原生类型的网络流量和网页视图类型的网络流量等。此外，客户端应用的网络流量并非都在应用的所有者的管理和控制之下。例如，客户端应用的网络流量可以包括来自第三方广告商的网络流量。因此，管理客户端应用的各种类型的网络流量是十分困难的。

本公开的示例实施例提出了一种管理客户端应用的网络流量的方法。该方法包括：基于对目标用户的确定，检测目标用户的用户数据从客户端应用到服务器的网络传输；基于网络

传输对应的网络流量的类型，在网络传输的不同层分析网络流量；以及基于分析指示网络流量满足与目标用户对应的数据交换约束，将网络流量发送到由数据交换约束限定的服务器。

以此方式，通过基于网络流量的类型在网络传输的不同层分析网络流量以及限制不满足数据交换约束的网络流量的传输，可以有效地防止用户数据经由各种类型的网络流量传输到未经允许的服务器。

以下将参照附图来具体描述本公开的实施例。下文将以移动端应用为例来示例性地说明本公开的方案。

图 4A 示出了根据本公开的一些实施例的管理移动端应用的网络流量的示例方法 4100 的流程图。该方法 4100 例如可以在图 1 的安全沙盒子系统 1090 处实施。移动端应用可以是移动端的目标应用 1080。

在框 4102，基于对目标用户的确定，检测目标用户的用户数据从目标应用 1080 到服务器的网络传输。换言之，如果确定当前用户是目标用户，则安全沙盒子系统 1090 可以检测目标用户的用户数据的网络传输。

在一些实现中，可以基于对目标用户的确定将网络流量路由到安全沙盒子系统 1090，以使得安全沙盒子系统 1090 可以检测和分析与用户数据的网络传输对应的网络流量。安全沙盒子系统 1090 可以分析目标应用 1080 的网络请求并且基于数据交换约束来限制不满足条件的网络请求。

数据交换约束可以包括与数据主权有关的交换约束，例如数据主权保护规则。数据主权保护规则可以根据各个国家或区域的规定而被确定。数据主权保护规则也可以由应用的运营方确定（例如，与用户数据使用协议有关）。

数据主权保护规则可以基于具体场景而被设置。例如，数据主权保护规则可以规定不允许数据主权国家的用户数据传输到数据主权国家之外的任何服务器。在另一些实现中，数据主权保护规则可以规定不允许数据主权国家的隐私的用户数据传输到未经注册的任何服务器。本公开的范围对此不作限制。

如图 1 所示，目标应用 1080 的网络请求经由安全沙盒子系统 1090 的分析和处理之后被传输到应用防火墙子系统 1020。安全沙盒子系统 1090 的原理和细节将在下文详细描述。

目标用户是指其用户数据的传输需要被检测和管理的用户。目标用户可以是具有数据主权国家的国籍的用户。备选地或附加地，目标用户也可以是根据数据主权保护的具体规则而确定的用户。例如，目标用户可以是具有数据主权国家的国籍并且当前在地理上位于该数据主权国家中的用户。

在一些实现中，可以基于用户信息来确定目标用户。用户信息可以包括用户的账号信息、个人信息、注册信息等。备选地或附加地，可以基于设备信息来确定目标用户。设备信息可以包括用户身份识别模块 (Subscriber Identity Module，SIM)信息、IP 地址、网络服务提供商信息、设备的系统设置信息、应用设置信息等。

在一些实现中，可以基于多种信息的组合来确定目标用户。多种信息可以具有不同的优先级。例如，SIM 信息、网络服务提供商信息的优先级可以高于 IP 地址、系统设置信息、应用设置信息等。

在一些实现中，对目标用户的确定可以基于对目标用户所在地区的确定。可以利用上述用户信息或设备信息来确定目标用户的所在地区，从而确定目标用户。例如，可以利用智能手机的系统设置中的地区设置来确定当前用户所在地区，并以此确定当前用户是否为目标用

户。又例如，可以利用 SIM 卡的国家代码来确定目标用户所在地区，并以此来确定目标用户。

在一些实现中，可以在初次启动应用时确定目标用户。换言之，可以在初次启动应用时确定当前用户是否是目标用户。备选地或附加地，可以在用户注册时确定当前用户是否是目标用户。备选地或附加地，可以在用户登入、登出、切换账号时确定当前用户是否是目标用户。

在一些实现中，可以将确定结果存储在本地或服务器中。可以在第一次将用户确定为目标用户之后存储确定结果并且设置在阈值时间段内使用所存储的确定结果。这样，当用户再次登录时，可以无需再次对用户进行确定。

在框 4104，基于网络传输对应的网络流量的类型，在网络传输的不同层分析网络流量。目标应用 1080 中的网络流量可以包括多个类型的网络流量，例如原生（native）、网页视图（Webview）和第三方软件开发工具包（SDK）类型的网络流量。原生类型的网络流量由业务层中的操作系统（例如，安卓和 IOS）代码产生和处理。原生类型的网络流量可以完全由目标应用 1080 的所有者来控制。

第三方 SDK 类型的网络流量由第三方 SDK 产生和处理。通常，目标应用 1080 中可以接入第三方 SDK 以用于实现登录或分享的功能。第三方 SDK 类型的网络流量由这些第三方 SDK 产生和处理。应理解，第三方 SDK 类型的网络流量通常不能完全由应用的所有者来控制。

网页视图类型的网络流量可以包括由应用的所有者控制的网络流量，例如，应用内置的浏览器通过调用原生应用的代码而产生的网络流量。网页视图类型的网络流量还可以包括由第三方控制的网络流量。例如，由第三方广告商产生和控制的网络流量。

基于网络流量的类型，安全沙盒子系统 1090 可以采取相应的分析策略，从而更好地管理应用中的用户数据的网络传输。

在框 4106，基于分析指示网络流量满足与目标用户对应的数据交换约束，将网络流量发送到由数据交换约束限定的服务器。可以针对不同的目标用户设置不同的数据交换约束。例如，对于敏感等级更高的目标用户，可以设置更严格的数据交换约束。数据交换约束可以限定哪些用户数据可以被传输到哪些服务器。在一些实现中，可以基于目标用户的用户信息或对应的设备信息来确定目标用户对应的数据交换约束。

在一些实现中，安全沙盒子系统 1090 可以包括针对不同类型的网络流量的多个子模块。例如，用于管理原生类型的网络流量的子模块、用于管理网页视图类型的网络流量的子模块、以及用于管理第三方 SDK 类型的网络流量的子模块。这些子模块可以分析相应类型的网络流量，以及限制或拦截不满足数据交换约束的网络流量。下文将参考图 4B 至图 4E 来详细描述针对不同类型的网络流量的管理的细节。

图 4B 示出了根据本公开的一些实施例的针对原生类型的网络流量的分析和限制过程 4200 的示意图。图 4B 示出了用于分析和限制原生类型的网络流量的子模块 4210。子模块 4210 可以是安全沙盒子系统 1090 的一部分，也可以是安全沙盒子系统 1090 的一种具体实现方式。

如图 4B 所示，业务逻辑层 4220 将网络请求下发给底层 OS 4230。业务逻辑层 4220 可以是图 1 所示的应用业务逻辑 1100 在网络传输方面的一种具体实现。子模块 4210 可以作为拦截器在网络层分析和限制网络请求。子模块 4210 可以通过分析端点、网络请求的参数、或模式（schema）来限制网络请求。例如，可以基于 schema 是否已被注册来确定是否限制该网络请求。备选地或附加地，可以基于网络请求中所请求的字段是否涉及敏感信息来确定是否限制该网络请求。

在一些实现中，子模块 4210 可以包括针对安卓的拦截器、针对 IOS 的拦截器。附加地，子模块 4210 还可以包括针对 C++的拦截器。以此方式，通过在网络层分析和限制网络请求，可以基于网络请求的协议信息来更好地判断该网络请求是否应该被限制。

图 4C 示出了根据本公开的一些实施例的针对网页视图类型的网络流量的分析和限制过程 4300 的示意图。图 4C 示出了用于分析和限制网页视图类型的网络流量的子模块 4310。子模块 4310 可以是安全沙盒子系统 1090 的一部分，也可以是安全沙盒子系统 1090 的一种具体实现方式。

子模块 4310 可以将网页视图类型的网络流量转移到原生的网络接口，以使得网页视图类型的网络流量可以由针对原生类型的网络流量的子模块 4210 来分析和限制。在一些实现中，子模块 4310 可以利用 JavaScript（JS）的钩子（hook）机制来将网页视图类型的网络流量转移到原生的网络接口。

如图 4C 所示，子模块 4310 可以包括启动器 4311、导航 URL 拦截器 4312 和内部请求拦截器 4313。子模块 4310 可以与应用内置的浏览器 4320 通信，以使得网页视图类型的网络流量可以被子模块 4310 管理和检测。启动器 4311 可以在应用内置的浏览器 4320 打开(被创建)时进行 JS 注入，以使得网页视图类型的网络流量可以利用 hook 机制被转移到原生的网络接口。被转移到原生的网络接口的网络流量可以由原生的网络模块接管。

在一些实现中，可以使用如下方式来利用 JS hook 技术进行网络流量的转移。

导航 URL 拦截器 4312 可以分析和限制主页面（初始页面）的 URL。例如，导航 URL 拦截器 4312 可以基于 URL 的 schema 是否被注册来确定是否限制该网络请求。如果该网络请求未被限制，则浏览器 4320 可以加载该主页面。

内部请求拦截器 4313 可以将与主页面的静态资源和动态资源有关的网络流量转接到原生的网络接口，以使得这些网络流量可以由子模块 4210 来在网络层进行限制和分析。具体的分析和限制过程与原生类型的网络流量类似，在此不再赘述。

在一些实现中，针对由应用的所有者控制的网页视图类型的网络流量和由第三方控制的网页视图类型的网络流量，子模块 4310 可以采取不同的分析和限制策略。例如，针对由第三方控制的网页视图类型的网络流量，可以仅利用导航 URL 拦截器 4312 来确定主页面的 URL 是否被注册来分析相关的网络流量，而无需进一步分析主页面的静态资源和动态资源。

图 4D 示出了根据本公开的一些实施例的针对第三方 SDK 类型的网络流量的分析和限制过程 4400 的示意图。图 4D 示出了用于分析和限制第三方 SDK 类型的网络流量的子模块 4410。子模块 4410 可以是安全沙盒子系统 1090 的一部分，也可以是安全沙盒子系统 1090 的一种具体实现方式。

子模块 4410 可以在应用程序接口（API）层分析和限制第三方 SDK 类型的网络流量。子模块 4410 可以通过在 API 层分析第三方 SDK 的 API 所请求的数据是否满足数据交换约束来限制第三方 SDK 类型的网络流量。

在一些实现中，子模块 4410 可以包裹（wrap）第三方 SDK 中请求用户数据的 API，并且在包裹中添加基于数据交换约束的判断逻辑。换言之，子模块 4410 可以通过向第三方 SDK 的 API 添加判断逻辑来确定包裹 API。这样，业务逻辑层 4220 不是直接调用第三方 SDK 的 API，而是调用添加了判断逻辑的包裹 API。

如图 4D 所示，子模块 4410 可以包括分别针对每个第三方 SDK 的包裹模块。例如，针对 SDK 4411 的包裹模块 4412、针对 SDK 4413 的包裹模块 4414、以及针对 SDK 4415 的包

裹模块 4416。包裹模块（例如，包裹模块 4412）可以包裹对应的 SDK（例如，SDK 4411）中的 API，以生成对应的包裹 API。在一些实现中，子模块 4410 可以动态地增加包裹模块以包裹第三方 SDK 的 API。

在一些实现中，可以通过如下方式来包裹第三方 SDK 的 API。包裹模块 4412 可以定义暴露给业务层的、与 SDK 4411 中的 API 相同的 API。包裹模块 4412 可以实现该 API 并且定义 SDK 4411 数据类型的包裹类。

判断逻辑可以基于数据交换约束来确定是否可以调用被包裹的第三方 SDK 的 API。在一些实现中，判断逻辑可以基于 SDK 的名称、API 的名称、API 的参数的名称等来分析第三方 SDK 的 API 是否可以被调用。如果判断结果为是，则第三方 SDK 的 API 可以被调用，并向业务层返回值。如果判断结果为否，则不调用第三方 SDK 的 API，也即，与该 API 相关的网络流量被限制。应理解，判断逻辑可以基于具体场景而变化。例如，判断逻辑可以设置为不允许向第三方 SDK 传入用户的隐私数据。

以此方式，通过在 API 层进行分析和限制，子模块 4410 可以在无需知晓第三方 SDK 的内部代码的情况下管理和检测第三方 SDK 类型的网络流量。

图 4E 示出了根据本公开的一些实施例的安全沙盒子系统 1090 的模块图。如图 4E 所示，安全沙盒子系统 1090 包括启动模块 4520。启动模块 4520 被配置为基于对目标用户的确定，启动对目标用户的用户数据从客户端应用到服务器的网络传输的检测。启动模块 4520 可以激活管理模块来检测、管理、分析和限制与用户数据的网络传输对应的网络流量。

管理模块被配置为基于网络传输对应的网络流量的类型，在网络传输的不同层分析网络流量；以及基于分析指示网络流量满足与目标用户对应的数据交换约束，将网络流量发送到由数据交换约束限定的服务器。

