

(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
2016 年 12 月 1 日 (01.12.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/188335 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2016/082162
- (22) 国际申请日: 2016 年 5 月 16 日 (16.05.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510267072.7 2015 年 5 月 22 日 (22.05.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 赵坤 (ZHAO, Kun); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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))。

(54) Title: ACCESS CONTROL METHOD, APPARATUS AND SYSTEM FOR USER DATA

(54) 发明名称: 用户数据的访问控制方法、装置及系统

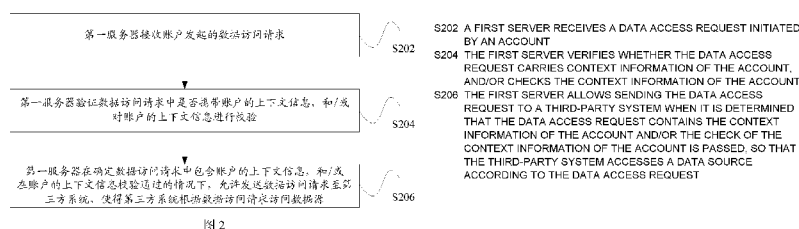


图 2

(57) Abstract: Disclosed are an access control method, apparatus and system for user data. The method comprises: a first server receives a data access request initiated by an account; the first server verifies whether the data access request carries context information of the account, and/or checks the context information of the account; and the first server allows sending the data access request to a third-party system when it is determined that the data access request contains the context information of the account and/or the check of the context information of the account is passed, so that the third-party system accesses a data source according to the data access request. The present application solves the technical problem of poor security of a data source due to poor security of an account initiating an access in a process in which a user accesses the data source by using a third-party system in the prior art.

(57) 摘要: 本发明公开了一种用户数据的访问控制方法、装置及系统。其中, 该方法包括: 第一服务器接收账户发起的数据访问请求; 第一服务器验证数据访问请求中是否携带账户的上下文信息, 和/或对账户的上下文信息进行校验; 第一服务器在确定数据访问请求中包含账户的上下文信息, 和/或在账户的上下文信息校验通过的情况下, 允许发送数据访问请求至第三方系统, 使得第三方系统根据数据访问请求访问数据源。本申请解决了现有技术在用户使用第三方系统访问数据源的过程中, 由于发起访问的账户的安全性差, 导致数据源数据安全性差, 导致数据源数据安全性差的技术问题。

WO 2016/188335 A1

用户数据的访问控制方法、装置及系统

本申请要求 2015 年 05 月 22 日递交的申请号为 201510267072.7、发明名称为“用户数据的访问控制方法、装置及系统”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。

5

技术领域

本发明涉及互联网领域，具体而言，涉及一种用户数据的访问控制方法、装置及系统。

10 背景技术

现有的服务提供商（例如淘宝、天猫等网站）为了更好的为用户提供服务，需要大量独立软件提供商 ISV 来共同为用户服务。在这种情况下，服务提供商通过建立数据开放平台来实现在数据源服务器中存储大量的对外开放的用户数据，用户可以授权第三方系统访问存储于数据源服务器中的用户数据，由此这种将大量用户数据开放给 ISV 提供的系统的方案，实现了一个数据开放的应用环境。

15

在上述数据开放的应用环境中，由于访问用户的安全性无法保证，例如黑客伪造合法用户的账户，使得伪造的账户可以替代合法用户来使用第三方系统来访问数据源，导致数据源服务器的用户数据被非法访问，造成数据泄密。

20

进一步的，由于 ISV 提供的系统是一种非可控的第三方系统，在第三方系统处理大量的用户数据的过程中，无法预估各种人为原因（例如在用户授权允许的时间内私下随意读写用户数据）或者黑客攻击而导致的用户数据泄密情况，从而非可控的第三方系统的安全性较差，使得在数据开发平台与 ISV 提供的系统所组成数据开放环境的安全性较差。

25

此处需要详细说明的是，在相关技术中，通常使用类似 OAuth(开放授权)协议进行授权。OAuth 是一个开放标准，允许用户授权第三方系统访问用户数据，而不需要将用户名和密码提供给第三方系统，避免了密码等敏感信息泄露给第三方系统。

由上可知，用户授权第三方系统访问用户数据时，一种可能的风险如下：第三方系统可以获得代表用户身份的临时会话令牌，该临时会话令牌和用户状态等信息无关，一般在授权时间内为固定值，如果该临时会话令牌被盗，盗用者将有可能随意读写用户数

据，造成了用户数据安全性低。而且，第三方系统良莠不齐，安全性差的第三方系统存在着被恶意控制或人为原因恶意操作的可能，在这种情况下，如果获取到了第三方系统上维护的所有用户列表和用户授权信息，也有可能使用该用户授权信息随意读写用户数据，造成了用户数据安全性低。

5 例如，当合法用户向第三方系统授权后，用户 B 冒充用户 A 发起的数据访问请求也可以送达第三方系统，在这种情况下，用户 B 请求访问用户 A 的用户数据，第三方系统无法甄别该数据访问请求是否由用户 A 发起，或者意外允许了用户 B 冒充用户 A 发起的数据访问请求，那么用户 B 就可以随意读写用户 A 的用户数据，同样造成了用户数据安全性低。

10 针对上述现有技术在使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的问题，目前尚未提出有效的解决方案。

发明内容

本申请实施例提供了一种用户数据的访问控制方法、装置及系统，以至少解决现有技术在用户使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

根据本申请实施例的一个方面，提供了一种用户数据的访问控制方法，包括：第一服务器接收账户发起的数据访问请求；第一服务器验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验；第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源。

根据本申请实施例的一个方面，还提供了一种用户数据的访问控制方法，包括：客户端获取账户的上下文信息；客户端发送账户触发的数据访问请求至第一服务器，其中，数据访问请求至少包括上下文信息；客户端接收第一服务器根据数据访问请求获取到的访问数据；其中，在第一服务器确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源。

根据本申请实施例的一个方面，还提供了一种用户数据的访问控制方法，包括：第三方系统接收第一服务器发送的数据访问请求，其中，数据访问请求为由账户发起的包含了账户的上下文信息的请求；第三方系统转发数据访问请求至数据源服务器；第三方

系统接收数据源服务器返回的数据访问请求所要访问的数据，其中，当数据源服务器根据数据访问请求中包含的上下文信息，确定发起数据访问请求的账户为安全访问账户，且数据访问请求为安全访问请求时，允许第三方系统根据数据访问请求访问数据源。

根据本申请实施例的另一方面，还提供了一种用户数据的访问控制装置，包括：接收模块，用于接收账户发起的数据访问请求；校验模块，包含第一校验单元和/或第二校验单元，其中，第一校验单元用于验证数据访问请求中是否携带账户的上下文信息，第二校验单元对账户的上下文信息进行校验；控制模块，用于在校验模块校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源。

根据本申请实施例的另一方面，还提供了一种用户数据的访问控制装置，包括：获取模块，用于获取账户的上下文信息；发送模块，用于发送账户触发的数据访问请求至第一服务器，其中，数据访问请求至少包括上下文信息；接收模块，用于接收第一服务器根据数据访问请求获取到的访问数据；其中，在第一服务器确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源。

根据本申请实施例的另一方面，还提供了一种用户数据的访问控制装置，包括：第一接收模块，用于接收第一服务器发送的数据访问请求，其中，数据访问请求为由账户发起的包含了账户的上下文信息的请求；转发模块，用于转发数据访问请求至数据源服务器；第二接收模块，用于接收数据源服务器返回的数据访问请求所要访问的数据，其中，当数据源服务器根据数据访问请求中包含的上下文信息，确定发起数据访问请求的账户为安全访问账户，且数据访问请求为安全访问请求时，允许第三方系统根据数据访问请求访问数据源。

根据本申请实施例的又一方面，还提供了一种用户数据的访问控制系统，包括：客户终端，用于在账户登录之后，发起数据访问请求；第一服务器，与客户终端通信，用于在验证数据访问请求中包含了账户的上下文信息，和/或验证上下文信息为合法信息之后，透传数据访问请求；第三方系统服务器，与第一服务器通信，用于接收第一服务器透传的数据访问请求；数据源服务器，与第三方系统服务器通信，用于接收第三方系统服务器通信转发的数据访问请求，在根据数据访问请求中包含的上下文信息，确定发起数据访问请求的账户为安全访问账户，且数据访问请求为安全访问请求时，返回数据访问请求对应的访问数据至第三方系统服务器。

在本申请实施例中，采用第一服务器接收账户发起的数据访问请求，验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验的方式，通过第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统。由以上方案可知，当前账户（可以是合法账户或者伪造账户冒充该合法账户）发出数据访问请求到达第一服务器后，第一服务器会对接收到的每一个数据访问请求进行校验，即第一服务器会判断数据访问请求是否携带账户上下文信息，和/或上下文信息是否能够校验通过，当对数据访问请求的校验通过的情况下，第一服务器允许该数据访问请求发送至第三方系统，进而第三方系统就可以根据该数据访问请求访问数据源。在上述方案中，只有合法账户发起的数据访问请求能够通过校验，而对于冒充合法账户的恶意账户发起的数据访问请求，要么在形式上不携带账户上下文信息，要么在内容上携带的上下文信息不能通过校验。从而达到了使得第三方系统根据数据访问请求访问数据源的目的，进而实现了在第三方系统接收数据访问前就能够鉴别发送该数据访问请求的账户是否为合法账户的技术效果，解决了现有技术在使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

图 1 是根据本申请实施例的一种用户数据的访问控制方法的计算机终端的硬件结构框图；

图 2 是根据本申请实施例一的用户数据的访问控制方法的流程图；

图 3 是根据本申请实施例一的一种可选的用户数据的访问控制方法的业务流程示意图；

图 4 是根据本申请图 2 所示实施例的一种可选的用户数据的访问控制方法的流程示意图；

图 5 是根据本申请图 2 所示实施例的另一种可选的用户数据的访问控制方法的流程示意图；

图 6 是根据本申请实施例一的用户数据的访问控制系统的业务流程交互示意图；

图 7 是根据本申请实施例二的用户数据的访问控制方法的流程示意图；

图 8 是根据本申请实施例三的用户数据的访问控制方法的流程图；

图 9 是根据本申请实施例四的用户数据的访问控制装置的结构示意图；

图 10 是根据本申请图 9 所示实施例的一种可选的第二校验单元的结构示意图；

图 11 是根据本申请图 9 所示实施例的另外一种可选的第二校验单元的结构示意图；

5 图 12 是根据本申请实施例五的用户数据的访问控制装置的结构示意图；

图 13 是根据本申请实施例六的用户数据的访问控制装置的结构示意图；

图 14 是根据本申请实施例七的用户数据的访问控制系统的结构示意图；

图 15 是根据本申请实施例的一种计算机终端的结构框图。

10 具体实施方式

为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分的实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保
15 护的范围。

需要说明的是，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”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变
20 形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

下面对本申请涉及到的术语进行解释如下：

独立软件提供商(Independent Software Vendors, ISV)，或称为独立软件开发商，指
25 专门从事软件的开发、生产、销售和服务的企业。

上下文信息，或称 context 信息，与账户的活动状态和活动信息相关，账户的上下文信息可以作为重要的评判标准，用以决定第三方系统是否能获取以及能获取多高权限等级的用户数据。

实施例一

30 根据本申请实施例，还提供了一种用户数据的访问控制方法的方法实施例，需要说

明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

本申请实施例一所提供的方法实施例可以在移动终端、计算机终端或者类似的运算
5 装置中执行。以运行在计算机终端上为例，图 1 是本申请实施例的一种用户数据的访问控制方法的计算机终端的硬件结构框图。如图 1 所示，计算机终端 10 可以包括一个或多个（图中仅示出一个）处理器 102（处理器 102 可以包括但不限于微处理器 MCU 或可编程逻辑器件 FPGA 等的处理装置）、用于存储数据的存储器 104、以及用于通信功能的传输模块 106。本领域普通技术人员可以理解，图 1 所示的结构仅为示意，其并不对上
10 述电子装置的结构造成限定。例如，计算机终端 10 还可包括比图 1 中所示更多或者更少的组件，或者具有与图 1 所示不同的配置。

存储器 104 可用于存储应用软件的程序以及模块，如本申请实施例中的用户数据的访问控制方法对应的程序指令/模块，处理器 102 通过运行存储在存储器 104 内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的应用程序的漏洞
15 检测方法。存储器 104 可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 104 可进一步包括相对于处理器 102 远程设置的存储器，这些远程存储器可以通过网络连接至计算机终端 10。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

20 传输装置 106 用于经由一个网络接收或者发送数据。上述的网络具体实例可包括计算机终端 10 的通信供应商提供的无线网络。在一个实例中，传输装置 106 包括一个网络适配器（Network Interface Controller，NIC），其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置 106 可以为射频（Radio Frequency，RF）模块，其用于通过无线方式与互联网进行通讯。

25 在上述运行环境下，本申请提供了如图 2 所示的用户数据的访问控制方法。图 2 是根据本申请实施例一的用户数据的访问控制方法的流程图。

结合图 1 和图 2 可知，上述计算机终端 10 可以是第一服务器，如图 2 所示，一种可选的用户数据的访问控制方法包括如下实施步骤：

步骤 S202：第一服务器接收账户发起的数据访问请求。

30 本申请上述步骤 S202 中，结合图 3 可知，上述账户可以是客户端注册的合法账户，

也可以是伪造后的非法账户。其中，合法账户登录的客户端可以不限于淘宝、天猫等产品，用户可以在该客户端上注册账户，每个用户使用账户登录客户端之后，可以通过使用该客户端发起上述数据访问请求。

此处需要说明的是，结合图 3 可知，上述第一服务器可以为图 3 中所示的一种网关，此处的网关用于透传所述数据访问请求。一种可选方案中，上述第一服务器可以是阿里云的负载均衡服务器。

例如，以淘宝网的卖家实现订单管理功能为例，淘宝网可以提供该卖家的所有数据源（例如订单的产品信息、交易内容、交易金额和产品评价等信息），由于淘宝网没有提供订单管理的功能，此时淘宝网通过提供一个接口实现授权独立软件提供商提供一个可以提供订单管理功能的第三方系统，因此，当任意一个注册成功的登录账户成功登录淘宝之后，可以通过在浏览器中打开上述第三方系统的网页发起数据访问请求，来实现通过第三方系统访问淘宝的数据源来获取访问数据，进一步实现订单管理功能。

步骤 S204：第一服务器验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验。

本申请上述步骤 S204 中涉及到的上下文信息与账户的活动状态和活动信息相关，用于表征该上下文信息对应的账户赋予第三方系统访问该账户用户数据的权限。在本申请实施例中，上下文信息可以包括但不限于账户的在线状态、账户的离线状态、账户的在线时间、账户的离线时间、账户的登录时间、账户的登录地点、账户的登录设备、账户访问用户数据的记录、账户的数据隐私安全等级、账户的常用登录设备、账户的常用登录地点、账户的账号安全状态以及账户的账号风险评估等信息。

本申请提供的上述步骤可以实现通过对接收到的数据访问请求中是否携带有上下文信息和/或账户的上下文信息进行校验，来确定发起该数据访问请求的账户是否是合法账户。从上述上下文信息包含的信息种类来看，上下文信息是一种具有非固定值，且黑客无法盗取等特性的数据，因此，采用基于上下文信息来验证账户是否合法具有较高的可信度。本申请这种引入上下文检查机制的方案，可以使得账户的验证结果更加准确，具体的，可以有效解决在用户授权允许的的时间内，用户数据被随意访问的问题。

仍旧以淘宝网的卖家实现订单管理功能为例，在淘宝网卖家通过打开提供订单管理功能的第三方系统，触发发送数据访问请求的行为后，客户端的当前登录账户会发出包含该卖家账户的上下文信息的数据访问请求，此时，如果有黑客或者恶意用户伪造该卖家账户，该伪造账户也会冒充该卖家账户并发出数据访问请求，那么卖家自己触发发送

的数据访问请求和冒充卖家发送的数据访问请求都会传送至第一服务器，此时，第一服务器可以通过验证接收到的数据访问请求是否包含上下文信息，和/或该上下文信息是否为合法信息，来分辨出伪造账户。例如图 3 中所示的网关，对接收到的所有数据访问请求进行上述的验证或校验，以实现发起该数据访问请求的账户的甄别。

- 5 步骤 S206：第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源。

10 本申请上述步骤 S206 中，由于在数据访问请求中包含了账户的上下文信息，和/或该上下文信息是合法信息的情况下，可以确定当前的账户为安全账户，因此，第一服务器（可以是图 3 所示的网关）将允许安全账户发起的数据访问请求透传至第三方系统，进入第三方系统中处理该数据访问请求，即第三方系统根据接收到的数据访问请求访问数据源，向数据源请求该用户的数据。

15 可选的，第三方系统可以通过向数据源服务器转发该数据访问请求的方式，请求访问存储于数据源服务器中的用户数据，然后，数据源服务器将根据该数据访问请求读取到的用户数据返回至第三方系统。

20 此处需要说明的是，本申请涉及到的第三方系统为基于软件提供商提供的系统服务器来实现相关系统功能，可以通过至少如下一种方式来触发第三方系统实现相关功能：在浏览器中输入地址来打开上述第三方系统的网页来访问对应的系统服务器，调用启动第三方系统的相关功能；通过触发安装在客户端上的插件来访问对应的系统服务器，从而启动第三方系统的相关功能、通过触发安装在客户端上的应用软件来访问对应的系统服务器，从而启动第三方系统的相关功能。

25 由此可知，本申请提供的上述步骤可以实现第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，第一服务器认为发出该数据访问请求的账户为合法账户，并将该数据访问请求发送至第三方系统。可以看出，经过第一服务器透传至第三方系统的合法账户发出的数据访问请求，相当于给予第三方系统一个数据源访问权限，并指示了第三方系统去数据源中读取何种类型的用户数据，由此实现了分辨第三方系统接收到的数据访问请求是否由合法账户发出。

30 一种本申请涉及到的数据开放的应用环境中，用户注册得到的合法账户发起的数据访问请求中携带了该账户的上下文信息，未注册账户或者冒充注册账户发出的数据访问请求中则没有携带账户的上下文信息。在这种情况下，第一服务器通过验证数据访问请

求中是否携带账户的上下文信息就可判断该数据访问请求是否是由合法账户发起。

另一种本申请涉及到的数据开放的应用环境中，用户注册得到的合法账户发起的数据访问请求中携带了该账户的上下文信息；而可能经过伪造，未注册账户或者冒充注册账户发出的数据访问请求中看起来像是携带了账户的上下文信息。由于账户的上下文信息具有账户本身的活动状态和活动信息，且该活动状态和活动信息具有可变的属性，无法被黑客获取，因此伪造的数据访问请求即便在形式上看起来携带了上下文信息，在内容上也无法与其冒充的合法账户的真实的上下文信息一致。在这种情况下，第一服务器需要对账户的上下文信息进行校验；或者第一服务器在判断出数据访问请求中是否携带账户的上下文信息后进一步的对账户的上下文信息进行校验，来判断该数据访问请求是否是由合法账户发起。

具体的，对于淘宝、天猫等产品，第三方系统可以是包括订单管理系统、物流管理系统或虚拟机服务器等，数据源可以是账户在使用淘宝、天猫网站时生成并被记录的各种用户数据，例如对于淘宝买家而言，数据源可以包括：用户头像、用户昵称、用户注册时间、用户登录信息、用户手机号码、用户邮箱、用户地址、用户历史购物信息、用户购物需求、用户收藏信息以及用户支付信息等等。

仍旧以淘宝网的卖家实现订单管理功能为例，对于黑客或者恶意用户伪造淘宝卖家账户，并通过该伪造账户冒充淘宝卖家账户发出的数据访问请求，不可能携带正确的该淘宝卖家账户的上下文信息，因此第一服务器或者验证处该数据访问请求不包含账户上下文信息，或者校验包含的账户上下文信息失败，故而第一服务器可以认定该数据访问请求不是通过合法账户发出的数据访问请求；而对于淘宝卖家自己触发第三方系统（例如订单管理系统）提供的插件发送出的数据访问请求，携带了该卖家账户的上下文信息，第一服务器经验证该数据请求包含了账户上下文信息，且携带的上下文信息校验正确，故而第一服务器可以认定该数据访问请求是通过合法账户发出的数据访问请求，进而将该数据访问请求发送至提供订单管理功能的第三方系统，提供订单管理功能的第三方系统就可以凭借该数据访问请求，访问淘宝网提供的数据源中关于该卖家账户的相关数据（例如订单的产品信息、交易内容、交易金额和产品评价等信息），以获得用户数据，完成第三方系统提供的订单管理功能。

由上可知，本申请上述实施例一所提供的方案中，当前账户（可以是合法账户或者伪造账户冒充该合法账户）发出数据访问请求到达第一服务器后，第一服务器会对接收到的每一个数据访问请求进行校验，即第一服务器会判断数据访问请求是否携带账户上

下文信息,和/或上下文信息是否能够校验通过,当对数据访问请求的校验通过的情况下,第一服务器允许该数据访问请求发送至第三方系统,进而第三方系统就可以根据该数据访问请求访问数据源。在上述方案中,只有合法账户发起的数据访问请求能够通过校验,而对于冒充合法账户的恶意账户发起的数据访问请求,要么在形式上不携带账户上下文信息,要么在内容上携带的上下文信息不能通过校验。通过上述方案,实现了允许具有访问权限的合法账户发起的数据访问请求发送至第三方系统,解决了现有技术在使用第三方系统访问数据源的过程中,由于发起访问的账户的安全性差,导致数据源数据安全性差的技术问题。

本申请上述实施例提供的可选方案中,在步骤 S206:第一服务器在确定数据访问请求中包含账户的上下文信息,和/或在账户的上下文信息校验通过的情况下,允许该数据访问请求发送至第三方系统之后,还可以执行如下实施步骤:

第一种可选的实施步骤中,第一服务器在确定数据访问请求中没有包含账户的上下文信息,或在账户的上下文信息校验失败的情况下,第一服务器禁止发送数据访问请求至第三方系统,并发出报警信息。

本申请上述实施步骤中,第一服务器禁止发送未通过校验的数据访问请求至第三方系统,并发出报警信息,用于警示该数据访问请求没有包含上下文信息或者上下文信息校验失败,针对没有包含上下文信息和上下文信息校验失败这两种不同情况,还可以发出不同类型的报警信息。

通过上述第一种可选的实施步骤,只有第一服务器判断数据访问请求中携带了账户上下文信息,和/或上下文信息通过校验的数据访问请求,才可以传送至第三方系统,确保了第三方系统接收到的数据访问请求均是由合法账户发出,保证了第三方系统根据数据访问请求访问数据源时,发起该数据访问请求的账户均是合法账户,进而保证了第三方系统接收到的数据访问请求的发起账户的安全性。

第二种可选的实施步骤中,第一服务器在确定数据访问请求中没有包含账户的上下文信息,或在账户的上下文信息校验失败的情况下,第一服务器发送数据访问请求至第三方系统。

本申请上述实施步骤中,即便第一服务器确定数据访问请求中没有包含账户的上下文信息,或账户的上下文信息校验失败,第一服务器依旧发送数据访问请求至第三方系统。此处需要说明的是,尽管第一服务器允许没有包含账户上下文信息的数据访问请求或者账户的上下文信息校验失败的数据访问请求发送至第三方系统,并不意味着第一服

务器可以不执行上述步骤 S202 至步骤 S206 提供的方案。

本申请上述实施例提供的一种可选方案中，在执行步骤 S202：第一服务器接收账户发起的数据访问请求之前，还可以执行如下实施步骤：

步骤 S2012：账户登录客户端之后，向登录服务器发起登录请求。

- 5 本申请上述步骤 S2012 中，客户端可以是软件产品，例如淘宝客户端、天猫客户端等软件，也可以是移动终端设备或计算机设备。在用户使用账户登录客户端时，开始向登陆服务器发起登陆请求，登陆服务器会计算生成该账户对应的完整上下文信息（即完整 Context 信息），同时登录服务器会存储该账户的账号密码信息和上述完整上下文信息。一种优选方案中，登录服务器接收到账户的登录请求后，可以首先判断接收到的登
10 录请求中携带的信息与登录服务器本地存储的账户信息是否匹配，在判断匹配的情况下，允许账户登录并生成完整上下文信息，在判断不匹配的情况下，拒绝账户登录。

仍旧以淘宝网的卖家实现订单管理功能为例，使用提供订单管理功能的第三方系统时，淘宝卖家首先需要登录淘宝客户端，淘宝卖家账户向登录服务器，例如淘宝服务器，发起登录请求，完成淘宝卖家账号的登录。

- 15 步骤 S2014：客户端接收登录服务器返回的上下文信息，其中，上下文信息为登录服务器根据登录请求生成的完整上下文信息中的子集。

本申请上述步骤 S2014 中，在登录服务器根据登录请求生成完整的上下文信息之后，登陆服务器会返回上下文信息（Context 信息）到客户端，此处的 Context 信息可以为登陆服务器生成的完整 Context 信息的子集。

- 20 此处需要说明的是，完整的上下文信息中可以包含指定的所有种类的账户信息。出于实际需求或登录服务器传输数据量考虑，登录服务器可以选择仅将完整上下文信息的其中一个子集返回至客户端，上下文信息包含但不限于用户的账户 ID，用户信息的某种变形处理算法结果等（例如采用 md5 等不可逆算法，对账户信息进行变换处理，得到对应的哈希值）。对于向客户端返回的是完整上下文信息中的哪一个子集，本申请实施例
25 不做限定。登录服务器向客户端返回的上下文信息可以采用明文传输，也可以采用密文传输。

- 通过上述步骤 S2014，登录服务器可以通过提取完整上下文信息中的必要信息，形成一个完整上下文信息的子集返回至客户端。在返回的上下文信息能满足第一服务器对于数据访问请求中是否携带上下文信息进行验证、和/或对包含的上下文信息是否正确进
30 行校验的需求的情况下，向客户端返回完整上下文信息的其中一个子集的方式能有效减

少登录服务器向客户端发送的信息量。在短时间内有大量用户向登录服务器发起登录请求的情况下，这种方式将能有效节约登录服务器的系统资源，减少登录服务器的数据传输负担。

仍旧以淘宝网的卖家实现订单管理功能为例，登录服务器（例如是淘宝服务器）中不仅存储了该淘宝卖家的用户名和用户密码信息，还存储了该淘宝卖家账户的例如账户的在线状态、账户的离线状态、账户的在线时间、账户的离线时间、账户的登录时间、账户的登录地点、账户的登录设备、账户访问用户数据的记录、账户的数据隐私安全等级、账户的常用登录设备、账户的常用登录地点、账户的账号安全状态以及账户的账号风险评估等信息。淘宝服务器向卖家账户返回信息时，淘宝服务器根据存储的卖家账户的信息，计算生成账户的完整上下文信息，并将生成的完整上下文信息中的其中一个子集返回至客户端。

步骤 S2016：客户端发送携带有上下文信息的数据访问请求至第一服务器。

本申请上述步骤 S2016 提供的方案，可以实现在客户端接收到登录服务器返回的上下文信息之后，当客户端发起数据访问请求时，会将上下文信息加载至数据访问请求中，一并发送给第一服务器。由此，当登录账户触发第三方系统发起数据访问请求（例如用户在浏览器中打开第三方系统网页产生的数据访问请求），均会生成包含该上下文信息的数据访问请求。