在一些实现中，管理模块可以包括子模块（也称为第一管理模块）4210、子模块（也称为第二管理模块）4310 和子模块（也称为第三管理模块）4410。子模块 4210、子模块 4310 和子模块 4410 可以分析和限制客户端应用的网络流量。

在一些实现中，子模块 4210 被配置为基于网络流量的类型为原生类型的网络流量，在网络层分析网络流量。

在一些实现中，子模块 4310 被配置为基于网络流量的类型为网页视图类型的网络流量，将网页视图类型的网络流量转移到客户端应用的网络接口以由客户端应用的原生网络模块管理；以及在网络层分析所转移的网络流量。

在一些实现中，将网页视图类型的网络流量转移到移动端应用的网络接口包括：利用 JavaScript 的钩子机制来转移网页视图类型的网络流量。

在一些实现中，子模块 4410 被配置为基于网络流量的类型为第三方 SDK 类型的网络流量，在应用程序接口 API 层分析网络流量。

在一些实现中，在 API 层分析所述网络流量包括：通过向第三方 SDK 的 API 添加基于所述数据交换约束的判断逻辑来确定包裹 API；以及调用所述包裹 API 以利用所述判断逻辑来分析所述网络流量。

在一些实现中，启动模块 4520 可以基于对目标用户的确定来激活子模块 4210、4310 和 4410。例如，启动模块 4520 可以在用户注册时确定当前用户是否是目标用户。如果确定结果为是，则启动模块 4520 可以激活子模块 4210、4310 和 4410。又例如，启动模块 4520 可以在用户登录时从本地或服务器获取对该用户的确定结果，并基于确定结果来确定是否激活子

模块 4210、4310 和 4410。

安全沙盒子系统 1090 中还可以包括用于对网络流量进行采样的采样模块 4510。在一些实现中，采样模块 4510 可以向启动模块 4520 发送采样信号来触发启动模块 4520。采样信号可以指示对网络流量进行采样的采样率。

采样模块 4510 可以基于数据交换约束来采样目标用户和不同类型的网络流量。例如，采样模块 4510 可以以不同的采样率来对不同类型的网络流量进行采样。利用采样模块 4510，可以仅分析网络流量中的一部分，从而降低开销并维持应用的稳定性。

应理解，安全沙盒子系统 1090 还可以包括其他模块，或者仅包括图 4E 所示的部分模块。例如，在目标应用 1080 仅是移动端的原生应用时，安全沙盒子系统 1090 可以不包括针对网页视图类型的网络流量的子模块 4310。本公开的范围对此不作限制。

在一些实现中，基于网络流量的类型，还可以在套接字（Socket）层来分析和限制网络流量。例如，可以在 Socket 层转接第三方 SDK 类型的网络流量，以使得可以直接分析第三方 SDK 类型的网络请求。备选地或附加地，也可以在 Scoket 层分析和限制原生类型的网络流量以及网页视图类型的网络流量。

在一些实现中，还可以在目标应用 1080 上建立作为代理的本地服务器。通过将目标应用 1080 的网络请求转发给本地服务器，并且通过在本地服务器分析和限制网络流量，可以管理由本地服务器转发给外部服务器的网络请求。以此方式，可以在考虑协议信息的情况下分析和限制不同类型的网络流量，从而更好地管理应用的网络流量不被传输到未经允许的外部服务器。

上文参考图 4B 至图 4E 详细描述了针对不同类型的网络流量的分析和限制的原理和细节。应理解，上述限制规则、判断逻辑和数据交换约束仅是示例性的，而非限制本公开的范围。例如，根据不同国家的法律法规要求可以设置不同的数据主权保护规则。此外，取决于计算机网络的层的定义，可以在与上述层相近或相似的层处来分析和限制网络流量。

此外，在上文的描述中，安全沙盒子系统 1090 可以直接分析和限制目标应用 1080 中的网络流量。换言之，只有未被安全沙盒子系统 1090 限制的网络流量才能继续传输。备选地或附加地，安全沙盒子系统 1090 可以不直接限制网络流量，而是仅提供分析报告。在这种情况下，可以在正常传输网络请求的同时向安全沙盒子系统 1090 发送网络请求的副本。安全沙盒子系统 1090 可以分析网络请求的副本，并提供分析报告。

在一些实现中，针对多个数据主权国家的情况，可以相应地设置多个安全沙盒子系统 1090 来分别针对每个数据主权国家进行处理。例如，可以基于对目标用户所在地区的确定，启动对应的安全沙盒子系统来分析和限制网络流量，以使得应用中的用户数据的网络传输符合对应国家的数据主权保护规则。

推荐管理子系统

如上文所讨论的，目标应用例如可以通过推荐机制来向用户提供各种内容的推荐，诸如，多媒体内容推荐、用户推荐、商品推荐等等。在这样的应用中，推荐策略的公平性已经成为许多地区管理的重点。例如，一些应用可能通过推荐机制来引导用户去关注与用户习惯无关的特定内容，则这样的推荐机制可能是不合规的。

另一方面，通常的推荐算法往往依赖于机器学习模型来实施，诸如由安全计算子系统 1060 所执行的代码层级核查可能无法有效地检测推荐算法的公平性。而另一方面，推荐模型的训

练与更新往往与实际用户数据息息相关，人们也不期望在检查过程中暴露用户的隐私数据，因为这可能会导致数据合规的风险。

本公开的实施例进一步提出了一种管理推荐策略的方案。图 5 示出了管理推荐策略的过程 500 的流程图。该过程 500 例如可以由推荐管理子系统 1050 执行。

如图 5 所示，在框 502，推荐管理子系统 1050 获取与目标应用中的一组对象相关联的一组对象特征，其中一组对象特征是基于一组对象的属性而转换得到的，一组对象特征不直接表达一组对象的属性。

在一些实施例中，推荐管理子系统 1050 可以经由目标应用提供的应用程序接口 API 来获取该组对象特征。在一些实施例中，推荐管理子系统 1050 例如可以经由专用 API 而从目标应用平台 1030 来获取与目标应用 1080 中的一组对象相关联的一组对象特征。

在一些实施例中，该组对象特征例如可以是由特征提取模型基于该组对象的属性而转换得到的。基于这样的方式，可以使得推荐策略的管理方或者其他第三方无法基于对象特征来确定对象的原始属性信息。由此，可以保证目标应用中的数据的安全性。

在框 504，推荐管理子系统 1050 从一组对象特征中确定第一对象特征和第二对象特征，其中第一对象特征和第二对象特征之间的第一差异小于第一阈值。

在一些实施例中，该组对象特征例如可以表示为多个向量。进一步地，推荐管理子系统 1050 例如可以基于向量之间的差异，而从该组对象特征中选择出差异小于第一阈值的至少一对对象特征。

在框 506，推荐管理子系统 1050 基于目标应用中的推荐策略，确定与第一对象特征对应的第一推荐结果和与第二对象特征对应的第二推荐结果。

在一些实施例中，推荐管理子系统 1050 可以将第一对象特征提供至与推荐策略相关联的推荐模型，以确定第一推荐结果，并且将第二对象特征提供至推荐模型，以确定第二推荐结果。

在一些实施例中，为了保证推荐策略的安全性，可以由推荐管理子系统 1050 经由目标应用提供的 API 而将所选择得到的第一对象特征和第二对象特征发送至远程运行的推荐模型，以用于确定第一推荐结果和第二推荐结果。示例性地，该推荐模型例如可以是由目标应用的维护方所运行的。

在一些实施例中，生成第一推荐结果和第二推荐结果的过程将不会影响目标应用中真正部署的推荐模型。

在一些实施例中，第一推荐结果和第二推荐结果可以是由推荐模型输出的向量表示。由此，推荐管理子系统 1050 将无法直接解读第一推荐结果和第二推荐结果的语义，从而进一步提高了目标应用内数据的安全性。

在框 508，推荐管理子系统 1050 基于第一推荐结果和第二推荐结果，评估推荐策略。

在一些实施例中，推荐管理子系统 1050 可以确定第一推荐结果和第二推荐结果之间的第二差异，并且基于第二差异与第二阈值之间的比较，确定推荐策略的公平性。

具体地，对于合理的推荐策略而言，对于两个相似的对象，其推荐结果应当是相似的。因此，如果推荐管理子系统 1050 确定第二差异超过第二阈值时，可以确定推荐策略具有较差的公平性。

或者，推荐管理子系统 1050 例如也可以基于第二差异超过第二阈值的对象特征对的占比，来确定推荐策略的公平性。例如，推荐管理子系统 1050 例如可以随机采样多组对象特征对，

并如果其中第二差异超过第二阈值的对象特征对的占比超过阈值占比，则可以确定推荐策略具有较差的公平性。

在一些实施例中，推荐管理子系统 1050 还可以基于用于输入到推荐模型的对象特征和历史推荐结果之间的相关性，来确定推荐策略的公平性。具体地，推荐管理子系统 1050 还可以从目标应用获取第三对象特征和针对第三对象特征的历史推荐结果。进一步地，推荐管理子系统 1050 基于第三对象特征和历史推荐结果之间的相关性，确定推荐策略的公平性。例如，推荐管理子系统 1050 可以基于确定对象特征与历史推荐结果的类别信息是否匹配。

在一些实施例，推荐管理子系统 1050 可以确定与第三对象特征和历史推荐结果对应的向量表示，并基于两个向量表示之间的差异来确定第三对象特征和历史推荐结果之间的相关性。例如，如果一个对象和其历史推荐结果的向量差异大于阈值，则推荐管理子系统 1050 可以确定推荐策略具有较差的公平性。

在一些实施例中，如上文所提及的，还可以由安全计算子系统 1060 例如对于推荐策略相关联的源代码进行检查。具体地，安全计算子系统 1060 例如可以获取与推荐策略相对应的源代码，并且基于源代码或与源代码对应的中间代码来评估推荐策略。

在一些实施例中，推荐策略例如可以用于向目标应用 1080 中的用户推荐至少一项多媒体内容。多媒体内容的示例例如可以包括：图像、视频、音乐或其组合等。

示例装置和设备

本公开的实施例还提供了用于实现上述方法或过程的相应装置。图 6 示出了根据本公开的一些实施例的用于数据交换的装置 600 的示例框图。

如图 6 所示，装置 600 包括获取模块 610，被配置为获取目标应用要在第一平台与第二平台之间交换的原始数据。装置 600 还包括预处理模块 620，被配置为基于原始数据的类型来处理原始数据，以获得类型对应的统一格式化数据。装置 600 还包括约束满足确定模块 630，被配置为从统一格式化数据确定对数据交换约束的满足。

在一些实施例中，所述第一平台为特定国家或地区管辖的目标应用平台，第二平台为其他国家或地区管辖的目标应用平台。

在一些实施例中，装置 600 还包括：转换模块，被配置为如果确定统一格式化数据满足数据交换约束，将统一格式化数据转换为原始数据。交互执行模块，被配置为执行原始数据在第一平台与第二平台之间的交换。

在一些实施例中，原始数据的类型选自包括以下类型的组：消息队列（MQ）类型，离线聚合数据类型，目标对象存储（TOS）类型，和服务调用类型。

在一些实施例中，预处理模块 620 被配置为：检测原始数据的格式，数据的类型包括多个格式；以及通过格式转换将原始数据的格式转换为多个数据格式中的指定格式，以获得统一格式化数据。

在一些实施例中，在第一平台与第二平台之间创建与多个类型的原始数据分别对应的多个数据通道。在一些实施例中，预处理模块 620 被配置为：基于原始数据的类型，从多个数据通道中选择与类型对应的数据通道；以及将原始数据提供到所选择的数据通道进行处理。

在一些实施例中，数据交换约束包括与原始数据的类型相关联的特定类型的数据交换约束，特定类型的数据交换约束被注册在所选择的数据通道中。在一些实施例中，约束满足确定模块 630 被配置为在所选择的数据通道中，从统一格式化数据确定特定类型的数据交换约

束的满足。

在一些实施例中，装置 600 还包括：通道创建模块，被配置为如果要在第一平台与第二平台之间交换的新类型的原始数据，在第一平台与第二平台之间创建与新类型的原始数据对应的另一数据通道，以及约束注册模块，被配置为在另一数据通道中注册与新类型相关联的特定类型的数据交换约束。

在一些实施例中，预处理模块 620 被实现在第一数据中心中执行，约束满足确定模块 630 被实现在第二数据中心中执行，并且转换模块被实现在第三数据中心。在一些实施例中，第一数据中心与第三数据中心不具有直接通信连接，并且第一数据中心和第二数据中心分别与第二数据中心具有直接通信连接。

在一些实施例中，第一数据中心、第二数据中心和第三数据中心分别由虚拟私有数据中心（VPC）来实现。

图 7 示出了可以用来实施本公开内容的实施例的示例设备 700 的示意性框图。例如，根据本公开实施例的系统 100 和/或系统 400 可以由设备 700 来实施。如图所示，设备 700 包括中央处理单元（CPU）701，其可以根据存储在只读存储器（ROM）702 中的计算机程序指令或者从存储单元 708 加载到随机访问存储器（RAM）703 中的计算机程序指令，来执行各种适当的动作和处理。在 RAM 703 中，还可存储设备 700 操作所需的各种程序和数据。CPU 701、ROM 702 以及 RAM 703 通过总线 704 彼此相连。输入/输出（I/O）接口 705 也连接至总线 704。

设备 700 中的多个部件连接至 I/O 接口 705，包括：输入单元 706，例如键盘、鼠标等；输出单元 707，例如各种类型的显示器、扬声器等；存储单元 708，例如磁盘、光盘等；以及通信单元 709，例如网卡、调制解调器、无线通信收发机等。通信单元 709 允许设备 700 通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

上文所描述的各个过程和处理，例如过程 500，可由处理单元 701 执行。例如，在一些实施例中，过程 500 可被实现为计算机软件程序，其被有形地包含于机器可读介质，例如存储单元 708。在一些实施例中，计算机程序的部分或者全部可以经由 ROM 702 和/或通信单元 709 而被载入和/或安装到设备 700 上。当计算机程序被加载到 RAM 703 并由 CPU 701 执行时，可以执行上文描述的过程 500 的一个或多个动作。

本公开可以是方法、装置、系统和/或计算机程序产品。计算机程序产品可以包括计算机可读存储介质，其上载有用于执行本公开的各个方面的计算机可读程序指令。

计算机可读存储介质可以是可以保持和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质例如可以是但不限于电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或者上述的任意合适的组合。计算机可读存储介质的更具体的例子（非穷举的列表）包括：便携式计算机盘、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）、静态随机存取存储器（SRAM）、便携式压缩盘只读存储器（CD-ROM）、数字多功能盘（DVD）、记忆棒、软盘、机械编码设备、例如其上存储有指令的打孔卡或凹槽内凸起结构、以及上述的任意合适的组合。这里所使用的计算机可读存储介质不被解释为瞬时信号本身，诸如无线电波或者其他自由传播的电磁波、通过波导或其他传输媒介传播的电磁波（例如，通过光纤电缆的光脉冲）、或者通过电线传输的电信号。

这里所描述的计算机可读程序指令可以从计算机可读存储介质下载到各个计算/处理设

备，或者通过网络、例如因特网、局域网、广域网和/或无线网下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光纤传输、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配卡或者网络接口从网络接收计算机可读程序指令，并转发该计算机可读程序指令，以供存储在各个计算/处理设备中的计算机可读存储介质中。

用于执行本公开操作的计算机程序指令可以是汇编指令、指令集架构（ISA）指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、或者以一种或多种编程语言的任意组合编写的源代码或目标代码，所述编程语言包括面向对象的编程语言—诸如 Smalltalk、C++等，以及常规的过程式编程语言—诸如“C”语言或类似的编程语言。计算机可读程序指令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）。在一些实施例中，通过利用计算机可读程序指令的状态信息来个性化定制电子电路，例如可编程逻辑电路、现场可编程门阵列（FPGA）或可编程逻辑阵列（PLA），该电子电路可以执行计算机可读程序指令，从而实现本公开的各个方面。

这里参照根据本公开实施例的方法、装置（系统）和计算机程序产品的流程图和/或框图描述了本公开的各个方面。应当理解，流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合，都可以由计算机可读程序指令实现。

这些计算机可读程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理单元，从而生产出一种机器，使得这些指令在通过计算机或其它可编程数据处理装置的处理单元执行时，产生了实现流程图和/或框图中的一个或多个方框中规定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中，这些指令使得计算机、可编程数据处理装置和/或其他设备以特定方式工作，从而，存储有指令的计算机可读介质则包括一个制造品，其包括实现流程图和/或框图中的一个或多个方框中规定的功能/动作的各个方面的指令。

也可以把计算机可读程序指令加载到计算机、其它可编程数据处理装置、或其它设备上，使得在计算机、其它可编程数据处理装置或其它设备上执行一系列操作步骤，以产生计算机实现的过程，从而使得在计算机、其它可编程数据处理装置、或其它设备上执行的指令实现流程图和/或框图中的一个或多个方框中规定的功能/动作。

附图中的流程图和框图显示了根据本公开的多个实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或指令的一部分，所述模块、程序段或指令的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

以上已经描述了本公开的各实施方式，上述说明是示例性的，并非穷尽性的，并且也不限于所披露的各实施方式。在不偏离所说明的各实施方式的范围和精神的情况下，对于本技

术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择，旨在最好地解释各实施方式的原理、实际应用或对市场中的技术的改进，或者使本技术领域的其他普通技术人员能理解本文披露的各实施方式。

权利要求书

1. 一种数据交换方法，包括:

获取目标应用要在第一平台与第二平台之间交换的原始数据;

基于所述原始数据的类型来处理所述原始数据，以获得所述类型对应的统一格式化数据;以及

从所述统一格式化数据确定对数据交换约束的满足。

2. 根据权利要求 1 所述的方法，其中所述第一平台为特定国家或地区管辖的目标应用平台，所述第二平台为其他国家或地区管辖的目标应用平台。

3. 根据权利要求 1 所述的方法，还包括:

如果确定所述统一格式化数据满足所述数据交换约束，将所述统一格式化数据转换为所述原始数据；以及

执行所述原始数据在所述第一平台与所述第二平台之间的交换。

4. 根据权利要求 1 所述的方法，其中所述原始数据的类型选自包括以下类型的组：消息队列（MQ）类型，离线聚合数据类型，目标对象存储（TOS）类型，和服务调用类型。

5. 根据权利要求 1 所述的方法，其中处理所述原始数据包括:

检测所述原始数据的格式，所述数据的类型包括多个格式；以及

通过格式转换将所述原始数据的格式转换为所述多个数据格式中的指定格式，以获得所述统一格式化数据。

6. 根据权利要求 1 所述的方法，其中在所述第一平台与所述第二平台之间创建与多个类型的原始数据分别对应的多个数据通道，并且处理所述原始数据包括:

基于所述原始数据的类型，从所述多个数据通道中选择与所述类型对应的数据通道；以及

将所述原始数据提供到所选择的数据通道进行处理。

7. 根据权利要求 6 所述的方法，其中所述数据交换约束包括与所述原始数据的类型相关联的特定类型的数据交换约束，所述特定类型的数据交换约束被注册在所选择的所述数据通道中，并且

其中确定对数据交换约束的满足包括:

在所选择的数据通道中，从所述统一格式化数据确定所述特定类型的数据交换约束的满足。

8. 根据权利要求 6 所述的方法，还包括:

如果要在所述第一平台与所述第二平台之间交换新类型的原始数据，在所述第一平台与所述第二平台之间创建与所述新类型的原始数据对应的另一数据通道；以及

在所述另一数据通道中注册与所述新类型相关联的特定类型的数据交换约束。

9. 根据权利要求 3 所述的方法，其中所述原始数据的所述处理在第一数据中心中执行，所述数据交换约束的满足的确定在第二数据中心中执行，并且所述统一格式化数据到所述原始数据的所述转换在第三数据中心，

其中所述第一数据中心与所述第三数据中心不具有直接通信连接，并且所述第一数据中心和所述第二数据中心分别与所述第二数据中心具有直接通信连接。

10. 根据权利要求 9 所述的方法，其中所述第一数据中心、所述第二数据中心和所述第

三数据中心分别由虚拟私有数据中心（VPC）来实现。

11. 一种数据交换系统，包括:

第一数据中心，被配置为获取要在目标应用第一平台与所述目标应用的外部第二平台之间交换的原始数据，并且基于所述原始数据的类型来处理所述原始数据，以获得所述类型对应的统一格式化数据；以及

第二数据中心，被配置为从所述第一数据中心获取所述统一格式化数据，并且基于所述统一格式化数据确定对数据交换约束的满足。

12. 根据权利要求 11 所述的数据交换系统，还包括第三数据中心，

其中如果所述第二数据中心确定所述统一格式化数据满足所述数据交换约束，将所述统一格式化数据提供给所述第三数据中心，

其中所述第三数据中心被配置为将所述统一格式化数据转换为所述原始数据；以及执行所述原始数据在所述第一平台与所述第二平台之间的交换。

13. 根据权利要求 12 所述的数据交换系统，其中所述第一数据中心与所述第三数据中心不具有直接通信连接，并且所述第一数据中心和所述第二数据中心分别与所述第二数据中心具有直接通信连接。

14. 根据权利要求 12 所述的数据交换系统，其中所述第一数据中心、所述第二数据中心和所述第三数据中心分别由虚拟私有数据中心（VPC）来实现。

15. 根据权利要求 11 至 14 中任一项所述的数据交换系统，其中所述数据交换系统被划分为与数据的多个类型分别对应的多个数据通道，在每个数据通道中执行相应类型的数据的交换。

16. 一种用于数据交换的装置，包括:

获取模块，被配置为获取目标应用要在第一平台与第二平台之间交换的原始数据;

预处理模块，被配置为基于所述原始数据的类型来处理所述原始数据，以获得所述类型对应的统一格式化数据；以及

约束满足确定模块，被配置为从所述统一格式化数据确定对数据交换约束的满足。

17. 一种电子设备，包括:

存储器和处理器;

其中所述存储器用于存储一条或多条计算机指令，其中所述一条或多条计算机指令被所述处理器执行以实现根据权利要求 1 至 10 中任一项所述的方法。

18. 一种计算机可读存储介质，其上存储有一条或多条计算机指令，其中所述一条或多条计算机指令被处理器执行以实现根据权利要求 1 至 10 中任一项所述的方法。

19. 一种计算机程序产品，包括一条或多条计算机指令，其中所述一条或多条计算机指令被处理器执行以实现根据权利要求 1 至 10 中任一项所述的方法。

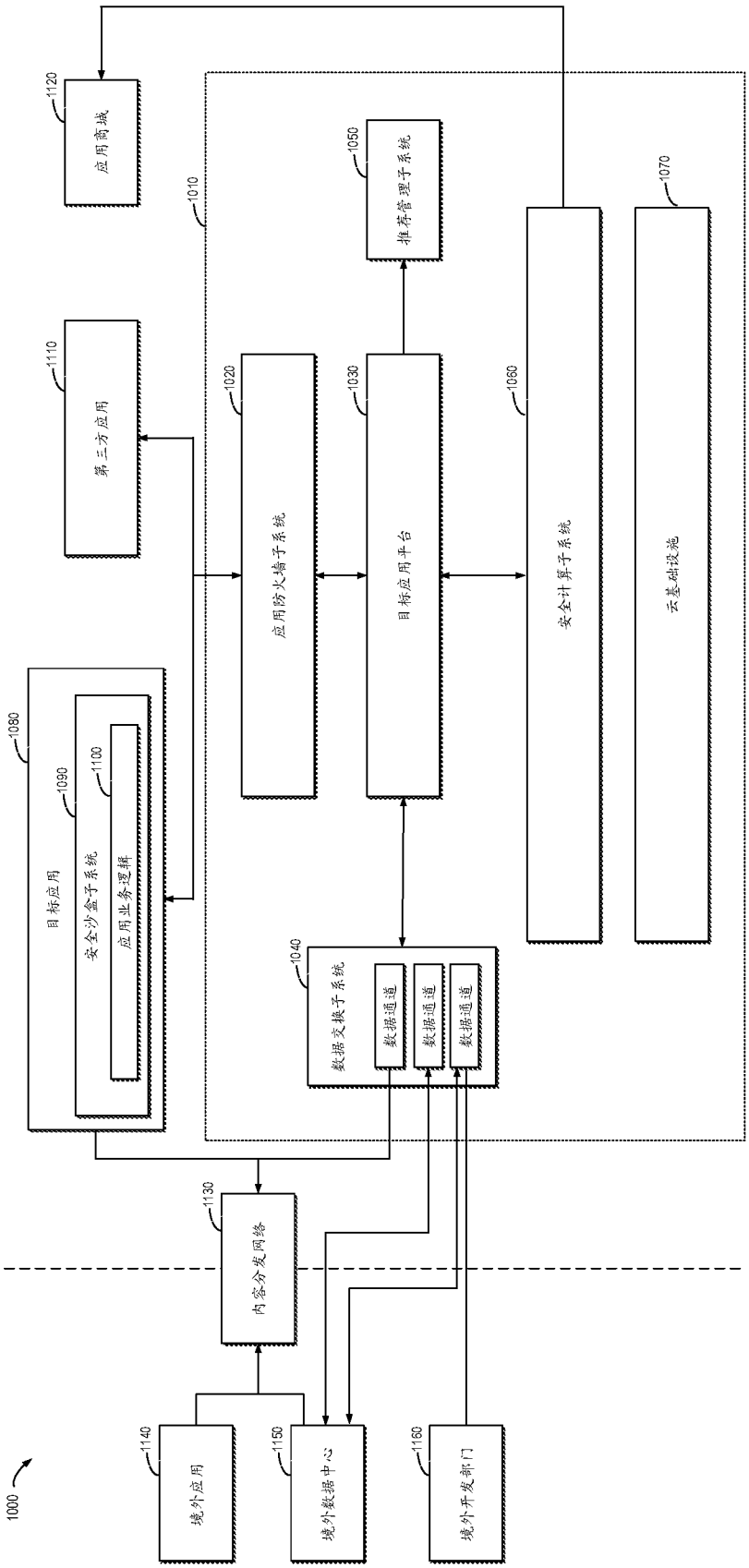
1000
1010
1020
1030
1040
1050
1060
1070
1080
1090
1100
1110
1120
1130
1140
1150
1160
应用商城
第三方应用
应用防火墙子系统
目标应用平台
推荐管理子系统
安全计算子系统
云基础设施
目标应用
安全沙盒子系统
应用业务逻辑
数据交换子系统
数据通道
数据通道
数据通道
内容分发网络
境外应用
境外数据中心
境外开发部门