仍旧以淘宝网的卖家实现订单管理功能为例，当淘宝卖家在浏览器中打开提供订单管理功能的第三方系统时后，产生包含该淘宝卖家账户的数据访问请求数据访问请求，发送至第一服务器。该请求数据访问请求用于指示第三方系统访问淘宝提供的数据源服务器中该卖家账户用户数据的权限。

由上可知，本申请上述步骤 S2012 至步骤 S2016 提供了一种生成并将上下文信息发送至第一服务器的可选方案。基于上述步骤 S2012 发起登录请求，通过步骤 S2014 来接收由该登录请求触发后生成的上下文信息，在第三方系统需要访问数据源时，生成包含上下文信息的数据访问请求，并最终通过步骤 S2016 发送至第一服务器。

本申请上述实施例提供的一种可选方案中，在上述步骤 S2014：客户端接收登录服务器返回的上下文信息之前，还可以执行如下实施步骤：

步骤 S2013：登录服务器对账户信息进行加密，并根据加密后的数据生成上下文信息。

本申请上述步骤 S2013 中，上下文信息仍旧可以是登录服务器在生成的完整上下文

信息的子集。在生成上下文信息时，可以对用户账户信息进行加密，或者进行一次变换，例如采用 MD5 进行处理，根据加密后的密文信息或者变换后的数据生成上下文信息。通过上述步骤实现登录服务器与客户端之间信息的可靠传输，避免了本次用户上下文信息被窃取的可能性，同时，当加密或变换后的数据量小于原始信息的数据量时，在传输过程中还可以进一步节省系统资源，提高传输效率。例如，对上下文信息进行一次不可逆变换（比如进行 md5 等不可逆运算），得到对应的哈希值，由于哈希值的数据长度更小，使得登录服务器与客户端之间传输的数据不仅具有更高密级，且占用更少系统资源。

本申请上述实施例提供的一种可选方案中，上述步骤 S204：对账户的上下文信息进行校验可以包括如下至少两种具体的实施步骤，下面结合图 4 和图 5，分别对两种具体的实施步骤进行介绍：

本申请的第一服务器可以是图 3 所示的网关，如图 4 所示，本申请上述实施例提供的一种可选方案中，上述步骤 S204 中：对账户的上下文信息进行校验，第一种具体的实施步骤包括如下步骤 S402 至步骤 S406：

步骤 S402：第一服务器在确定数据访问请求中携带上下文信息之后，读取数据访问请求中携带的上下文信息。

本申请上述步骤 S402 中，第一服务器在接收到数据访问请求后，在确定数据访问请求中携带有至少看起来像是上下文信息的内容后，读取数据访问请求中携带的上下文信息。

步骤 S404：第一服务器将上下文信息与预存的完整上下文信息进行匹配，在匹配成功的情况下，确定账户的上下文信息为合法信息。

本申请上述步骤 S404 中，如本申请上述实施例中所述，合法帐户可以发出包含上下文信息的数据访问请求，伪造账户也可以冒充合法账户，发出包含看起来像是该合法账户的上下文信息的数据访问请求。因此，第一服务器在读取到上下文信息后，会将该上下文信息与预存的完整上下文信息进行匹配。预存的完整上下文信息，可以是存储的完整上下文信息，也可以是缓存的完整上下文信息。

在一种可能的情况下，结合图 4 可知，由于登录服务器中有完整上下文信息，可以将完整上下文信息固定存储在登录服务器中时，待到第一服务器执行将上下文信息与预存的完整上下文信息进行匹配的步骤时，第一服务器向登录服务器发出读取该完整上下文信息的请求，并接收登录服务器返回的完整上下文信息。

在另一种可能的情况下，结合图 4 可知，尽管登录服务器中有完整上下文信息，但

是每次第一服务器执行将上下文信息与预存的完整上下文信息进行匹配的步骤时，都向登录服务器发出读取该完整上下文信息的请求，会导致登录服务器的负担过重。因此，可以将完整上下文信息仅是缓存在登录服务器中，以便降低对于登录服务器的存储量的要求。在这种情况下，在登录服务器生成上下文信息并返回给客户端时，登录服务器还可以将完整上下文信息发送至第一服务器进行存储，待到第一服务器执行将上下文信息与预存的完整上下文信息进行匹配的步骤时，第一服务器读取本地存储的完整上下文信息。至于登录服务器将完整上下文信息发送给第一服务器后，登录服务器中的完整上下文信息是否要删除，本申请实施例中不做限定。

在又一种可能的情况下，结合图 4 可知，尽管登录服务器中有完整上下文信息，但是每次第一服务器执行将上下文信息与预存的完整上下文信息进行匹配的步骤时，都向登录服务器发出读取该完整上下文信息的请求，会导致登录服务器的负担过重。因此，可以将完整上下文信息仅是缓存在登录服务器中，以便降低对于登录服务器的存储量的要求。在这种情况下，可配置上下文信息服务器，在登录服务器生成上下文信息并返回给客户端时，登录服务器还可以将完整上下文信息发送至上下文信息服务器进行存储，待到第一服务器执行将上下文信息与预存的完整上下文信息进行匹配的步骤时，第一服务器向上下文信息服务器发出读取该完整上下文信息的请求，并接收上下文信息服务器返回的完整上下文信息。至于登录服务器将完整上下文信息发送给上下文信息服务器后，登录服务器中的完整上下文信息是否要删除，本申请实施例中不做限定。

针对登录服务器不执行上述步骤 S2013 和登录服务器执行上述步骤 S2013 和两种实施方案，在本申请上述步骤 S404 还可包括如下两种具体步骤：

在一种可选的实施方案中，登录服务器不执行上述步骤 S2013，即登录服务器没有对账户信息进行加密，那么步骤 S404：第一服务器将上下文信息与预存的完整上下文信息进行匹配的具体步骤还包括：第一服务器从预存的完整上下文信息提取与上下文信息对应的信息类型和数据内容，第一服务器通过判断提取到的数据与第一服务器读取到的上下文信息是否匹配，就可以得出第一服务器读取到的上下文信息与预存的完整上下文信息是否匹配的结果。

在另一种可选的实施方案中，登录服务器执行上述步骤 S2013，即登录服务器对账户信息进行加密或变换，并根据加密后或变换后的数据生成上下文信息；那么步骤 S404：第一服务器将上下文信息与预存的完整上下文信息进行匹配的具体步骤还包括如下两种方式：

在第一种方式中，第一服务器从预存的完整上下文信息提取与上下文信息对应的信息类型和数据内容，并对提取后的数据进行加密，其中，第一服务器对提取后的数据进行加密算法与步骤 S2013 中登录服务器所执行的加密算法相同或相应。此后，第一服务器可以通过判断加密后得到的数据与第一服务器读取到的上下文信息是否匹配，就可以得出第一服务器读取到的上下文信息与预存的完整上下文信息是否匹配的结果。

在第二种方式中，在第一服务器执行将上下文信息与预存的完整上下文信息进行匹配的步骤时，第一服务器向上下文信息服务器发出匹配认证请求，该匹配认证请求中包含了第一服务器读取到的上下文信息；上下文信息服务器接收第一服务器发来的上下文信息，并且，上下文信息服务器从预存在本地的完整上下文信息中提取与第一服务器发来的上下文信息对应的信息类型和数据内容，并对提取后的数据进行加密。其中，上下文信息服务器对提取后的数据进行加密算法与步骤 S2013 中登录服务器所执行的加密算法相同或相应。此后，上下文信息服务器可以通过判断加密后得到的数据与上下文信息服务器接收到的由第一服务器转发来的上下文信息是否匹配，就可以得出第一服务器转发来的上下文信息与预存在本地的完整上下文信息是否匹配的结果。上下文信息服务器将该结果返回给第一服务器。

步骤 S406：第一服务器生成账户的合法访问标识信息，其中，合法访问标识信息用于表征发起数据访问请求的账户为合法账户。

本申请上述步骤 S406 中，合法访问标识信息由第一服务器生成，表示该数据访问请求经第一服务器验证通过。对于伪造账户冒充合法账户的情况，伪造账户冒充合法账户发出的数据访问请求无法通过第一服务器验证，即伪造账户无法被第一服务器认定为是合法账户，由于伪造账户发起的数据访问请求中没有携带上下文信息，因此，第一服务器不会透传伪造账户发出的数据访问请求，进而不会为伪造账户发起的数据访问请求生成一个合法访问标识信息。

此处需要说明的是，在本申请上述实施例中，第一服务器可以仅允许通过验证的数据访问请求发送至第三方系统；第一服务器也可以允许未通过验证的数据访问请求发送至第三方系统。此时，合法访问标识信息就可以用于标识第一服务器的验证结果，具有合法访问标识信息的数据访问请求所对应的账户为合法账户。

此处还需要说明的是，第一服务器在确定账户的上下文信息为合法信息后，可以通过更新用户上下文信息中特定的元素数据来实现上述步骤 S406，在这种情况下，更新后的元素数据可视为合法访问标识信息。

由上可知，本申请上述步骤 S402 至步骤 S406 提供了一种第一服务器对账户的上下文信息进行校验的可选方案。第一服务器读取访问请求中包含的账户上下文信息，并判断上下文信息与预存的完整上下文信息是否匹配，在匹配成功的情况下，确定账户的上下文信息为合法信息，并生成账户的合法访问标识信息。

5 本申请上述实施例提供的一种可选方案中，如图 5 所示，上述步骤 S204 中：对账户的上下文信息进行校验，第二种具体的实施步骤包括如下步骤 S502 至步骤 S506：

 步骤 S502：第一服务器在确定数据访问请求中携带上下文信息之后，发送上下文信息至上下文信息服务器。

 本申请上述步骤 S502 中，第一服务器在接收到数据访问请求后，在确定数据访问请求中携带有至少看起来像是上下文信息的内容后，读取数据访问请求中携带的上下文信息，并将该数据访问请求中上下文信息发送至上下文信息服务器。

10

 步骤 S504：第一服务器接收上下文信息服务器验证上下文信息的验证结果。

 此处需要说明的时，在本申请上述步骤 S504 之前，登录服务器生成上下文信息并返回给客户端时，登录服务器还将完整上下文信息发送至上下文信息服务器进行存储。并且，上下文信息服务器将通过上述步骤 S502 接收到的上下文信息与预存在本地的完整上下文信息进行匹配，在匹配成功的情况下，验证结果为账户的上下文信息为合法信息，上下文信息服务器将验证结果再返回至第一服务器后，第一服务器执行上述步骤 S504。

15

 针对登录服务器不执行上述步骤 S2013 和登录服务器执行上述步骤 S2013 和两种实施方案，在本申请上下文信息服务器将上下文信息与预存在本地的完整上下文信息进行匹配的具体步骤还可包括如下两种具体步骤：

20

 在第一种实施方案中，登录服务器不执行上述步骤 S2013，即登录服务器没有对账户信息进行加密，那么上下文信息服务器将上下文信息与预存在本地的完整上下文信息进行匹配的具体步骤包括：上下文信息服务器从预存在本地的完整上下文信息中提取与第一服务器发来的上下文信息对应的信息类型和数据内容，上下文信息服务器通过判断提取到的数据与第一服务器发来的上下文信息是否匹配，就可以得出第一服务器发来的上下文信息与预存在本地的完整上下文信息是否匹配的结果。

25

 在第二种实施方案中，登录服务器执行上述步骤 S2013，即登录服务器对账户信息进行加密或变换，并根据加密后或变换后的数据生成上下文信息；那么第一服务器读取到的上下文信息是根据加密后的数据生成的，此时，那么上下文信息服务器将上下文信息与预存在本地的完整上下文信息进行匹配的具体步骤包括：上下文信息服务器从预存

30

在本地的完整上下文信息中提取与第一服务器发来的上下文信息对应的信息类型和数据内容，并对提取后的数据进行加密。其中，上下文信息服务器对提取后的数据进行加密算法与步骤 S2013 中登录服务器所执行的加密算法相同或相应。此后，上下文信息服务器可以通过判断加密后得到的数据与上下文信息服务器接收到的由第一服务器转发来的上下文信息是否匹配，就可以得出第一服务器转发来的上下文信息与预存在本地的完整上下文信息是否匹配的结果。上下文信息服务器将该结果返回给第一服务器。

步骤 S506：在验证结果为账户的上下文信息为合法信息的情况下，第一服务器接收上下文信息服务器生成的账户的合法访问标识信息，其中，合法访问标识信息用于表征发起的数据访问请求的账户为合法账户。

本申请上述步骤 S506 中，合法访问标识信息由上下文信息服务器生成，表示该数据访问请求经上下文服务器验证通过。对于伪造账户冒充合法账户的情况，伪造账户冒充合法账户发出的数据访问请求无法通过上下文服务器的验证，即伪造账户无法被上下文服务器认定为是合法账户，伪造账户不可能具有上下文服务器生成的合法访问标识信息。上下文信息服务器将生成的合法访问标识信息发送至第一服务器，第一服务器可以根据接收到的合法访问标识信息，控制是否允许数据访问请求发送至第三方系统。

此处需要说明的是，第一服务器在接收到上下文信息服务器发来的合法访问标识信息后，可以通过更新存储于第一服务器中的用户上下文信息中特定的元素数据，来实现第一服务器存储合法访问标识信息。

由上可知，本申请上述步骤 S502 至步骤 S506 提供了一种第一服务器对账户的上下文信息进行校验的可选方案。第一服务器将读取到的账户上下文信息发送至上下文信息服务器，由上下文信息服务器完成上下文信息的匹配认证工作，并在匹配成功的情况下，确定账户的上下文信息为合法信息，并生成账户的合法访问标识信息发给第一服务器。第一服务器通过接收上下文信息服务器发来的合法访问标识信息，实现了第一服务器对账户的上下文信息进行校验。

由上可知，对于上述步骤 S204：对账户的上下文信息进行校验包含两种具体的实施步骤，在步骤 S402 至步骤 S406 所提供的第一种具体的实施步骤中，第一服务器完成了获取数据访问请求中携带的上下文信息，并完成上下文信息与预存的完整上下文信息是否匹配的判断，并针对匹配成功的账户生成合法访问标识信息，即认定该账户为合法账户。在步骤 S502 至步骤 S506 所提供的第二种具体的实施步骤中，上下文信息服务器通过接收第一服务器获取的数据访问请求中携带的上下文信息，完成上下文信息与预存在

本地的完整上下文信息是否匹配的判断，针对匹配成功的账户生成合法访问标识信息，即认定该账户为合法账户，并将该合法访问标识信息返回至第一服务器。上述两种具体实施步骤均可以实现对账户的上下文信息进行校验，第一种具体实施步骤由第一服务器完成，在数据处理上更具便捷性，第二种具体实施步骤由上下文信息服务器完成，可以有效分担第一服务器的数据处理任务，提高数据处理效率。

本申请上述实施例提供的可选方案中，在步骤 S206：允许发送数据访问请求至第三方系统之后，还可以包括如下实施步骤：

步骤 S207：数据源服务器接收第三方系统转发的数据访问请求；

本申请上述步骤 S207 中，第三方系统接收到第一服务器发送来的数据访问请求后，
10 第三方系统将数据访问请求转发至数据源服务器，数据访问请求用于指示第三方系统请求获取数据源中存储的合法账户的用户数据。

步骤 S208：数据源服务器访问第一服务器或上下文信息服务器，如果查询得到账户的合法访问标识信息，则确定合法账户发起的数据访问请求为安全访问请求；

此处需要说明的时，在上述步骤 S204 提供的具体实施步骤中，账户的合法访问标识
15 信息可由第一服务器生成并存储于第一服务器中，也可由上下文信息服务器生成并存储与第一服务器中，还可由上下文信息服务器生成并存储与上下文信息服务器中。因此，本申请上述步骤 S208 中，数据源服务器在查询账户的合法访问标识信息时，对于账户的合法访问标识信息由第一服务器生成的情况，数据源服务器访问第一服务器查询是否具有账户的合法访问标识信息；对于账户的合法访问标识信息由上下文信息服务器生成的
20 情况，数据源服务器访问第一服务器或者上下文信息服务器查询是否具有账户的合法访问标识信息。对于能够查询到合法访问标识信息的账户，数据源服务器认定该账户发起的数据访问请求为安全访问请求。

此处还需要说明的是，对于第一服务器仅允许通过校验的数据访问请求发送至第三方系统和第一服务器允许所有数据访问请求发送至第三方系统这两种情况，在步骤 S208
25 中有不同的处理方式。对于第一服务器仅允许通过校验的数据访问请求发送至第三方系统的情况，第三方系统接收并转发的数据访问请求通过了第一服务器的验证且具有合法访问标识信息，那么第一服务器就可以实现屏蔽伪造账户冒充合法账户发起的数据访问请求的技术效果。对于第一服务器允许所有数据访问请求发送至第三方系统的情况，第三方系统接收并转发的数据访问请求可能通过校验并具有合法访问标识信息，也可能没有通过校验且没有合法访问标识信息，那么数据源服务器就需要执行上述步骤 S208 来鉴
30

别发出数据访问请求的账户是否为合法账户，当查询不到合法访问标识信息时，数据源服务器可以确定该数据访问请求不是安全访问请求，并拒绝提供该数据访问请求所要访问的数据。

通过本申请上述步骤 S208，实现了数据源服务器识别接收到的数据访问请求是否是由合法账户发起的。并且进一步的，当第三方系统受到攻击时，第三方系统转发的数据访问请求可能被盗取，并在用户没有操作的情况下生成数据访问请求来冒充合法账户时，数据源服务器就可以向数据访问请求的源头进行追溯，通过查询第一服务器或上下文信息服务器是否具有合法访问标识信息，来判断该数据访问请求是否由合法用户发起的。

步骤 S209：数据源服务器向第三方系统返回数据访问请求所要访问的数据。

本申请上述步骤 S209 中，当数据源服务器确定数据访问请求为安全访问请求后，数据源服务器向第三方系统返回该数据访问请求所要访问的数据。数据源服务器通过查询是否具有账户的合法访问标识信息，实现了判断数据访问请求是否是由合法账户发起的效果，避免恶意账户通过冒充合法账户数据访问请求读取用户数据的不良后果。

由上可知，通过本申请上述实施例中步骤 S207 至步骤 S209 提供的可选方案，实现了数据源服务器对发起数据访问请求的账户进行鉴别的技术效果。进一步的，当第三方系统收到攻击时，即便第三方系统中存储的用户上下文信息被伪造账户利用，数据源服务器还可以通过查询位于第三方系统上游的第一服务器或者上下文信息服务器中是否具有账户的合法访问标识信息，有效识别数据访问请求是由合法用户发出还是由第三方系统伪造，进一步的保证了用户数据的安全。

此处还需要说明的是，上述账户的上下文信息（Context 信息）可以决定第三方系统是否能获取以及能获取多高权限等级的用户数据。其中，高等级数据一般涉及用户隐私，例如用户手机号码，家庭住址，甚至信用卡信息等，低等级数据一般不涉密，例如用户昵称，用户头像信息等，一般可以根据涉及用户隐私程度分若干等级。由于账户对应的上下文信息可以校验客户端账户发起的数据访问请求是否由合法用户发起，如果不是，第三方系统将无法获得用户数据，这样就有效的防止了当第三方系统被黑客入侵或者人为原因，用户数据被恶意读写的问题，用户数据安全性大大提高。

进一步地，在本申请上述实施例提供的一种可选方案中，在执行步骤 S208：确定发起数据访问请求的账户为安全访问账户之后，还可以执行如下实施步骤：

步骤 S2082：数据源服务器验证上下文信息中是否包含账户的在线信息；

本申请上述步骤 S2082 中，上下文信息中可以包含账户的在线信息，当通过技术手

段探测到账户在线后，生成账户在线信息，并将账户在线信息添加至上下文信息中。例如，可以通过向客户端定时发送心跳包的机制，根据客户端反馈的消息，判断账户是否在线，该判断账户是否在线的步骤可以由登录服务器执行。

步骤 S2084：当上下文信息中包含账户的在线信息时，数据源服务器执行向第三方系统返回数据访问请求所要访问的数据的步骤。

本申请上述步骤 S2084 中，当上下文信息中包含账户在线信息时，意味着当前账户在线，此时数据源服务器才执行步骤 S209：数据源服务器向第三方系统返回数据访问请求所要访问的数据。

本申请上述实施例提供的可选方案中，根据上下文信息中还包含的其他信息，步骤 S209：数据源服务器向第三方系统返回数据访问请求所要访问的数据，具体的实施步骤包括至少如下两种方式：

在第一种方式中，当上下文信息中还包括账户的安全隐私等级信息时，步骤 S209：数据源服务器向第三方系统返回数据访问请求所要访问的数据的步骤包括：

步骤 S2092：数据源服务器根据安全隐私等级信息生成对应的第一访问数据，并将第一访问数据返回至第三方系统。

本申请上述步骤 S2092 中，安全隐私等级信息是针对不同的第三方系统，根据对第三方系统的信任程度不同，以及用户对第三方系统的授权程度不同，可以开放给第三方系统不同隐私程度的用户数据的标识信息。例如当安全隐私等级信息指示数据访问请求具有较高安全等级，例如第一安全等级，时，第一访问数据中可以包含第一安全等级所对应的信息，例如，用户的邮箱信息、用户的手机号码、或者用户的地址信息等；当安全隐私等级信息指示数据访问请求具有较低安全等级，例如第二安全等级，时，第一访问数据中可以包含第二安全等级所对应的信息，例如，用户的昵称信息、用户的头像信息等。

在第二种方式中，当上下文信息中还包括账户的安全风险状态信息时，步骤 S209：数据源服务器向第三方系统返回数据访问请求所要访问的数据的步骤包括：

步骤 S2094：数据源服务器安全风险状态信息生成对应的第二访问数据，并将第二访问数据返回至第三方系统。

本申请上述步骤 S2094 中，安全风险状态信息是用于表征账户目前的风险状态的信息。例如，当安全风险状态信息指示账户处于较高风险状态时，例如第一风险状态时，第二访问数据中仅能包含第一风险状态所对应的信息，例如，用户的昵称信息、用户的

头像信息等。当安全风险状态信息指示账户处于较低风险状态时，例如第二风险状态时，第二访问数据中能包含第二风险状态所对应的信息，例如，用户的支付信息、用户的手机号码、或者用户的地址信息等。判断账户的风险状态时，可以考虑账户是否在可信地点登陆或者账户是否使用可信设备登陆等；账户的风险状态可以划分为例如：高安全风险，疑似风险状态，可信任状态等区域。安全风险状态信息可以由登录服务器生成。通过账户上下文信息中包括的账户安全风险状态信息，可以使得数据源服务器进一步控制数据的开放程度。

基于上述实施例一提供的方案可知，本申请提供的用户数据的访问控制方法关键在于在账户发起的数据访问请求中加载该账户的上下文信息，从而使得在账户使用第三方系统访问数据源时，可以保证账户为安全账户，且发起的数据访问请求也是安全请求，此处需要说明的是，本申请涉及到的第三方系统为非可控区域，第一服务器、数据源服务器、登录服务器为可控区域。

下面就结合图 6，将本申请的方案应用在实际场景所实现的功能进行详细描述：

步骤 A：客户端发起登录请求。

在本申请上述步骤 A 中，账户登录客户端，向登录服务器发起登录请求。客户端可以是软件产品，例如淘宝客户端、天猫客户端等软件，也可以是移动终端设备或计算机设备。登录服务器中存储了账户的账号密码信息和账户完整上下文信息。以淘宝网的卖家实现订单管理功能为例，使用提供订单管理功能的第三方系统时，淘宝卖家首先需要登录淘宝客户端，淘宝卖家账户向登录服务器，例如淘宝服务器，发起登录请求，完成淘宝卖家账号的登录。

步骤 B：登录服务器生成上下文信息。

在本申请上述步骤 B 中，上下文信息或称为 context 信息。登录服务器还会根据登录请求，生成完整的上下文信息。完整的上下文信息中包含了指定的所有种类的账户信息。出于实际需求或登录服务器传输数据量考虑，登录服务器可以选择仅将完整上下文信息的其中一个子集返回至客户端。仍旧以淘宝网的卖家实现订单管理功能为例，登录服务器（例如是淘宝服务器）中不仅存储了该淘宝卖家的用户名和用户密码信息，还存储了该淘宝卖家账户的例如账户的在线状态、账户的离线状态、账户的在线时间、账户的离线时间、账户的登录时间、账户的登录地点、账户的登录设备、账户访问用户数据的记录、账户的数据隐私安全等级、账户的常用登录设备、账户的常用登录地点、账户的账号安全状态以及账户的账号风险评估等信息。淘宝服务器向卖家账户返回信息时，淘宝

服务器根据存储的卖家账户的信息，计算生成账户的完整上下文信息。

步骤 C：登录服务器将上下文信息返回至客户端。

在本申请上述步骤 C 中，仍旧以淘宝网的卖家实现订单管理功能为例，淘宝服务器在收到登录请求后生成完整上下文信息，将生成的完整上下文信息中的其中一个子集返回至客户端。

步骤 D：客户端生成包含上下文信息的数据访问请求。

在本申请上述步骤 D 中，客户端接收登录服务器返回的上下文信息。账户每一次触发第三方系统，均会生成包含该上下文信息的数据访问请求。仍旧以淘宝网的卖家实现订单管理功能为例，由于淘宝网没有提供订单管理的功能，此时淘宝网通过提供一个接口实现授权独立软件提供商提供一个可以提供订单管理功能的第三方系统，因此，淘宝网的卖家账户在点击第三方系统提供的订单管理平台时，生成包含该卖家账户上下文信息的数据访问请求，用于给予该订单管理平台获取该卖家账户的用户数据的权限。卖家账户的用户数据存储于淘宝提供的数据源服务器中。

步骤 E：客户端发送数据访问请求至第一服务器。

步骤 F：第一服务器验证数据访问请求中是否携带上下文信息；

在本申请上述步骤 F 中，第一服务器在接收到数据访问请求后，验证数据访问请求中是否携带有至少看起来像是上下文信息的内容。仍旧以淘宝网的卖家实现订单管理功能为例，第一服务器接收到的该卖家账户的数据访问请求，可能是该真实的淘宝网卖家通过打开订单管理平台而发出发出的，也可能是伪造账户冒充该卖家账户发出的。第一服务器事先并不知道收到的数据访问请求的发起账户是否合法。然后，只有接收到登录服务器返回上下文信息的账户，在其发出的数据访问请求中才可能包含上下文信息。此时，第一服务器首先验证该数据访问请求中是否包含了上下文信息，来判断数据访问请求的发起账户。

步骤 G：第一服务器发送上下文信息至上下文信息服务器。

在本申请上述步骤 F 中，第一服务器验证数据访问请求中携带了上下文信息的情况下，读取数据访问请求中携带的上下文信息，并将该上下文信息发送至上下文信息服务器。第一服务器可以自己完成上下文信息是否合法的校验工作，第一服务器也可以委托上下文信息服务器来完成上下文信息是否合法的校验工作。在本交互示意图中，上下文信息服务器来完成上下文信息是否合法的校验工作。仍旧以淘宝网的卖家实现订单管理功能为例，第一服务器验证该数据访问请求中包含了上下文信息后，读取该上下文信息

的内容，并将该淘宝账户的上下文信息发送至上下文信息服务器。

步骤 H：上下文信息服务器对上下文信息进行校验。

在本申请上述步骤 H 中，上下文信息服务器将接收到的上下文信息与预存在本地的完整上下文信息进行匹配，在匹配成功的情况下，验证结果为账户的上下文信息为合法信息。上下文信息服务器中预存的完整上下文信息，是由登录服务器发送来并存储于上下文信息服务器中的信息。仍旧以淘宝网的卖家实现订单管理功能为例，上下文信息服务器对接收到的上下文信息进行校验，当上下文信息与预存在上下文信息服务器中的完整上下文信息匹配通过后，上下文信息服务器认为该上下文信息为合法信息。对于伪造账户冒充该卖家账户发出的数据访问请求，即使包含看起来像是上下文信息的数据，也无法通过上下文信息服务器的校验。