图1

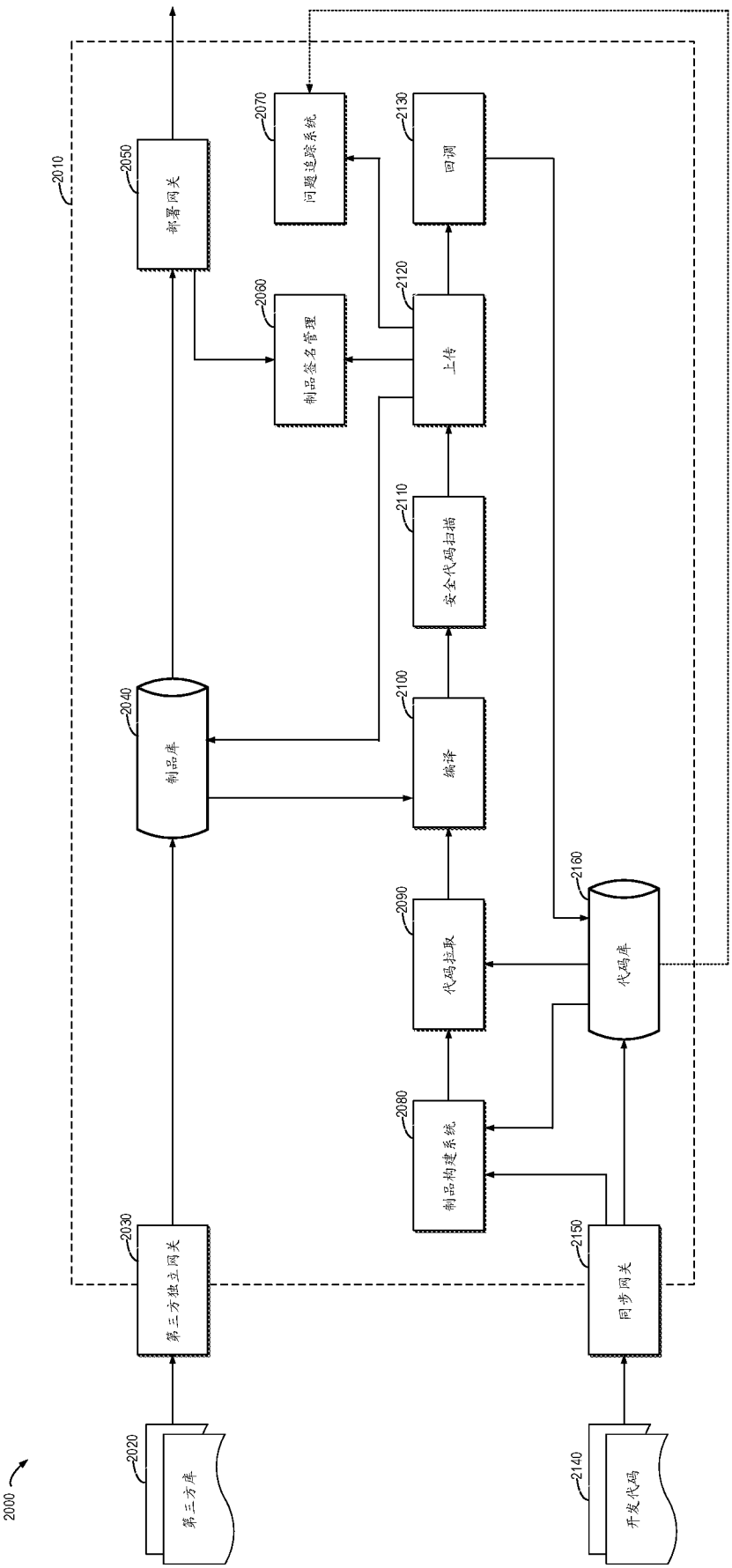
2000
2010
2020
第三方库
2030
第三方独立网关
2040
制品库
2050
部署网关
2060
制品签名管理
2070
问题追踪系统
2080
制品构建系统
2090
代码拉取
2100
编译
2110
安全代码扫描
2120
上传
2130
回调
2140
开发代码
2150
同步网关
2160
代码库

图2

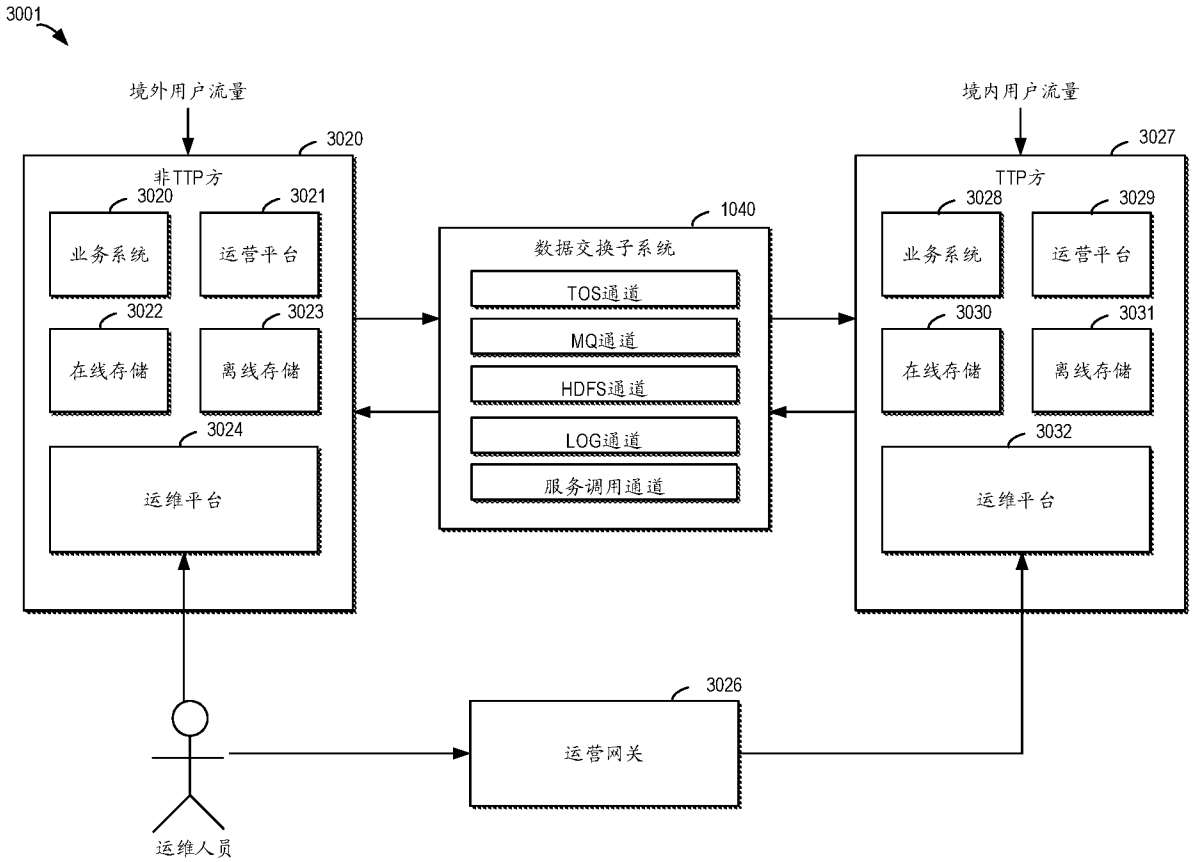
3001
境外用户流量
境内用户流量
3020
非TTP方
3020
业务系统
3021
运营平台
3022
在线存储
3023
离线存储
3024
运维平台
1040
数据交换子系统
TOS通道
MQ通道
HDFS通道
LOG通道
服务调用通道
3027
TTP方
3028
业务系统
3029
运营平台
3030
在线存储
3031
离线存储
3032
运维平台
3026
运营网关
运维人员

图 3A

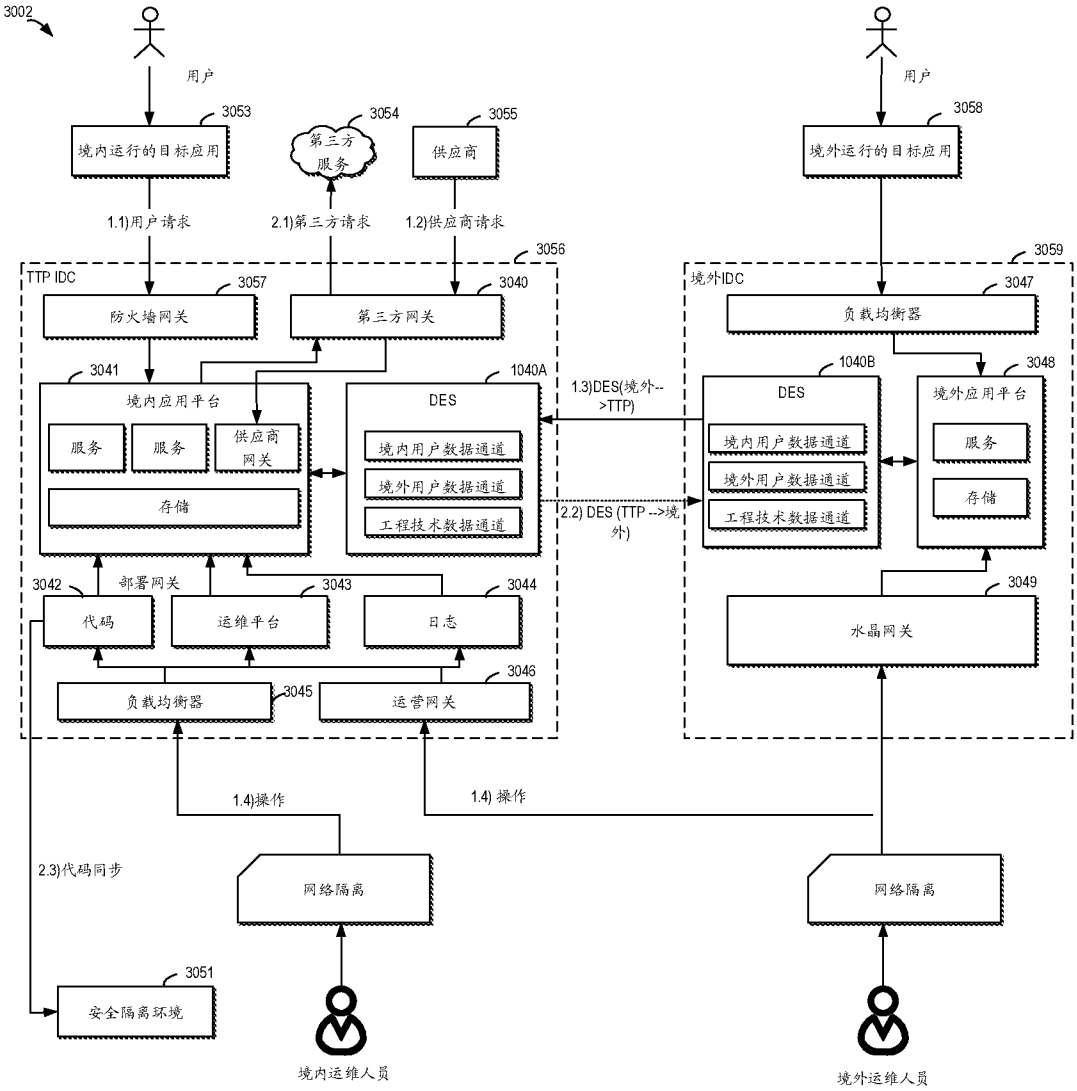
3002
用户
3053
境内运行的目标应用
3054
第三方服务
3055
供应商
1.1)用户请求
2.1)第三方请求
1.2)供应商请求
3056
TTP IDC
3057
防火墙网关
3040
第三方网关
3041
境内应用平台
服务
服务
供应商网关
存储
1040A
DES
境内用户数据通道
境外用户数据通道
工程技术数据通道
1.3)DES(境外-->TTP)
2.2) DES (TTP -->境外)
3042
部署网关
代码
3043
运维平台
3044
日志
负载均衡器
3045
运营网关
3046
1.4)操作
1.4) 操作
2.3)代码同步
网络隔离
3051
安全隔离环境
境内运维人员
用户
3058
境外运行的目标应用
3059
境外IDC
3047
负载均衡器
1040B
DES
境内用户数据通道
境外用户数据通道
工程技术数据通道
3048
境外应用平台
服务
存储
3049
水晶网关
网络隔离
境外运维人员

图 3B

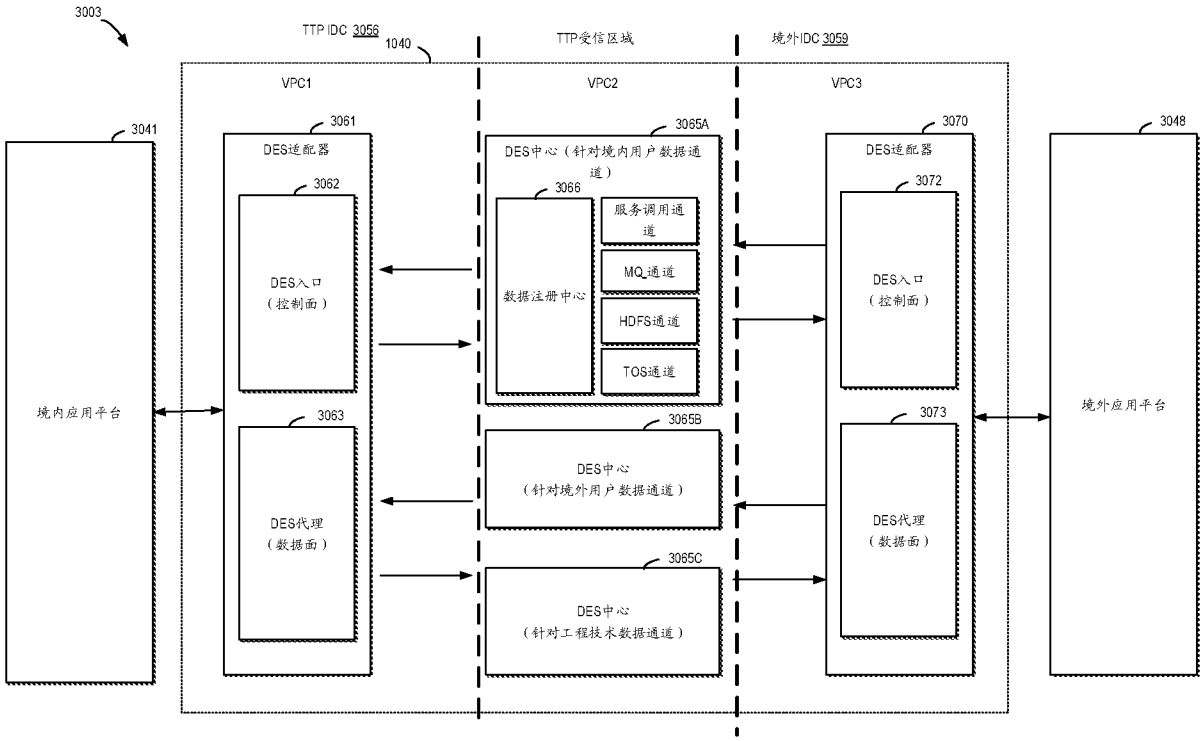
3003
TTP IDC 3056
1040
TTP受信区域
境外IDC 3059
VPC1
VPC2
VPC3
3041
3061
DES适配器
3062
DES入口
（控制面）
3063
DES代理
（数据面）
3065A
DES中心（针对境内用户数据通道）
3066
数据注册中心
服务调用通道
MQ通道
HDFS通道
TOS通道
3065B
DES中心
（针对境外用户数据通道）
3065C
DES中心
（针对工程技术数据通道）
3070
DES适配器
3072
DES入口
（控制面）
3073
DES代理
（数据面）
3048
境内应用平台
境外应用平台

图 3C

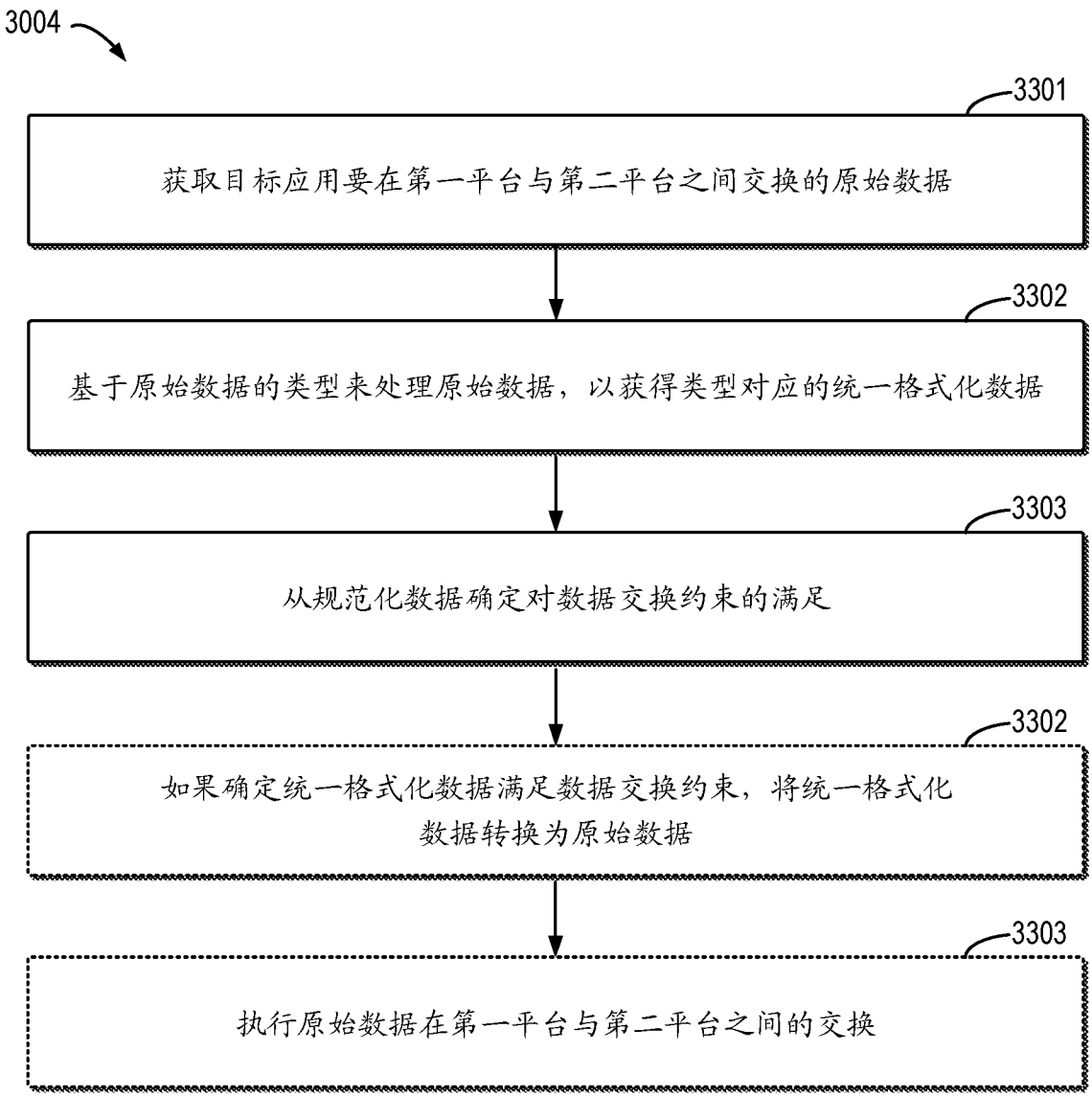
3004
3301
获取目标应用要在第一平台与第二平台之间交换的原始数据
3302
基于原始数据的类型来处理原始数据，以获得类型对应的统一格式化数据
3303
从规范化数据确定对数据交换约束的满足
3302
如果确定统一格式化数据满足数据交换约束，将统一格式化数据转换为原始数据
3303
执行原始数据在第一平台与第二平台之间的交换

图 3D

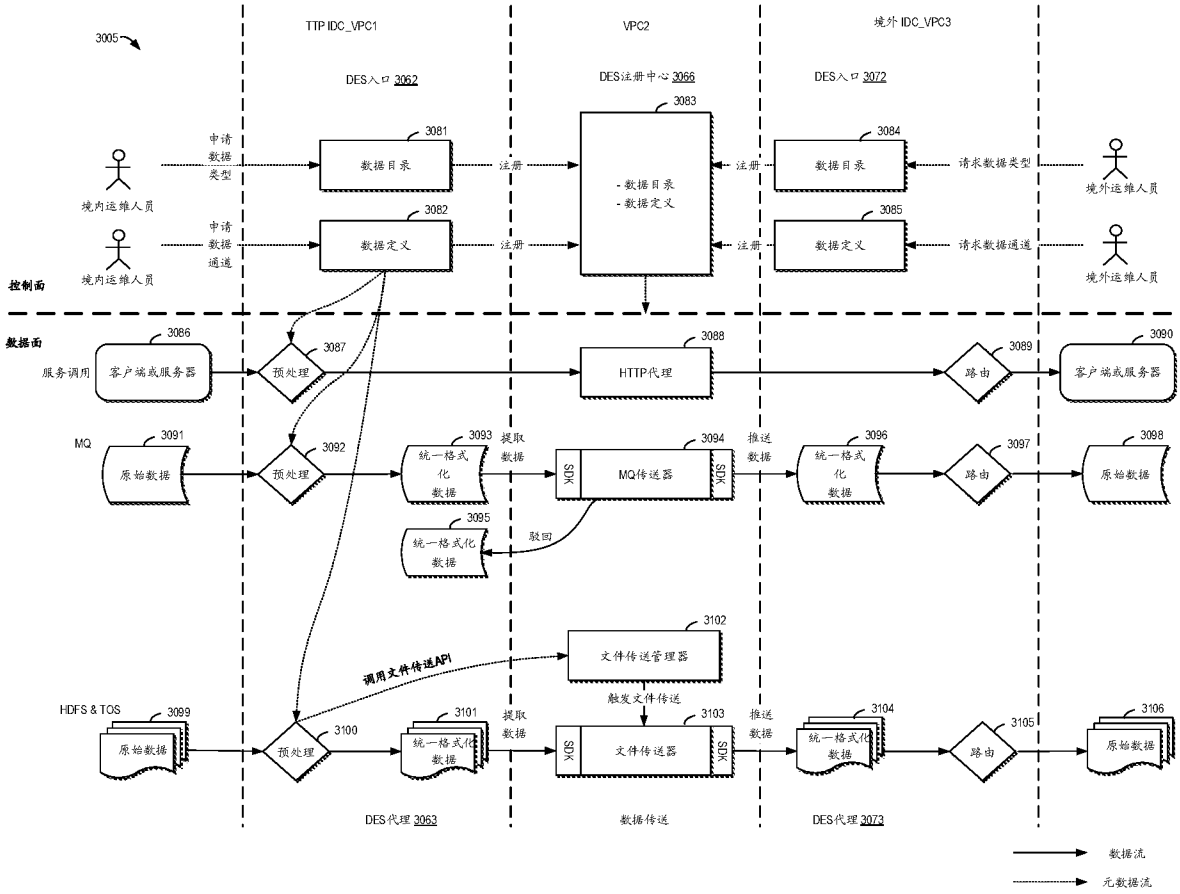
3005
TTP IDC_VPC1
VPC2
境外 IDC_VPC3
DES入口 3062
DES注册中心 3066
DES入口 3072
3083
3081
3084
申请数据类型
数据目录
注册
- 数据目录
- 数据定义
注册
数据目录
请求数据类型
境外运维人员
境内运维人员
3082
3085
申请数据通道
数据定义
注册
注册
数据定义
请求数据通道
境外运维人员
境内运维人员
控制面
数据面
3086
3087
3088
3089
3090
服务调用
客户端或服务器
预处理
HTTP代理
路由
客户端或服务器
MQ
3091
3092
3093
提取数据
3094
推送数据
3096
3097
3098
原始数据
预处理
统一格式化数据
SDK
MQ传送器
SDK
统一格式化数据
路由
原始数据
3095
驳回
统一格式化数据
3102
文件传送管理器
调用文件传送API
触发文件传送
HDFS & TOS
3099
3100
3101
提取数据
3103
推送数据
3104
3105
3106
原始数据
预处理
统一格式化数据
SDK
文件传送器
SDK
统一格式化数据
路由
原始数据
DES代理 3063
数据传送
DES代理 3073
数据流
元数据流