步骤 I：返回合法访问标识信息。

在本申请上述步骤 I 中，上下文信息服务器校验上下文信息通过的情况下，生成合法访问标识信息，并将合法访问标识信息返回至第一服务器。仍旧以淘宝网的卖家实现订单管理功能为例，在上下文信息服务器认为该上下文信息为合法信息后，上下文信息服务器生成合法访问标识，表示该数据访问请求是由真实的卖家账户发起，且携带的上下文信息无误。

步骤 J：允许发送数据访问请求至第三方系统。

在本申请上述步骤 J 中，第一服务器接收上下文信息服务器返回的合法访问标识信息，并允许将数据访问请求发送至第三方系统。仍旧以淘宝网的卖家实现订单管理功能为例，第一服务器接收到合法访问标识信息后，存储该合法访问标识信息，并且允许该数据访问请求透传至订单管理平台。

步骤 K：转发数据访问请求。

在本申请上述步骤 K 中，第三方系统接收到第一服务器发送来的数据访问请求后，第三方系统将数据访问请求转发至数据源服务器，数据访问请求用于指示第三方系统请求获取数据源中存储的合法账户的用户数据。仍旧以淘宝网的卖家实现订单管理功能为例，当订单管理平台接收到数据访问请求后，订单管理平台就将数据访问请求转发至数据源服务器，用于向数据源服务器申请读取该数据访问请求所要指的数据。例如是该淘宝卖家在过去一个月的订单成交金额、成交对象等。

步骤 L：数据源服务器查询是否存在合法访问标识信息；

在本申请上述步骤 L 中，账户的合法访问标识信息可由第一服务器生成并存储于第

一服务器中，也可由上下文信息服务器生成并存储与第一服务器中；数据源服务器访问第一服务器查询是否具有账户的合法访问标识信息。仍旧以淘宝网的卖家实现订单管理功能为例，如果淘宝提供的数据源服务器不对发送来的数据访问请求进行验证，去响应每一条数据访问请求，那么当第三方系统被入侵时，便难以保证存储于数据源服务器中

5 用户数据的安全。因此，数据源服务器会再次进行验证工作，此时，验证的主要途径是查询是否存在合法访问标识信息。

步骤 M：第一服务器向数据源服务器返回合法访问标识信息查询结果；

步骤 N：在数据源服务器查询到合法访问标识信息的情况下，确定数据访问请求为安全访问请求。

10 在本申请上述步骤 N 中，数据源服务器访问第一服务器或者上下文信息服务器查询是否具有账户的合法访问标识信息。对于能够查询到合法访问标识信息的账户，数据源服务器认定该账户发起的数据访问请求为安全访问请求。仍旧以淘宝网的卖家实现订单管理功能为例，当数据源服务器查询到第一服务器中具有该淘宝账户的合法访问标识信息时，可认为该淘宝账户主动发出了数据访问请求，且该数据访问请求中包含的上下文

15 信息经校验无误，此时，数据源服务器进一步对该上下文信息是否为合法信息进行校验。此时，数据源服务器确定该数据访问请求为安全访问请求。

步骤 O：数据源服务器向第三方系统返回数据访问请求所要访问的数据。

在本申请上述步骤 O 中，数据源服务器在确认该数据访问请求为安全访问请求后，还可以进一步判断用户是否在线。在判断出用户在线的情况下，获取数据访问请求中可能包含的安全隐私等级或者安全风险状态，来判断能够向第三方系统返回的数据内容。

20 仍旧以淘宝网的卖家实现订单管理功能为例，数据源服务器对于确定为安全访问请求的数据访问请求，向订单管理平台返回该数据访问请求所要求访问的数据。

综上可知，本申请提供的实施例一可以实现如下技术效果：

1、由于数据访问请求中携带的 Context 信息是一种非固定值，因此，非法的黑客无法盗取，从而避免了用户的某些固定值的授权令牌等被盗引起的数据泄密问题。

25

2、在非法用户 B 尝试访问合法用户 A 的数据的应用场景中，由于 Context 信息需要账户登录客户端，登录服务器才会生成该账户的上下文信息，由于非法用户 B 无法在网

30 源服务器校验 Context 信息后，由于查询不到合法用户 A 的访问记录，因此，系统

可以认定当前的账户以及发起的数据访问请求将会被数据源拒绝。

3、非可控的第三方系统被恶意控制或人为原因恶意操作的场景中，虽然黑客有可能获取到第三方系统上维护的所有用户列表，甚至用户授权的信息，同样因为不满足 Context 信息的校验，将会被数据源拒绝掉。

5 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请并不受所描述的动作顺序的限制，因为依据本申请，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本申请所必须的。

10 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。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介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可
15 以是手机，计算机，服务器，或者网络设备等）执行本申请各个实施例所述的方法。

实施例二

根据本申请实施例，还提供了一种用户数据的访问控制方法的方法实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中
20 执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

本申请实施例二所提供的方法实施例仍旧可以在移动终端、计算机终端或者类似的运算装置中执行。此处需要说明的是，实施例二所提供的方法实施例仍旧可以运行在图 1 所示的计算机终端上。

25 以在上述运行环境下为，本申请还可以提供如图 7 所示的用户数据的访问控制方法。图 7 是根据本申请实施例二的用户数据的访问控制方法的流程示意图。如图 7 所示，一种可选的用户数据的访问控制方法包括如下实施步骤：

步骤 S602：客户端获取账户的上下文信息。

步骤 S604：客户端发送账户触发的数据访问请求至第一服务器，其中，数据访问请
30 求至少包括上下文信息。

本申请上述步骤 S602 中，账户可以是客户端注册的合法账户。其中，该合法账户登录的客户端可以不限于淘宝、天猫等产品，用户可以在该客户端上注册账户，每个用户使用账户登录客户端之后，可以通过使用该客户端发起上述数据访问请求。

此处需要说明的是，上述第一服务器可以为图 3 中所示的一种网关，此处的网关用于透传所述数据访问请求。一种可选方案中，上述第一服务器可以是阿里云的负载均衡服务器。

步骤 S606：客户端接收第一服务器根据数据访问请求获取到的访问数据；其中，在第一服务器确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源。

本申请上述步骤 S606 中涉及到的上下文信息与账户的活动状态和活动信息相关，用于表征该上下文信息对应的账户赋予第三方系统访问该账户用户数据的权限。在本申请实施例中，上下文信息可以包括但不限于账户的在线状态、账户的离线状态、账户的在线时间、账户的离线时间、账户的登录时间、账户的登录地点、账户的登录设备、账户访问用户数据的记录、账户的数据隐私安全等级、账户的常用登录设备、账户的常用登录地点、账户的账号安全状态以及账户的账号风险评估等信息。

本申请提供的上述步骤可以实现通过对接收到的数据访问请求中是否携带有上下文信息和/或账户的上下文信息进行校验，来确定发起该数据访问请求的账户是否是合法账户。从上述上下文信息包含的信息种类来看，上下文信息是一种具有非固定值，且黑客无法盗取等特性的数据，因此，采用基于上下文信息来验证账户是否合法具有较高的可信度。本申请这种引入上下文检查机制的方案，可以使得账户的验证结果更加准确，具体的，可以有效解决在用户授权允许的的时间内，用户数据被随意访问的问题。

由于在数据访问请求中包含了账户的上下文信息，和/或该上下文信息是合法信息的情况下，可以确定当前的账户为安全账户，因此，第一服务器（可以是图 3 所示的网关）将允许安全账户发起的数据访问请求透传至第三方系统，进入第三方系统中处理该数据访问请求，即第三方系统根据接收到的数据访问请求访问数据源，向数据源请求该用户的数据。

可选的，第三方系统可以通过向数据源服务器转发该数据访问请求的方式，请求访问存储于数据源服务器中的用户数据，然后，数据源服务器将根据该数据访问请求读取到的用户数据返回至第三方系统。

由上可知，本申请上述实施例二所提供的方案中，当前账户（可以是合法账户或者伪造账户冒充该合法账户）发出数据访问请求到达第一服务器后，第一服务器会对接收到的每一个数据访问请求进行校验，即第一服务器会判断数据访问请求是否携带账户上下文信息，和/或上下文信息是否能够校验通过，当对数据访问请求的校验通过的情况下，

5 第一服务器允许该数据访问请求发送至第三方系统，进而第三方系统就可以根据该数据访问请求访问数据源。在上述方案中，只有合法账户发起的数据访问请求能够通过校验，而对于冒充合法账户的恶意账户发起的数据访问请求，要么在形式上不携带账户上下文信息，要么在内容上携带的上下文信息不能通过校验。通过上述方案，实现了允许具有访问权限的合法账户发起的数据访问请求发送至第三方系统，解决了现有技术在使用

10 使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

本申请上述实施例提供的可选方案中，在步骤 S602：客户端获取登录账户的上下文信息之后，还可以执行如下实施步骤：

步骤 S6032：账户登录客户端之后，向登录服务器发起登录请求。

15 本申请上述步骤 S6032 中，客户端可以是软件产品，例如淘宝客户端、天猫客户端等软件，也可以是移动终端设备或计算机设备。在用户使用账户登录客户端是，开始向登陆服务器发起登陆请求，登陆服务器会计算生成该账户对应的完整上下文信息（即完整 Context 信息），同时登录服务器会存储该账户的账号密码信息和上述完整上下文信息。一种优选方案中，登录服务器接收到账户的登录请求后，可以首先判断接收到的登

20 录请求中携带的信息与登录服务器本地存储的账户信息是否匹配，在判断匹配的情况下，允许账户登录并生成完整上下文信息，在判断不匹配的情况下，拒绝账户登录。

步骤 S6034：客户端接收登录服务器返回的上下文信息，其中，上下文信息为登录服务器根据登录请求生成的完整上下文信息中的子集。

通过上述步骤，登录服务器可以通过提取完整上下文信息中的必要信息，形成一个

25 完整上下文信息的子集返回至客户端。在返回的上下文信息能满足第一服务器对于数据访问请求中是否携带上下文信息进行验证、和/或对包含的上下文信息是否正确进行校验的需求的情况下，向客户端返回完整上下文信息的其中一个子集的方式能有效减少登录服务器向客户端发送的信息量。在短时间内有大量用户向登录服务器发起登录请求的情况下，这种方式将能有效节约登录服务器的系统资源，减少登录服务器的数据传输负担。

30 此处需要说明的是，本申请上述实施例二中步骤 S6032 至步骤 S6034 所提供的优选

实施方案与实施例一中步骤 S2012 到步骤 S2014 所提供的优选方案以及应用场景实施过程相同，但不限于实施例一所提供的方案。

本申请上述实施例提供的一种可选方案中，在步骤 S6032：账户登录客户端之后，还可以包括如下实施步骤：登录服务器接收登录请求，生成发起登录请求的账户的完整
5 上下文信息，将完整上下文信息的其中一个子集返回给客户端；并将完整上下文信息发送给第一服务器和/或上下文信息服务器。

本申请上述实施例提供的一种可选方案中，在步骤 S604：客户端发送账户触发的数据访问请求至第一服务器之后，还可以包括如下实施步骤：

步骤 S6052：第一服务器接收账户发起的数据访问请求。

10 步骤 S6054：第一服务器验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验。

步骤 S6056：第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源。

15 另一种可选方案中，第一服务器在确定数据访问请求中没有包含账户的上下文信息，或在账户的上下文信息校验失败的情况下，第一服务器发送数据访问请求至第三方系统，或者第一服务器禁止发送数据访问请求至第三方系统，并发出报警信息。

本申请上述实施例提供的可选方案中，步骤 S6054：对账户的上下文信息进行校验的具体步骤包括：

20 步骤 S60541：第一服务器在确定数据访问请求中携带上下文信息之后，读取数据访问请求中携带的上下文信息；

步骤 S60542：第一服务器将上下文信息与预存的完整上下文信息进行匹配，在匹配成功的情况下，确定账户的上下文信息为合法信息；

25 步骤 S60543：第一服务器生成账户的合法访问标识信息，其中，合法访问标识信息用于表征发起数据访问请求的账户为合法账户。

此处需要说明的是，本申请上述实施例二中步骤 S60541 至步骤 S60543 所提供的优选实施方案与实施例一中步骤 S402 到步骤 S406 所提供的优选方案以及应用场景实施过程相同，但不限于实施例一所提供的方案。

30 本申请上述实施例提供的可选方案中，步骤 S6054：对账户的上下文信息进行校验的具体步骤包括：

步骤 S60545: 第一服务器在确定数据访问请求中携带上下文信息之后, 发送上下文信息至上下文信息服务器;

步骤 S60546: 第一服务器接收上下文信息服务器验证上下文信息的验证结果;

步骤 S60547: 在验证结果为账户的上下文信息为合法信息的情况下, 第一服务器接收上下文信息服务器生成的账户的合法访问标识信息, 其中, 合法访问标识信息用于表征发起的数据访问请求的账户为合法账户;

其中, 上下文信息服务器将上下文信息与预存在本地的完整上下文信息进行匹配, 在匹配成功的情况下, 验证结果为账户的上下文信息为合法信息。

此处需要说明的是, 本申请上述实施例二中步骤 S60545 至步骤 S60547 所提供的优选实施方案与实施例一中步骤 S502 到步骤 S506 所提供的优选方案以及应用场景实施过程相同, 但不限于实施例一所提供的方案。

本申请上述实施例提供的可选方案中, 在步骤 S6056: 允许发送数据访问请求至第三方系统之后, 还可以包括如下实施步骤:

步骤 S60572: 数据源服务器接收第三方系统转发的数据访问请求;

步骤 S60574: 数据源服务器访问第一服务器或上下文信息服务器, 如果查询得到账户的合法访问标识信息, 则确定合法账户发起的数据访问请求为安全访问请求;

步骤 S60576: 数据源服务器向第三方系统返回数据访问请求所要访问的数据。

此处需要说明的是, 本申请上述实施例二中步骤 S60572 至步骤 S60576 所提供的优选实施方案与实施例一中步骤 S207 到步骤 S209 所提供的优选方案以及应用场景实施过程相同, 但不限于实施例一所提供的方案。

此处还需要说明的是, 上述账户的上下文信息 (Context 信息) 可以决定第三方系统是否能获取以及能获取多高权限等级的用户数据。其中, 高等级数据一般涉及用户隐私, 例如用户手机号码, 家庭住址, 甚至信用卡信息等, 低等级数据一般不涉密, 例如用户昵称, 用户头像信息等, 一般可以根据涉及用户隐私程度分若干等级。由于账户对应的上下文信息可以校验客户端账户发起的数据访问请求是否由合法用户发起, 如果不是, 第三方系统将无法获得用户数据, 这样就有效的防止了当第三方系统被黑客入侵或者人为原因, 用户数据被恶意读写的问题, 用户数据安全性大大提高。

本申请上述实施例提供的可选方案中, 在步骤在确定发起数据访问请求的账户为安全访问账户之后, 还可以包括如下实施步骤: 数据源服务器验证上下文信息中是否包含账户的在线信息; 当上下文信息中包含账户的在线信息时, 数据源服务器执行向第三方

系统返回数据访问请求所要访问的数据的步骤。

本申请方案中，上下文信息中可以包含账户的在线信息，当通过技术手段探测到账户在线后，生成账户在线信息，并将账户在线信息添加至上下文信息中。例如，可以通过向客户端定时发送心跳包的机制，根据客户端反馈的消息，判断账户是否在线，该判断账户是否在线的步骤可以由登录服务器执行。其中，当上下文信息中包含账户在线信息时，意味着当前账户在线，此时数据源服务器才执行向第三方系统返回数据访问请求所要访问的数据。

本申请上述实施例提供的可选方案中，当上下文信息中还包括账户的安全隐私等级信息时，数据源服务器向第三方系统返回数据访问请求所要访问的数据的步骤包括：数据源服务器根据安全隐私等级信息生成对应的第一访问数据，并将第一访问数据返回至第三方系统。

此处需要说明的是，本申请上述步骤中，安全隐私等级信息是针对不同的第三方系统，根据对第三方系统的信任程度不同，以及用户对第三方系统的授权程度不同，可以开放给第三方系统不同隐私程度的用户数据的标识信息。例如当安全隐私等级信息指示数据访问请求具有较高安全等级，例如第一安全等级，时，第一访问数据中可以包含第一安全等级所对应的信息，例如，用户的邮箱信息、用户的手机号码、或者用户的地址信息等；当安全隐私等级信息指示数据访问请求具有较低安全等级，例如第二安全等级，时，第一访问数据中可以包含第二安全等级所对应的信息，例如，用户的昵称信息、用户的头像信息等。

本申请上述实施例提供的可选方案中，当上下文信息中还包括账户的安全风险状态信息时，数据源服务器向第三方系统返回数据访问请求所要访问的数据的步骤包括：数据源服务器安全风险状态信息生成对应的第二访问数据，并将第二访问数据返回至第三方系统。

此处需要说明的是，本申请上述步骤中，安全风险状态信息是用于表征账户目前的风险状态的信息。例如，当安全风险状态信息指示账户处于较高风险状态时，例如第一风险状态时，第二访问数据中仅能包含第一风险状态所对应的信息，例如，用户的昵称信息、用户的头像信息等。当安全风险状态信息指示账户处于较低风险状态时，例如第二风险状态时，第二访问数据中能包含第二风险状态所对应的信息，例如，用户的支付信息、用户的手机号码、或者用户的地址信息等。判断账户的风险状态时，可以考虑账户是否在可信地点登陆或者账户是否使用可信设备登陆等；账户的风险状态可以划分为

例如：高安全风险，疑似风险状态，可信任状态等区域。安全风险状态信息可以由登录服务器生成。通过账户上下文信息中包括的账户安全风险状态信息，可以使得数据源服务器进一步控制数据的开放程度。

基于上述实施例二提供的方案可知，本申请提供的用户数据的访问控制方法关键在于在账户发起的数据访问请求中加载该账户的上下文信息，从而使得在账户使用第三方系统访问数据源时，可以保证账户为安全账户，且发起的数据访问请求也是安全请求，此处需要说明的是，本申请涉及到的第三方系统为非可控区域，第一服务器、数据源服务器、登录服务器为可控区域。

实施例三

根据本申请实施例，还提供了一种用户数据的访问控制方法的方法实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

本申请实施例三所提供的方法实施例仍旧可以在移动终端、计算机终端或者类似的运算装置中执行。此处需要说明的是，实施例三所提供的方法实施例仍旧可以运行在图 1 所示的计算机终端上。

以在上述运行环境下为，本申请还可以提供如图 8 所示的用户数据的访问控制方法。图 8 是根据本申请实施例三的用户数据的访问控制方法的流程示意图。如图 8 所示，一种可选的用户数据的访问控制方法包括如下实施步骤：

步骤 S702：第三方系统接收第一服务器发送的数据访问请求，其中，数据访问请求为由账户发起的包含了账户的上下文信息的请求。

步骤 S704：第三方系统转发数据访问请求至数据源服务器。

步骤 S706：第三方系统接收数据源服务器返回的数据访问请求所要访问的数据，其中，当数据源服务器根据数据访问请求中包含的上下文信息，确定发起数据访问请求的账户为安全访问账户，且数据访问请求为安全访问请求时，允许第三方系统根据数据访问请求访问数据源。

由上可知，本申请上述实施例三所提供的方案中，当前账户（可以是合法账户或者伪造账户冒充该合法账户）发出数据访问请求到达第一服务器后，第一服务器会对接收到的每一个数据访问请求进行校验，即第一服务器会判断数据访问请求是否携带账户上下文信息，和/或上下文信息是否能够校验通过，当对数据访问请求的校验通过的情况下，

第一服务器允许该数据访问请求发送至第三方系统，进而第三方系统就可以根据该数据访问请求访问数据源。在上述方案中，只有合法账户发起的数据访问请求能够通过校验，而对于冒充合法账户的恶意账户发起的数据访问请求，要么在形式上不携带账户上下文信息，要么在内容上携带的上下文信息不能通过校验。通过上述方案，实现了允许具有访问权限的合法账户发起的数据访问请求发送至第三方系统，解决了现有技术在使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

本申请上述实施例提供的可选方案中，在步骤 S702：第三方系统接收第一服务器发送的数据访问请求之前，还可以包括如下实施步骤：在第一服务器确定数据访问请求中携带账户的上下文信息，且账户的上下文信息为合法信息的情况下，生成账户的合法访问标识信息，其中，合法访问标识信息用于表征发起的数据访问请求的账户为合法账户。

本申请上述实施例提供的可选方案中，在步骤 S702：第三方系统接收第一服务器发送的数据访问请求之前，还可以包括如下实施步骤：

步骤 S7012：第一服务器验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验；

步骤 S7014：第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源；

步骤 S7016：第一服务器在确定数据访问请求中没有包含账户的上下文信息，和/或在账户的上下文信息校验失败的情况下，第一服务器仍旧发送数据访问请求至第三方系统，或者第一服务器禁止发送数据访问请求至第三方系统，并发出报警信息。

本申请上述实施例提供的可选方案中，数据源服务器根据数据访问请求中包含的上下文信息，确定发起数据访问请求的账户为安全访问账户，且数据访问请求为安全访问请求的具体实施步骤包括：

步骤 S7052：数据源服务器接收第三方系统转发的数据访问请求；

步骤 S7054：数据源服务器读取数据访问请求中携带的上下文信息；

步骤 S7056：在数据源服务器验证上下文信息为合法信息时，确定发起数据访问请求的账户为安全访问账户，且在查询得到账户具有合法访问标识信息时，确定数据访问请求为安全访问请求。

本申请上述实施例提供的可选方案中，在步骤 S702：第三方系统接收第一服务器发

送的数据访问请求之前，还可以包括如下实施步骤：第一服务器将接收到的数据访问请求转发至第三方系统，其中，向第一服务器发送数据访问请求的具体实施步骤包括：账户登录客户端之后，向登录服务器发起登录请求；客户端接收登录服务器返回的上下文信息，其中，上下文信息为登录服务器根据登录请求生成的完整上下文信息中的子集；

- 5 客户端获取账户的上下文信息；客户端发送账户触发的数据访问请求至第一服务器，其中，数据访问请求至少包括上下文信息；

此处需要说明的是，本申请上述实施例三所提供的优选实施方案与实施例一或实施例二所提供的可选方案以及应用场景实施过程相同，但不限于实施例一或实施例二所提供的方案。

10 实施例四

根据本申请实施例，还提供了一种用于实施上述方法实施例的装置实施例，本申请上述实施例所提供的装置可以在计算机终端上运行。

图 9 是根据本申请实施例四的用户数据的访问控制装置的结构示意图。

- 如图 9 所示，该装置包括：接收模块 802、校验模块 804 以及控制模块 806，其中，
15 校验模块 804 还包括第一校验单元 8042 和/或第二校验单元 8044。

- 其中，接收模块 802，用于接收账户发起的数据访问请求；校验模块，包含第一校验单元和/或第二校验单元，其中，所述第一校验单元用于验证所述数据访问请求中是否携带所述账户的上下文信息，所述第二校验单元对所述账户的上下文信息进行校验；控制模块，用于在校验模块校验通过的情况下，允许发送所述数据访问请求至第三方系统，
20 使得所述第三方系统根据所述数据访问请求访问数据源。

- 由上可知，本申请实施例四所提供的方案，当合法账户或者伪造账户冒充该合法账户是发出数据访问请求到达第一服务器后，第一服务器会对接收到每一个数据访问请求进行校验，即第一服务器会判断数据访问请求是否携带账户上下文信息，和/或上下文信息是否能够校验通过；当对数据访问请求的校验通过的情况下，第一服务器允许该数据
25 访问请求发送至第三方系统，进而第三方系统就可以根据该数据访问请求访问数据源。
- 在上述方案中，只有合法账户发起的数据访问请求能够通过校验，而对于冒充合法账户的恶意账户发起的数据访问请求，要么在形式上不携带账户上下文信息，要么在内容上携带的上下文信息不能通过校验。通过上述方案，实现了允许具有访问权限的合法账户发起的数据访问请求发送至第三方系统，解决了现有技术在使用第三方系统访问数
30 据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

此处需要说明的是，上述接收模块 802、校验模块 804 以及控制模块 806，对应于实施例一中的步骤 S202 至步骤 S206，三个模块与对应的步骤所实现的示例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的计算机终端 10 中，可以通过软件实现，也可以通过硬件实现。

5 可选地，如图 10 所示，第二校验单元包括：读取子单元 902，匹配子单元 904 以及生成子单元 906。

其中，读取子单元，用于在确定所述数据访问请求中携带所述上下文信息之后，读取所述数据访问请求中携带的所述上下文信息；匹配子单元，用于将所述上下文信息与预存的所述完整上下文信息进行匹配，在匹配成功的情况下，确定所述账户的上下文信息为合法信息；生成子单元，用于生成所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起所述数据访问请求的所述账户为合法账户。

10

此处需要说明的是，上述读取子单元 902，匹配子单元 904 以及生成子单元 906，对应于实施例一中的步骤 S402 至步骤 S406，三个模块与对应的步骤所实现的示例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的计算机终端 10 中，可以通过软件实现，也可以通过硬件实现。

15

可选地，如图 11 所示，第二校验单元包括：发送子单元 1002，第一接收子单元 1004 以及第二接收子单元 1006。

其中，发送子单元，用于在确定所述数据访问请求中携带所述上下文信息之后，发送所述上下文信息至上下文信息服务器；第一接收子单元，用于接收所述上下文信息服务器验证所述上下文信息的验证结果；第二接收子单元，用于在所述验证结果为所述账户的上下文信息为合法信息的情况下，接收所述上下文信息服务器生成的所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起的所述数据访问请求的所述账户为合法账户；所述上下文信息服务器将所述上下文信息与预存在本地的所述完整上下文信息进行匹配，在匹配成功的情况下，所述验证结果为所述账户的上下文信息为所述合法信息。

20

25

此处需要说明的是，上述发送子单元 1002，第一接收子单元 1004 以及第二接收子单元 1006，对应于实施例一中的步骤 S502 至步骤 S506，三个模块与对应的步骤所实现的示例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的计算机终端 10 中，可以通过软件实现，

30

也可以通过硬件实现。

可选地，控制模块还用于在校验单元校验不通过的情况下，发送所述数据访问请求至所述第三方系统，或者所述禁止发送所述数据访问请求至所述第三方系统，并发出报警信息。

- 5 本申请上述实施例四所提供的优选实施方案与实施例一所提供的方法实施例的可选方案以及应用场景实施过程相同，但不限于实施例一所提供的方案。

实施例五

根据本申请实施例，还提供了一种用于实施上述方法实施例的装置实施例，本申请上述实施例所提供的装置可以在计算机终端上运行。

- 10 图 12 是根据本申请实施例五的用户数据的访问控制装置的结构示意图。

如图 12 所示，该装置包括：获取模块 1102，发送模块 1104 以及接收模块 1106。

- 其中，获取模块，用于获取账户的上下文信息；发送模块，用于发送所述账户触发的数据访问请求至第一服务器，其中，所述数据访问请求至少包括所述上下文信息；接收模块，用于接收所述第一服务器根据所述数据访问请求获取到的访问数据；其中，在
15 所述第一服务器确定所述数据访问请求中包含所述账户的上下文信息，和/或在所述账户的上下文信息校验通过的情况下，允许发送所述数据访问请求至第三方系统，使得所述第三方系统根据所述数据访问请求访问数据源。

- 由上可知，本申请实施例五所提供的方案，当合法账户或者伪造账户冒充该合法账户是发出数据访问请求到达第一服务器后，第一服务器会对接收到每一个数据访问请求
20 进行校验，即第一服务器会判断数据访问请求是否携带账户上下文信息，和/或上下文信息是否能够校验通过；当对数据访问请求的校验通过的情况下，第一服务器允许该数据访问请求发送至第三方系统，进而第三方系统就可以根据该数据访问请求访问数据源。在上述方案中，只有合法账户发起的数据访问请求能够通过校验，而对于冒充合法账户的恶意账户发起的数据访问请求，要么在形式上不携带账户上下文信息，要么在内容上
25 携带的上下文信息不能通过校验。通过上述方案，实现了允许具有访问权限的合法账户发起的数据访问请求发送至第三方系统，解决了现有技术在用户使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

- 此处需要说明的是，上述获取模块 1102，发送模块 1104 以及接收模块 1106，对应于实施例二中的步骤 S602 至步骤 S606，三个模块与对应的步骤所实现的示例和应用场
30 景相同，但不限于上述实施例二所公开的内容。需要说明的是，上述模块作为装置的一

部分可以运行在实施例二提供的计算机终端 10 中，可以通过软件实现，也可以通过硬件实现。

此处需要说明的是，本申请上述实施例五所提供的优选实施方案与实施例二所提供的可选方案以及应用场景实施过程相同，但不限于实施例二所提供的方案。

5 实施例六

根据本申请实施例，还提供了一种用于实施上述方法实施例的装置实施例，本申请上述实施例所提供的装置可以在计算机终端上运行。

图 13 是根据本申请实施例六的用户数据的访问控制装置的结构示意图。

10 如图 13 所示，该装置包括：第一接收模块 1202，转发模块 1204 以及第二接收模块 1206。

其中，第一接收模块，用于接收第一服务器发送的数据访问请求，其中，所述数据访问请求为由账户发起的包含了所述账户的上下文信息的请求；转发模块，用于转发所述数据访问请求至数据源服务器；第二接收模块，用于接收所述数据源服务器返回的所述数据访问请求所要访问的数据，其中，当所述数据源服务器根据所述数据访问请求中包含的所述上下文信息，确定发起所述数据访问请求的所述账户为安全访问账户，且所述数据访问请求为安全访问请求时，允许第三方系统根据所述数据访问请求访问数据源。

20 由上可知，本申请实施例六所提供的方案，当合法账户或者伪造账户冒充该合法账户是发出数据访问请求到达第一服务器后，第一服务器会对接收到每一个数据访问请求进行校验，即第一服务器会判断数据访问请求是否携带账户上下文信息，和/或上下文信息是否能够校验通过；当对数据访问请求的校验通过的情况下，第一服务器允许该数据访问请求发送至第三方系统，进而第三方系统就可以根据该数据访问请求访问数据源。在上述方案中，只有合法账户发起的数据访问请求能够通过校验，而对于冒充合法账户的恶意账户发起的数据访问请求，要么在形式上不携带账户上下文信息，要么在内容上携带的上下文信息不能通过校验。通过上述方案，实现了允许具有访问权限的合法账户 25 发起的数据访问请求发送至第三方系统，解决了现有技术在用户使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

30 此处需要说明的是，上述第一接收模块 1202，转发模块 1204 以及第二接收模块 1206，对应于实施例三中的步骤 S702 至步骤 S706，三个模块与对应的步骤所实现的示例和应用场景相同，但不限于上述实施例三所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例三提供的计算机终端 10 中，可以通过软件实现，也可以通过

硬件实现。

本申请上述实施例六所提供的优选实施方案与实施例三所提供的可选方案以及应用场景实施过程相同，但不限于实施例三所提供的方案。

实施例七

5 根据本申请实施例，还提供了一种用户数据的访问控制系统，图 14 是根据本申请实施例七的用户数据的访问控制系统的结构示意图。

如图 14 所示，该系统包括：

客户终端 141，用于在账户登录之后，发起数据访问请求；

10 第一服务器 143，与客户终端 141 通信，用于在验证数据访问请求中包含了账户的上下文信息，和/或验证上下文信息为合法信息之后，透传数据访问请求；

第三方系统服务器 145，与第一服务器 143 通信，用于接收第一服务器透传的数据访问请求；

15 数据源服务器 147，与第三方系统服务器 145 通信，用于接收第三方系统服务器通信转发的数据访问请求，在根据数据访问请求中包含的上下文信息，确定发起数据访问请求的账户为安全访问账户，且数据访问请求为安全访问请求时，返回数据访问请求对应的访问数据至第三方系统服务器。

本申请上述实施例七提供了一种系统方案，可以实现当合法账户登录客户端中的 141 之后，合法账户可以发出数据访问请求到达第一服务器 143，第一服务器 143 可以对接收到数据访问请求进行校验，即第一服务器会判断数据访问请求是否携带账户上下文信息，和/或上下文信息是否能够校验通过，当对数据访问请求的校验通过的情况下，第一服务器允许该数据访问请求发送至第三方系统，进而第三方系统就可以根据该数据访问请求访问数据源。在上述方案中，只有合法账户发起的数据访问请求能够通过校验，而对于冒充合法账户的恶意账户发起的数据访问请求，要么在形式上不携带账户上下文信息，要么在内容上携带的上下文信息不能通过校验。通过上述方案，实现了允许具有访问权限的合法账户发起的数据访问请求发送至第三方系统，解决了现有技术在用户使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

25

可选的，上述系统还可以包括：登录服务器和上下文信息服务器。

30 其中，当账户登录客户端时，开始向登陆服务器发起登陆请求，登陆服务器会计算生成该账户对应的完整上下文信息（即完整 Context 信息），同时登录服务器会存储该

账户的账号密码信息和上述完整上下文信息，或者将上下文信息发送至上下文信息服务器进行保存。

本申请上述实施例七所提供的优选实施方案与实施例一至实施例三所提供的可选方案以及应用场景实施过程相同，但不限于实施例一至实施例三所提供的方案。

5 实施例八

本申请的实施例可以提供一种计算机终端，该计算机终端可以是计算机终端群中的任意一个计算机终端设备。可选地，在本实施例中，上述计算机终端也可以替换为移动终端等终端设备。

10 可选地，在本实施例中，上述计算机终端可以位于计算机网络的多个网络设备中的至少一个网络设备。

在本实施例中，上述计算机终端可以执行应用程序的漏洞检测方法中以下步骤的程序代码：第一服务器接收账户发起的数据访问请求；所述第一服务器验证所述数据访问请求中是否携带所述账户的上下文信息，和/或对所述账户的上下文信息进行校验；所述第一服务器在确定所述数据访问请求中包含所述账户的上下文信息，和/或在所述账户的上下文信息校验通过的情况下，允许发送所述数据访问请求至第三方系统，使得所述第
15 三方系统根据所述数据访问请求访问数据源。

可选地，图 15 是根据本申请实施例的一种计算机终端的结构框图。如图 15 所示，该计算机终端 A 可以包括：一个或多个（图中仅示出一个）处理器 51、存储器 53、以及传输装置 55。

20 其中，存储器 53 可用于存储软件程序以及模块，如本申请实施例中的安全漏洞检测方法和装置对应的程序指令/模块，处理器 51 通过运行存储在存储器 53 内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的系统漏洞攻击的检测方法。存储器 53 可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 53 可进一步包括
25 相对于处理器 51 远程设置的存储器，这些远程存储器可以通过网络连接至终端 A。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

上述的传输装置 55 用于经由一个网络接收或者发送数据。上述的网络具体实例可包括有线网络及无线网络。在一个实例中，传输装置 55 包括一个网络适配器（Network Interface Controller, NIC），其可通过网线与其他网络设备与路由器相连从而可与互联网
30 或局域网进行通讯。在一个实例中，传输装置 55 为射频（Radio Frequency, RF）模块，

其用于通过无线方式与互联网进行通讯。

其中，具体地，存储器 53 用于存储预设动作条件和预设权限用户的信息、以及应用程序。

处理器 51 可以通过传输装置调用存储器 53 存储的信息及应用程序，以执行下述步骤：第一服务器接收账户发起的数据访问请求；所述第一服务器验证所述数据访问请求中是否携带所述账户的上下文信息，和/或对所述账户的上下文信息进行校验；所述第一服务器在确定所述数据访问请求中包含所述账户的上下文信息，和/或在所述账户的上下文信息校验通过的情况下，允许发送所述数据访问请求至第三方系统，使得所述第三方系统根据所述数据访问请求访问数据源。

10 可选的，上述处理器 51 还可以执行如下步骤的程序代码：所述账户登录客户端之后，向登录服务器发起登录请求；所述客户端接收所述登录服务器返回的所述上下文信息，其中，所述上下文信息为所述登录服务器根据所述登录请求生成的完整上下文信息中的子集；所述客户端发送携带有所述上下文信息的所述数据访问请求至所述第一服务器。

15 可选的，上述处理器 51 还可以执行如下步骤的程序代码：所述第一服务器在确定所述数据访问请求中携带所述上下文信息之后，读取所述数据访问请求中携带的所述上下文信息；所述第一服务器将所述上下文信息与预存的所述完整上下文信息进行匹配，在匹配成功的情况下，确定所述账户的上下文信息为合法信息；所述第一服务器生成所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起所述数据访问请求的所述账户为合法账户。

20 可选的，上述处理器 51 还可以执行如下步骤的程序代码：所述第一服务器在确定所述数据访问请求中携带所述上下文信息之后，发送所述上下文信息至上下文信息服务器；所述第一服务器接收所述上下文信息服务器验证所述上下文信息的验证结果；在所述验证结果为所述账户的上下文信息为合法信息的情况下，所述第一服务器接收所述上下文信息服务器生成的所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表
25 征发起的所述数据访问请求的所述账户为合法账户；其中，所述上下文信息服务器将所述上下文信息与预存在本地的所述完整上下文信息进行匹配，在匹配成功的情况下，所述验证结果为所述账户的上下文信息为所述合法信息。

30 可选的，上述处理器 51 还可以执行如下步骤的程序代码：数据源服务器接收所述第三方系统转发的所述数据访问请求；所述数据源服务器访问所述第一服务器或所述上下文信息服务器，如果查询得到所述账户的所述合法访问标识信息，则确定所述合法账户

发起的所述数据访问请求为安全访问请求；所述数据源服务器向所述第三方系统返回所述数据访问请求所要访问的数据。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：所述数据源服务器验证所述上下文信息中是否包含所述账户的在线信息；当所述上下文信息中包含所述账户的在线信息时，所述数据源服务器执行向所述第三方系统返回所述数据访问请求所要访问的数据的步骤。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：所述数据源服务器根据所述安全隐私等级信息生成对应的第一访问数据，并将所述第一访问数据返回至所述第三方系统。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：所述数据源服务器根据所述安全风险状态信息生成对应的第二访问数据，并将所述第二访问数据返回至所述第三方系统。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：所述第一服务器在确定所述数据访问请求中没有包含所述账户的上下文信息，或在所述账户的上下文信息校验失败的情况下，所述第一服务器发送所述数据访问请求至所述第三方系统，或者所述第一服务器禁止发送所述数据访问请求至所述第三方系统，并发出报警信息。

采用本申请实施例，提供了一种用户数据的访问控制方案。采用第一服务器接收账户发起的数据访问请求，验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验的方式，通过第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，达到了使得第三方系统根据数据访问请求访问数据源的目的，从而实现了在第三方系统接收数据访问前就能够鉴别发送该数据访问请求的账户是否为合法账户的技术效果，进而解决了现有技术在使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

本领域普通技术人员可以理解，图 15 所示的结构仅为示意，计算机终端也可以是智能手机（如Android 手机、iOS 手机等）、平板电脑、掌上电脑以及移动互联网设备（Mobile Internet Devices，MID）、PAD 等终端设备。图 15 其并不对上述电子装置的结构造成限定。例如，计算机终端 A 还可包括比图 15 中所示更多或者更少的组件（如网络接口、显示装置等），或者具有与图 15 所示不同的配置。

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

过程来指令终端设备相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器（Read-Only Memory, ROM）、随机存取器（Random Access Memory, RAM）、磁盘或光盘等。

实施例九

5 本申请的实施例可以提供一种计算机终端，该计算机终端可以是计算机终端群中的任意一个计算机终端设备。可选地，在本实施例中，上述计算机终端也可以替换为移动终端等终端设备。

可选地，在本实施例中，上述计算机终端可以位于计算机网络的多个网络设备中的至少一个网络设备。

10 在本实施例中，上述计算机终端可以执行应用程序的漏洞检测方法中以下步骤的程序代码：客户端获取账户的上下文信息；客户端发送账户触发的数据访问请求至第一服务器，其中，数据访问请求至少包括上下文信息；客户端接收第一服务器根据数据访问请求获取到的访问数据；其中，在第一服务器确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，
15 使得第三方系统根据数据访问请求访问数据源。

可选地，仍旧参照图 15 所提供的一种计算机终端的结构框图。如图 15 所示，该计算机终端 A 可以包括：一个或多个（图中仅示出一个）处理器 51、存储器 53、以及传输装置 55。

其中，存储器 53 可用于存储软件程序以及模块，如本申请实施例中的安全漏洞检测方法
20 和装置对应的程序指令/模块，处理器 51 通过运行存储在存储器 53 内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的系统漏洞攻击的检测方法。存储器 53 可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 53 可进一步包括相对于处理器 51 远程设置的存储器，这些远程存储器可以通过网络连接至终端 A。上述
25 网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