图 3E

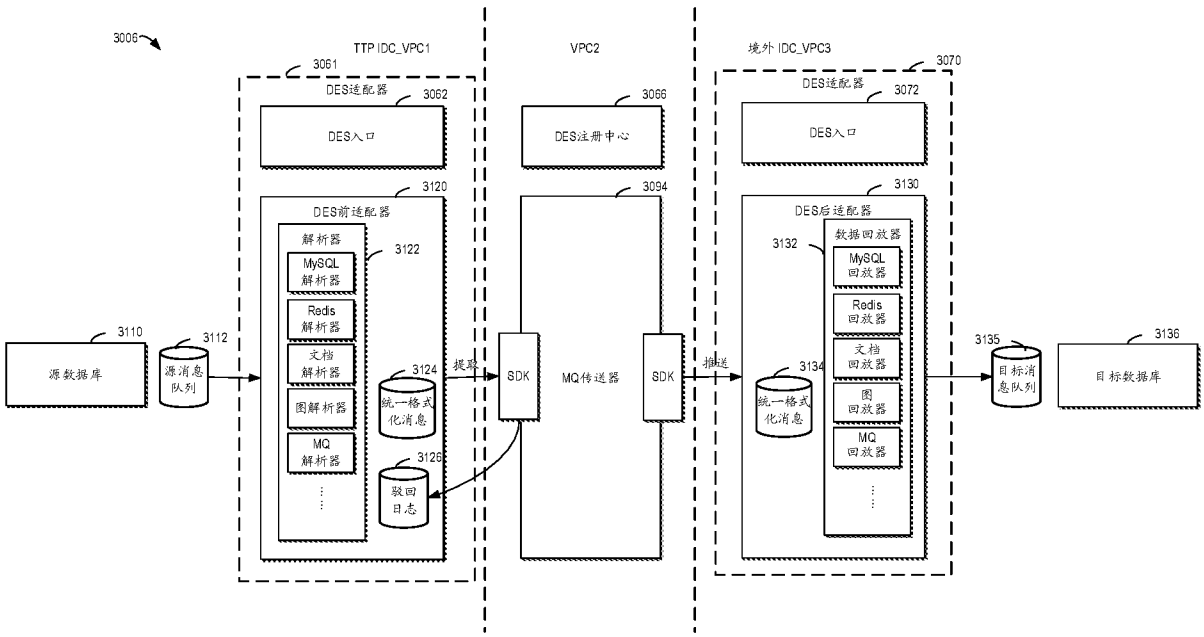
3006
TTP IDC_VPC1
VPC2
境外 IDC_VPC3
3061
DES适配器
3062
DES入口
3066
DES注册中心
3070
DES适配器
3072
DES入口
3120
DES前适配器
3094
3130
DES后适配器
解析器
3122
MySQL 解析器
Redis 解析器
文档 解析器
图解析器
MQ 解析器
3124
统一格式化消息
3126
驳回日志
SDK
MQ传送器
SDK
3132
数据回放器
MySQL 回放器
Redis 回放器
文档 回放器
图 回放器
MQ 回放器
3134
统一格式化消息
3110
源数据库
3112
源消息队列
提取
推送
3135
目标消息队列
3136
目标数据库

图 3F

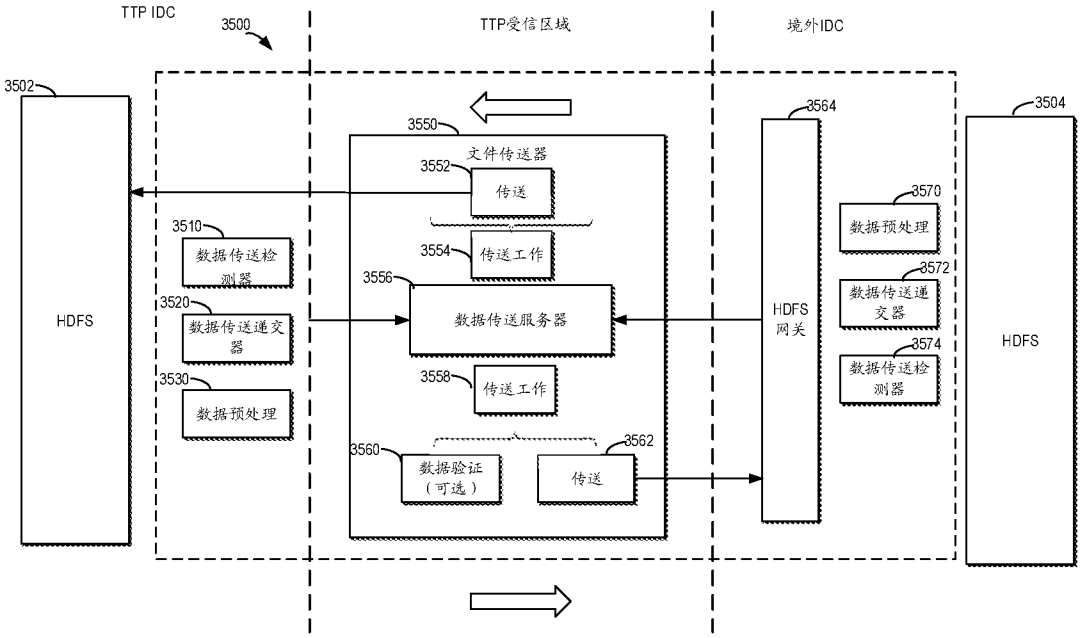
TTP IDC
3500
TTP受信区域
境外IDC
3502
HDFS
3550
文件传送器
3552
传送
3554
传送工作
3556
数据传送服务器
3558
传送工作
3560
数据验证（可选）
3562
传送
3510
数据传送检测器
3520
数据传送递交器
3530
数据预处理
3564
HDFS网关
3570
数据预处理
3572
数据传送递交器
3574
数据传送检测器
3504
HDFS

图 3G

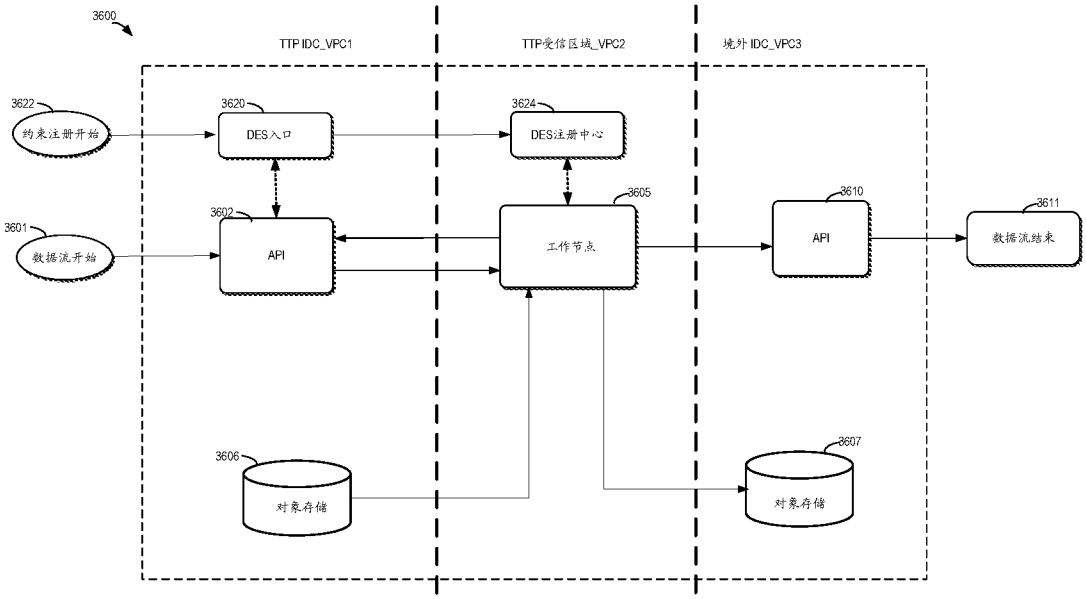
3600
TTP IDC_VPC1
TTP受信区域_VPC2
境外 IDC_VPC3
3622
约束注册开始
3620
DES入口
3624
DES注册中心
3601
数据流开始
3602
API
3605
工作节点
3610
API
3611
数据流结束
3606
对象存储
3607
对象存储

图 3H

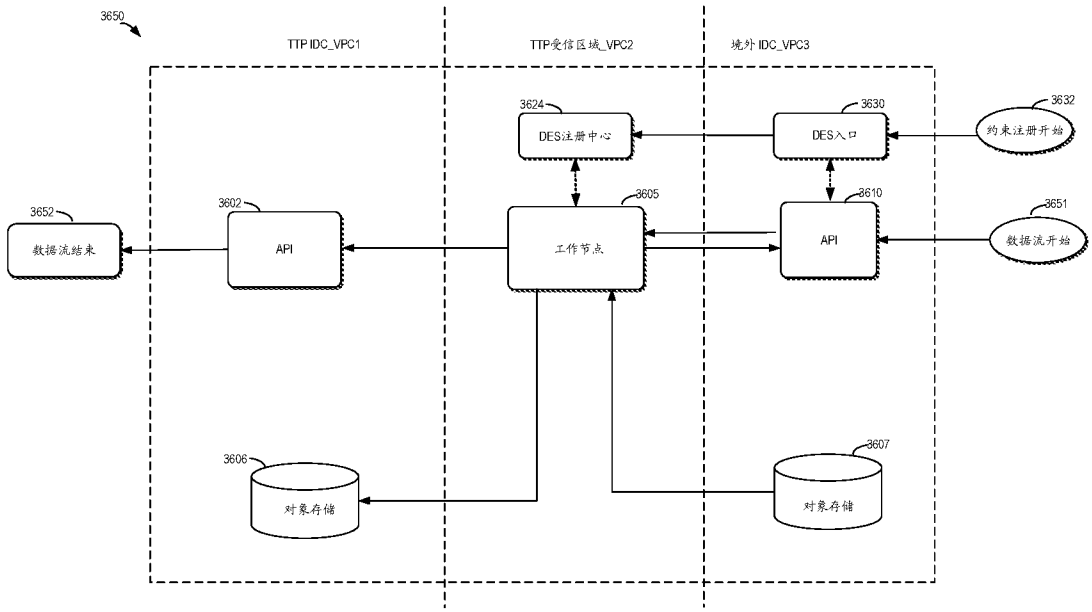
3650
TTP IDC_VPC1
TTP受信区域_VPC2
境外 IDC_VPC3
3624
DES注册中心
3630
DES入口
3632
约束注册开始
3652
数据流结束
3602
API
3605
工作节点
3610
API
3651
数据流开始
3606
对象存储
3607
对象存储

图 3I

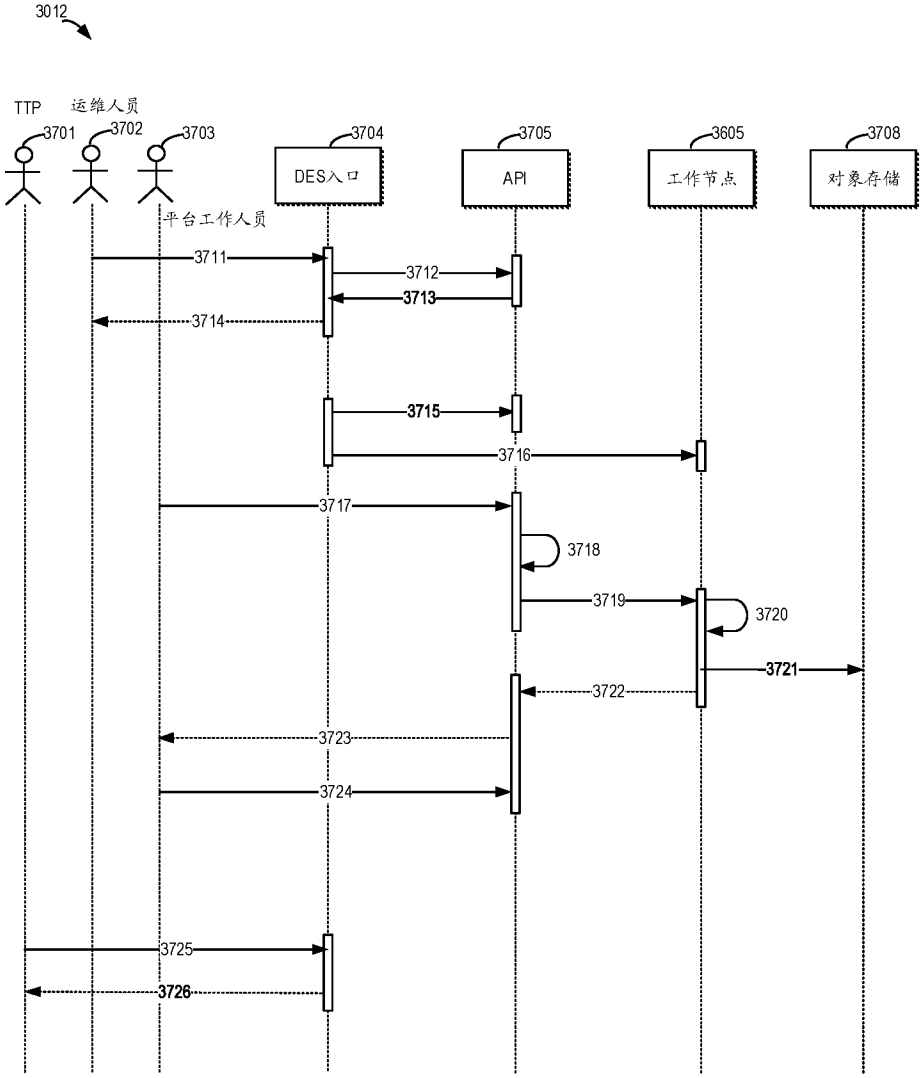
3012
TTP
运维人员
3701
3702
3703
平台工作人员
3704
DES入口
3705
API
3605
工作节点
3708
对象存储
3711
3712
3713
3714
3715
3716
3717
3718
3719
3720
3721
3722
3723
3724
3725
3726

图 3J

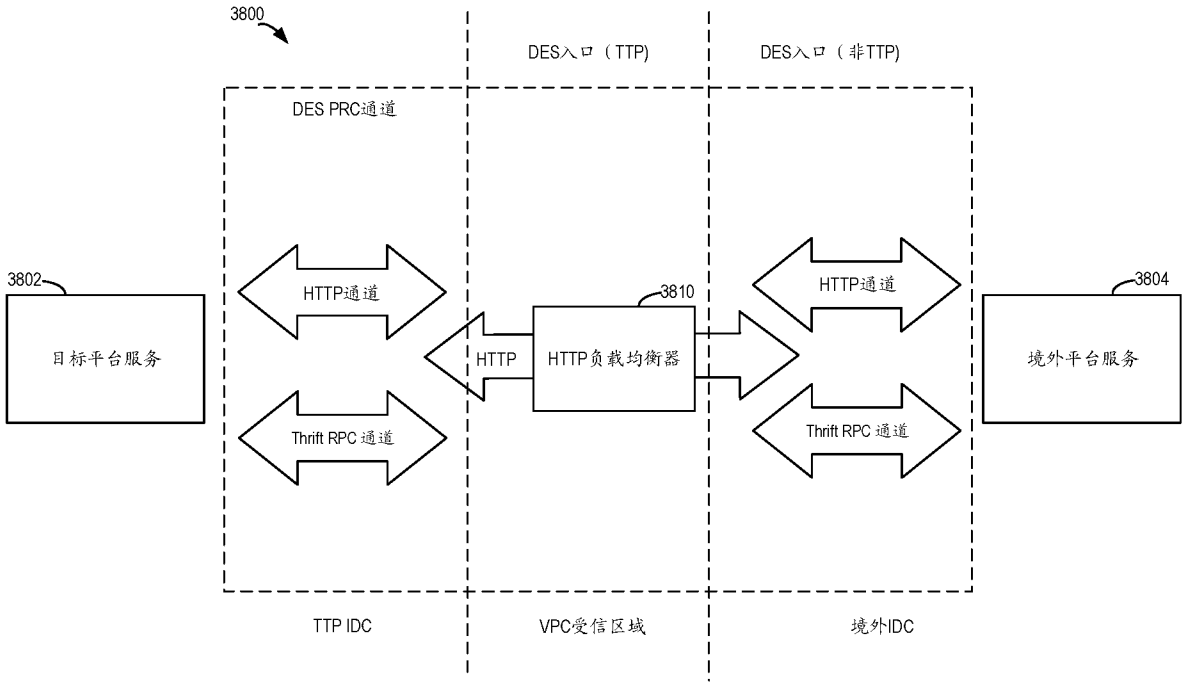
3800
DES入口（TTP）
DES入口（非TTP）
DES PRC通道
3802
目标平台服务
HTTP通道
Thrift RPC 通道
HTTP
3810
HTTP负载均衡器
HTTP通道
Thrift RPC 通道
3804
境外平台服务
TTP IDC
VPC受信区域
境外IDC

图 3K

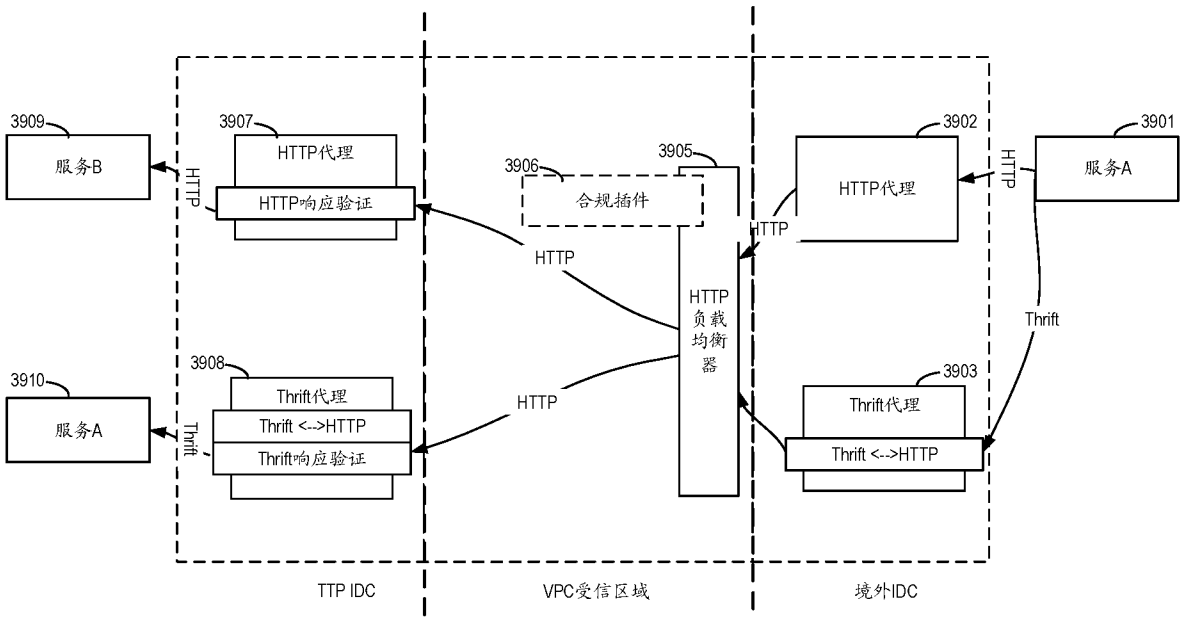
3909
服务B
3907
HTTP代理
HTTP响应验证
HTTP
3906
合规插件
3905
HTTP
HTTP
HTTP负载均衡器
3902
HTTP代理
HTTP
3901
服务A
Thrift
3910
服务A
3908
Thrift代理
Thrift <-->HTTP
Thrift响应验证
Thrift
HTTP
3903
Thrift代理
Thrift <-->HTTP
TTP IDC
VPC受信区域
境外IDC

图 3L

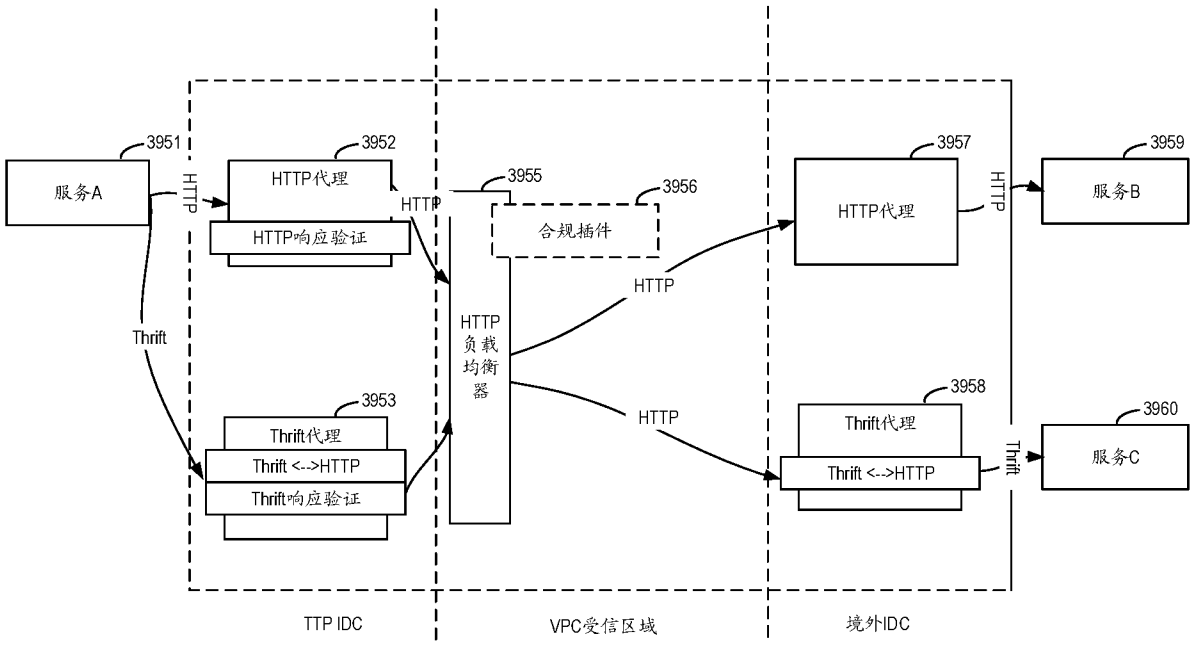
3951
服务A
HTTP
3952
HTTP代理
HTTP响应验证
HTTP
3955
3956
合规插件
HTTP
HTTP负载均衡器
Thrift
3953
Thrift代理
Thrift <-->HTTP
Thrift响应验证
HTTP
3957
HTTP代理
HTTP
3959
服务B
HTTP
3958
Thrift代理
Thrift <-->HTTP
Thrift
3960
服务C
TTP IDC
VPC受信区域
境外IDC

图 3M

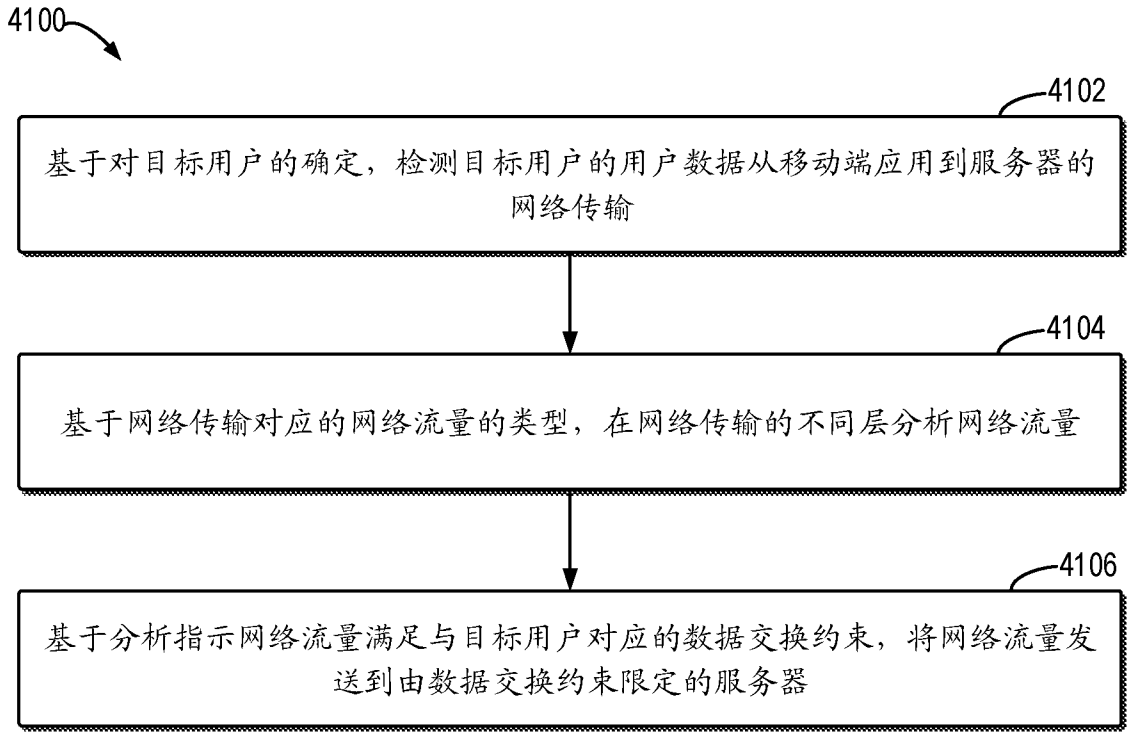
4100
4102
基于对目标用户的确定，检测目标用户的用户数据从移动端应用到服务器的网络传输
4104
基于网络传输对应的网络流量的类型，在网络传输的不同层分析网络流量
4106
基于分析指示网络流量满足与目标用户对应的数据交换约束，将网络流量发送到由数据交换约束限定的服务器

图 4A

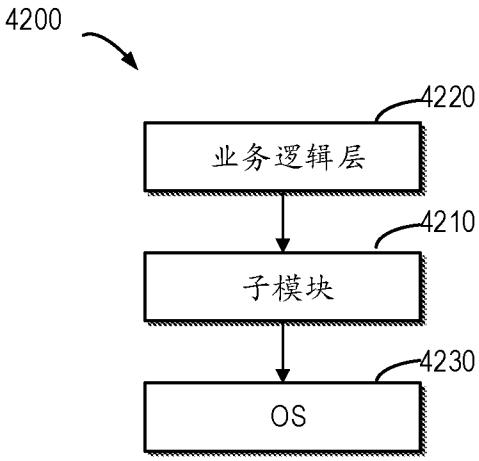
4200
4220
业务逻辑层
4210
子模块
4230
OS

图 4B

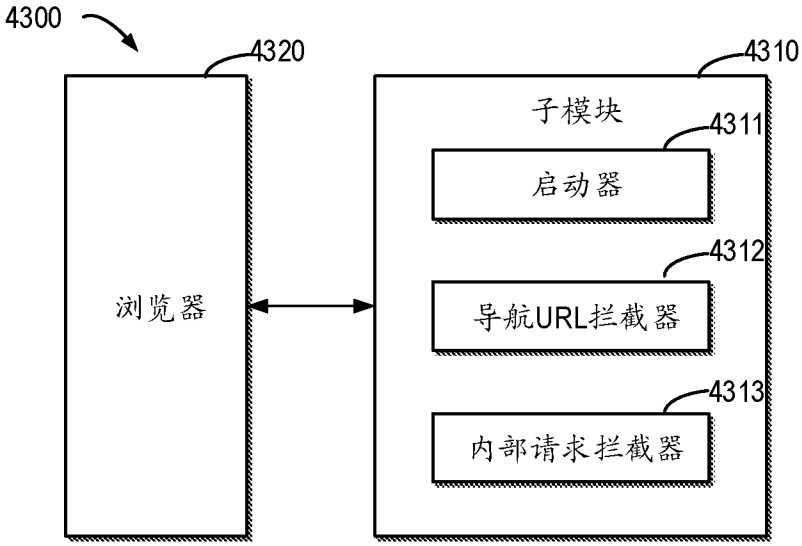
4300
4320
浏览器
4310
子模块
4311
启动器
4312
导航URL拦截器
4313
内部请求拦截器

图 4C

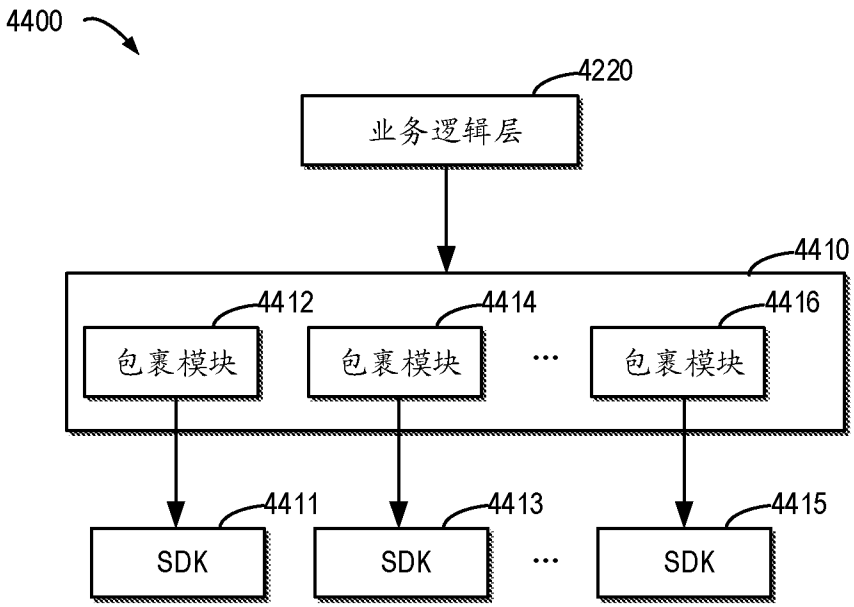
4400
4220
业务逻辑层
4410
4412
4414
4416
包裹模块
包裹模块
包裹模块
4411
4413
4415
SDK
SDK
SDK

图 4D

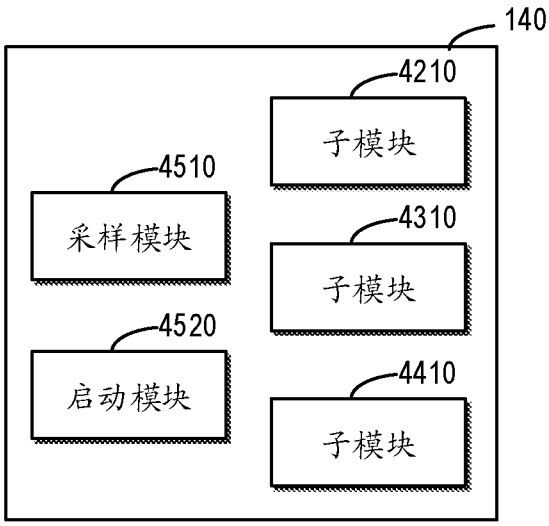
140
4210
子模块
4510
采样模块
4310
子模块
4520
启动模块
4410
子模块

图 4E

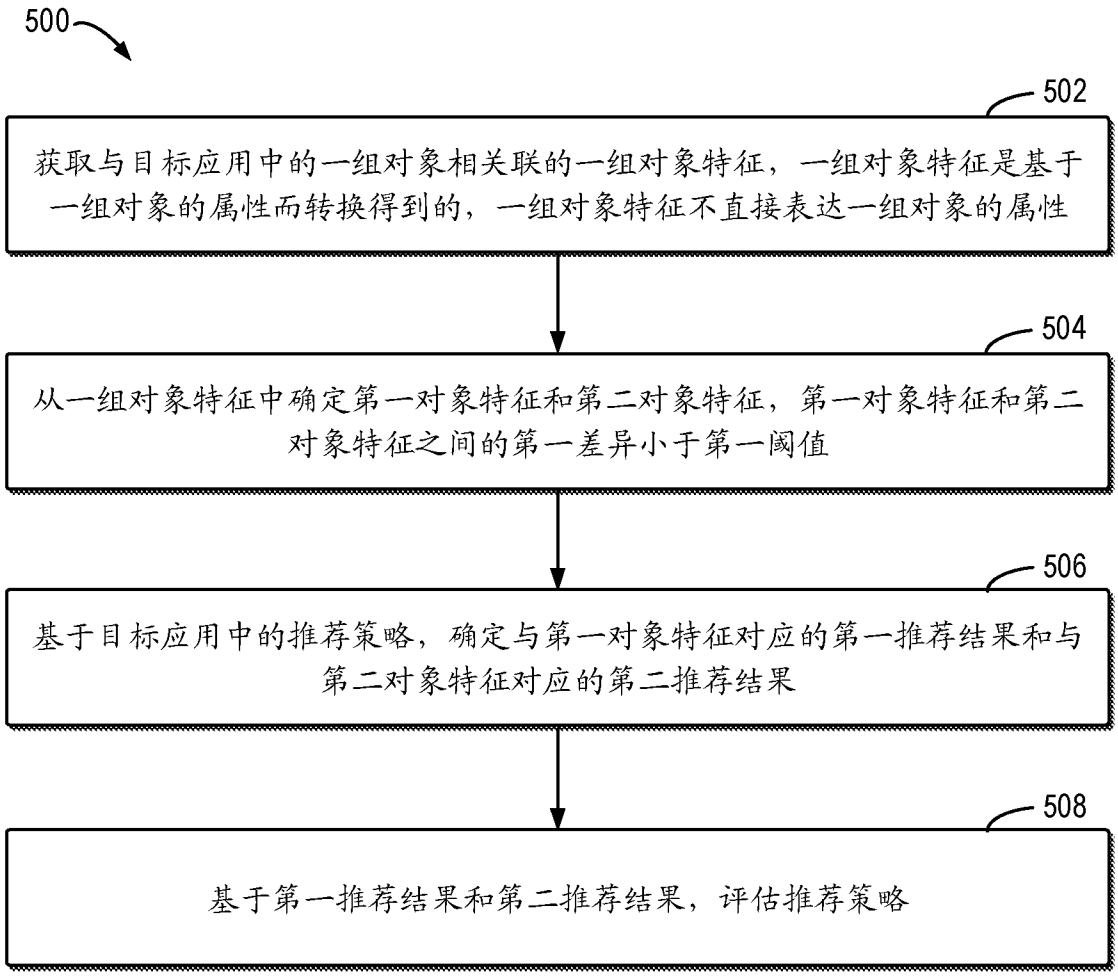
500
502
获取与目标应用中的一组对象相关联的一组对象特征，一组对象特征是基于一组对象的属性而转换得到的，一组对象特征不直接表达一组对象的属性
504
从一组对象特征中确定第一对象特征和第二对象特征，第一对象特征和第二对象特征之间的第一差异小于第一阈值
506
基于目标应用中的推荐策略，确定与第一对象特征对应的第一推荐结果和与第二对象特征对应的第二推荐结果
508
基于第一推荐结果和第二推荐结果，评估推荐策略

图 5

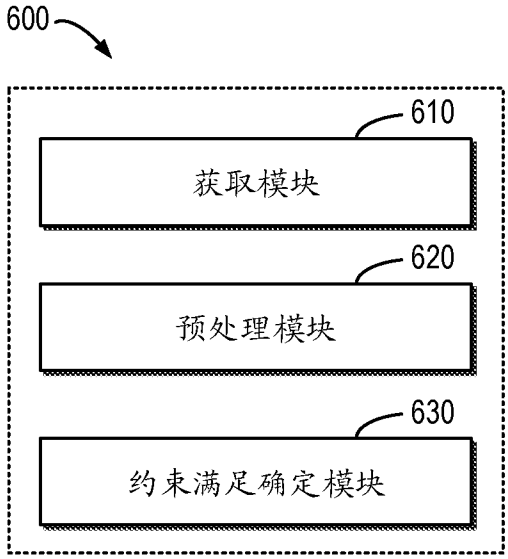
600
610
获取模块
620
预处理模块
630
约束满足确定模块

图 6

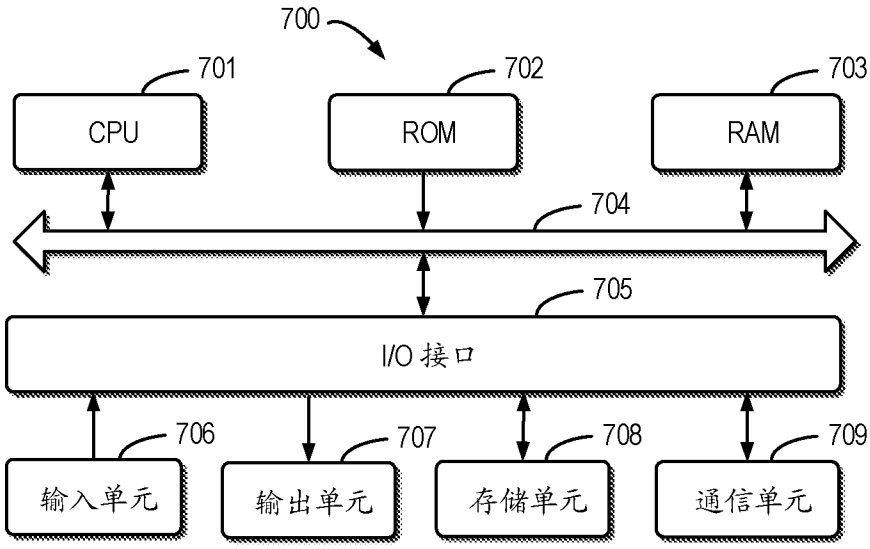
700
701
CPU
702
ROM
703
RAM
704
705
I/O 接口
706
输入单元
707
输出单元
708
存储单元
709
通信单元

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/113751

A. CLASSIFICATION OF SUBJECT MATTER

H04L 67/2866(2022.01)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)

H04L; 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)

CNPAT, CNKI, WPI, EPODOC: 数据, 信息, 内容, 交换, 交互, 转移, 统一, 同一, 标准, 中间, 格式, 结构, 形式, 满足, 约束, 条件, 限制, 审核, 审查, 跨国, 境外, data, information, content, exchange, interact, transfer, uniform, same, standard, format, structure, satisf+, constraint, condition, restrict, review, country

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105787065 A (INSPUR GENERAL SOFTWARE CO., LTD.) 20 July 2016 (2016-07-20) description, paragraphs [0019]-[0029], and figures 1-3	1-19
A	CN 101447999 A (GOLDEN VISTA (BEIJING) TECHNOLOGY CO., LTD.) 03 June 2009 (2009-06-03) entire document	1-19
A	CN 112333286 A (BEIJING ZIYUN INTELLIGENT TECHNOLOGY CO., LTD.) 05 February 2021 (2021-02-05) entire document	1-19
A	US 2003016682 A1 (SAMSUNG ELECTRONICS CO., LTD.) 23 January 2003 (2003-01-23) entire document	1-19

☐ 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	Date of mailing of the international search report
07 November 2022	**17 November 2022**
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
Information on patent family members

International application No.
PCT/CN2022/113751

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 105787065 A	20 July 2016	None	
CN 101447999 A	03 June 2009	None	
CN 112333286 A	05 February 2021	None	
US 2003016682 A1	23 January 2003	KR 20030004540 A	15 January 2003
		JP 2003134142 A	09 May 2003
		CN 1492647 A	28 April 2004

国际检索报告

国际申请号
PCT/CN2022/113751

A. 主题的分类

H04L 67/2866(2022.01)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)

H04L; 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））

CNPAT,CNKI,WPI,EPODOC： 数据，信息，内容，交换，交互，转移，统一，同一，标准，中间，格式，结构，形式，满足，约束，条件，限制，审核，审查，跨国，境外， data, information, content, exchange, interact, transfer, uniform, same, standard, format, structure, satisf+, constraint, condition, restrict, review, country

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
X	CN 105787065 A (浪潮通用软件有限公司) 2016年7月20日 (2016-07-20) 说明书第[0019]-[0029]段，图1-3	1-19
A	CN 101447999 A (神州数码金程北京科技有限公司) 2009年6月3日 (2009-06-03) 全文	1-19
A	CN 112333286 A (北京紫云智能科技有限公司) 2021年2月5日 (2021-02-05) 全文	1-19
A	US 2003016682 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2003年1月23日 (2003-01-23) 全文	1-19

☐ 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	国际检索报告邮寄日期
2022年11月7日	2022年11月17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 张枫 电话号码 86-(10)-53961628

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/113751

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	105787065	A	2016年7月20日	无			
CN	101447999	A	2009年6月3日	无			
CN	112333286	A	2021年2月5日	无			
US	2003016682	A1	2003年1月23日	KR	20030004540	A	2003年1月15日
				JP	2003134142	A	2003年5月9日
				CN	1492647	A	2004年4月28日