上述的传输装置 55 用于经由一个网络接收或者发送数据。上述的网络具体实例可包括有线网络及无线网络。在一个实例中，传输装置 55 包括一个网络适配器（Network Interface Controller, NIC），其可通过网线与其他网络设备与路由器相连从而可与互联网或局域网进行通讯。在一个实例中，传输装置 55 为射频（Radio Frequency, RF）模块，
30 其用于通过无线方式与互联网进行通讯。

其中，具体地，存储器 53 用于存储预设动作条件和预设权限用户的信息、以及应用程序。

处理器 51 可以通过传输装置调用存储器 53 存储的信息及应用程序，以执行下述步骤：客户端获取账户的上下文信息；客户端发送账户触发的数据访问请求至第一服务器，
5 其中，数据访问请求至少包括上下文信息；客户端接收第一服务器根据数据访问请求获取到的访问数据；其中，在第一服务器确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：账户登录客户端之后，向
10 登录服务器发起登录请求；客户端接收登录服务器返回的上下文信息，其中，上下文信息为登录服务器根据登录请求生成的完整上下文信息中的子集。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：登录服务器接收登录请求，生成发起登录请求的账户的完整上下文信息，将完整上下文信息的其中一个子集返回给客户端；并将完整上下文信息发送给第一服务器和/或上下文信息服务器。

15 可选的，上述处理器 51 还可以执行如下步骤的程序代码：第一服务器接收账户发起的数据访问请求；第一服务器验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验；第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源。

20 可选的，上述处理器 51 还可以执行如下步骤的程序代码：第一服务器在确定数据访问请求中携带上下文信息之后，读取数据访问请求中携带的上下文信息；第一服务器将上下文信息与预存的完整上下文信息进行匹配，在匹配成功的情况下，确定账户的上下文信息为合法信息；第一服务器生成账户的合法访问标识信息，其中，合法访问标识信息用于表征发起数据访问请求的账户为合法账户。

25 可选的，上述处理器 51 还可以执行如下步骤的程序代码：第一服务器在确定数据访问请求中携带上下文信息之后，发送上下文信息至上下文信息服务器；第一服务器接收上下文信息服务器验证上下文信息的验证结果；在验证结果为账户的上下文信息为合法信息的情况下，第一服务器接收上下文信息服务器生成的账户的合法访问标识信息，其中，合法访问标识信息用于表征发起的数据访问请求的账户为合法账户；其中，上下文
30 信息服务器将上下文信息与预存在本地的完整上下文信息进行匹配，在匹配成功的情况

下，验证结果为账户的上下文信息为合法信息。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：数据源服务器接收第三方系统转发的数据访问请求；数据源服务器访问第一服务器或上下文信息服务器，如果查询得到账户的合法访问标识信息，则确定合法账户发起的数据访问请求为安全访问请求；
5 数据源服务器向第三方系统返回数据访问请求所要访问的数据。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：数据源服务器验证上下文信息中是否包含账户的在线信息；当上下文信息中包含账户的在线信息时，数据源服务器执行向第三方系统返回数据访问请求所要访问的数据的步骤。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：数据源服务器根据安全隐私等级信息生成对应的第一访问数据，并将第一访问数据返回至第三方系统。
10

可选的，上述处理器 51 还可以执行如下步骤的程序代码：数据源服务器安全风险状态信息生成对应的第二访问数据，并将第二访问数据返回至第三方系统。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：第一服务器在确定数据访问请求中没有包含账户的上下文信息，或在账户的上下文信息校验失败的情况下，第一服务器发送数据访问请求至第三方系统，或者第一服务器禁止发送数据访问请求至第三方系统，并发出报警信息。
15

采用本申请实施例，提供了一种用户数据的访问控制方案。采用第一服务器接收账户发起的数据访问请求，验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验的方式，通过第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，达到了使得第三方系统根据数据访问请求访问数据源的目的，从而实现了在第三方系统接收数据访问前就能够鉴别发送该数据访问请求的账户是否为合法账户的技术效果，进而解决了现有技术在使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。
20

本领域普通技术人员可以理解，图 15 所示的结构仅为示意，计算机终端也可以是智能手机（如Android 手机、iOS 手机等）、平板电脑、掌上电脑以及移动互联网设备（Mobile Internet Devices，MID）、PAD 等终端设备。图 15 其并不对上述电子装置的结构造成限定。例如，计算机终端 A 还可包括比图 15 中所示更多或者更少的组件（如网络接口、显示装置等），或者具有与图 15 所示不同的配置。
25

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
30

过程序来指令终端设备相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器（Read-Only Memory，ROM）、随机存取器（Random Access Memory，RAM）、磁盘或光盘等。

实施例十

5 本申请的实施例可以提供一种计算机终端，该计算机终端可以是计算机终端群中的任意一个计算机终端设备。可选地，在本实施例中，上述计算机终端也可以替换为移动终端等终端设备。

 可选地，在本实施例中，上述计算机终端可以位于计算机网络的多个网络设备中的至少一个网络设备。

10 在本实施例中，上述计算机终端可以执行应用程序的漏洞检测方法中以下步骤的程序代码：第三方系统接收第一服务器发送的数据访问请求，其中，数据访问请求为由账户发起的包含了账户的上下文信息的请求；第三方系统转发数据访问请求至数据源服务器；第三方系统接收数据源服务器返回的数据访问请求所要访问的数据，其中，当数据源服务器根据数据访问请求中包含的上下文信息，确定发起数据访问请求的账户为安全访问账户，且数据访问请求为安全访问请求时，允许第三方系统根据数据访问请求访问数据源。

 可选地，仍旧参照图 15 所提供的一种计算机终端的结构框图。如图 15 所示，该计算机终端 A 可以包括：一个或多个（图中仅示出一个）处理器 51、存储器 53、以及传输装置 55。

20 其中，存储器 53 可用于存储软件程序以及模块，如本申请实施例中的安全漏洞检测方法和装置对应的程序指令/模块，处理器 51 通过运行存储在存储器 53 内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的系统漏洞攻击的检测方法。存储器 53 可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 53 可进一步包括
25 相对于处理器 51 远程设置的存储器，这些远程存储器可以通过网络连接至终端 A。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

 上述的传输装置 55 用于经由一个网络接收或者发送数据。上述的网络具体实例可包括有线网络及无线网络。在一个实例中，传输装置 55 包括一个网络适配器（Network Interface Controller，NIC），其可通过网线与其他网络设备与路由器相连从而可与互联网
30 或局域网进行通讯。在一个实例中，传输装置 55 为射频（Radio Frequency，RF）模块，

其用于通过无线方式与互联网进行通讯。

其中，具体地，存储器 53 用于存储预设动作条件和预设权限用户的信息、以及应用程序。

处理器 51 可以通过传输装置调用存储器 53 存储的信息及应用程序，以执行下述步
5 骤：第三方系统接收第一服务器发送的数据访问请求，其中，数据访问请求为由账户发
起的包含了账户的上下文信息的请求；第三方系统转发数据访问请求至数据源服务器；
第三方系统接收数据源服务器返回的数据访问请求所要访问的数据，其中，当数据源服
务器根据数据访问请求中包含的上下文信息，确定发起数据访问请求的账户为安全访问
账户，且数据访问请求为安全访问请求时，允许第三方系统根据数据访问请求访问数据
10 源。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：在第一服务器确定数据访
问请求中携带账户的上下文信息，且账户的上下文信息为合法信息的情况下，生成账户
的合法访问标识信息，其中，合法访问标识信息用于表征发起的数据访问请求的账户为
合法账户。

15 可选的，上述处理器 51 还可以执行如下步骤的程序代码：第一服务器验证数据访问
请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验；第一服务器在
确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的况
下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据
源；第一服务器在确定数据访问请求中没有包含账户的上下文信息，和/或在账户的上下
20 文信息校验失败的情况下，第一服务器仍旧发送数据访问请求至第三方系统，或者第一
服务器禁止发送数据访问请求至第三方系统，并发出报警信息。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：数据源服务器接收第三方
系统转发的数据访问请求；数据源服务器读取数据访问请求中携带的上下文信息；在数
据源服务器验证上下文信息为合法信息时，确定发起数据访问请求的账户为安全访问账
25 户，且在查询得到账户具有合法访问标识信息时，确定数据访问请求为安全访问请求。

可选的，上述处理器 51 还可以执行如下步骤的程序代码：第一服务器将接收到的数
据访问请求转发至第三方系统，其中，向第一服务器发送数据访问请求的具体实施步骤
包括：账户登录客户端之后，向登录服务器发起登录请求；客户端接收登录服务器返回
的上下文信息，其中，上下文信息为登录服务器根据登录请求生成的完整上下文信息中
30 的子集；客户端获取账户的上下文信息；客户端发送账户触发的数据访问请求至第一服

务器，其中，数据访问请求至少包括上下文信息。

采用本申请实施例，提供了一种用户数据的访问控制方案。采用第一服务器接收账户发起的数据访问请求，验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验的方式，通过第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，达到了使得第三方系统根据数据访问请求访问数据源的目的，从而实现了在第三方系统接收数据访问前就能够鉴别发送该数据访问请求的账户是否为合法账户的技术效果，进而解决了现有技术在使用第三方系统访问数据源的过程中，由于发起访问的账户的安全性差，导致数据源数据安全性差的技术问题。

本领域普通技术人员可以理解，图 15 所示的结构仅为示意，计算机终端也可以是智能手机（如Android 手机、iOS 手机等）、平板电脑、掌上电脑以及移动互联网设备（Mobile Internet Devices，MID）、PAD 等终端设备。图 15 其并不对上述电子装置的结构造成限定。例如，计算机终端 15 还可包括比图 15 中所示更多或者更少的组件（如网络接口、显示装置等），或者具有与图 15 所示不同的配置。

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终端设备相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器（Read-Only Memory，ROM）、随机存取器（Random Access Memory，RAM）、磁盘或光盘等。

实施例十一

本申请的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以用于保存上述实施例一所提供的用户数据的访问控制方法所执行的程序代码。

可选地，在本实施例中，上述存储介质可以位于计算机网络中计算机终端群中的任意一个计算机终端中，或者位于移动终端群中的任意一个移动终端中。

可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第一服务器接收账户发起的数据访问请求；所述第一服务器验证所述数据访问请求中是否携带所述账户的上下文信息，和/或对所述账户的上下文信息进行校验；所述第一服务器在确定所述数据访问请求中包含所述账户的上下文信息，和/或在所述账户的上下文信息校验通过的情况下，允许发送所述数据访问请求至第三方系统，使得所述第三方系统根据所述数据访问请求访问数据源。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：所述账户登录客

户端之后，向登录服务器发起登录请求；所述客户端接收所述登录服务器返回的所述上下文信息，其中，所述上下文信息为所述登录服务器根据所述登录请求生成的完整上下文信息中的子集；所述客户端发送携带有所述上下文信息的所述数据访问请求至所述第一服务器。

5 可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：所述第一服务器在确定所述数据访问请求中携带所述上下文信息之后，读取所述数据访问请求中携带的所述上下文信息；所述第一服务器将所述上下文信息与预存的所述完整上下文信息进行匹配，在匹配成功的情况下，确定所述账户的上下文信息为合法信息；所述第一服务器生成所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起所述数据访问请求的所述账户为合法账户。

10 可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：所述第一服务器在确定所述数据访问请求中携带所述上下文信息之后，发送所述上下文信息至上下文信息服务器；所述第一服务器接收所述上下文信息服务器验证所述上下文信息的验证结果；在所述验证结果为所述账户的上下文信息为合法信息的情况下，所述第一服务器接收所述上下文信息服务器生成的所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起的所述数据访问请求的所述账户为合法账户；其中，所述上下文信息服务器将所述上下文信息与预存在本地的所述完整上下文信息进行匹配，在匹配成功的情况下，所述验证结果为所述账户的上下文信息为所述合法信息。

15 可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：数据源服务器接收所述第三方系统转发的所述数据访问请求；所述数据源服务器访问所述第一服务器或所述上下文信息服务器，如果查询得到所述账户的所述合法访问标识信息，则确定所述合法账户发起的所述数据访问请求为安全访问请求；所述数据源服务器向所述第三方系统返回所述数据访问请求所要访问的数据。

20 可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：所述数据源服务器验证所述上下文信息中是否包含所述账户的在线信息；当所述上下文信息中包含所述账户的在线信息时，所述数据源服务器执行向所述第三方系统返回所述数据访问请求所要访问的数据的步骤。

25 可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：所述数据源服务器根据所述安全隐私等级信息生成对应的第一访问数据，并将所述第一访问数据返回至
30 所述第三方系统。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：所述数据源服务器所述安全风险状态信息生成对应的第二访问数据，并将所述第二访问数据返回至所述第三方系统。

5 可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：所述第一服务器在确定所述数据访问请求中没有包含所述账户的上下文信息，或在所述账户的上下文信息校验失败的情况下，所述第一服务器发送所述数据访问请求至所述第三方系统，或者所述第一服务器禁止发送所述数据访问请求至所述第三方系统，并发出报警信息。

此处需要说明的是，上述计算机终端群中的任意一个可以与网站服务器和扫描器建立通信关系，扫描器可以扫描计算机终端上 php 执行的 web 应用程序的值命令。

10 实施例十二

本申请的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以用于保存上述实施例二所提供的用户数据的访问控制方法所执行的程序代码。

可选地，在本实施例中，上述存储介质可以位于计算机网络中计算机终端群中的任意一个计算机终端中，或者位于移动终端群中的任意一个移动终端中。

15 可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：客户端获取账户的上下文信息；客户端发送账户触发的数据访问请求至第一服务器，其中，数据访问请求至少包括上下文信息；客户端接收第一服务器根据数据访问请求获取到的访问数据；其中，在第一服务器确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三
20 方系统根据数据访问请求访问数据源。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：账户登录客户端之后，向登录服务器发起登录请求；客户端接收登录服务器返回的上下文信息，其中，上下文信息为登录服务器根据登录请求生成的完整上下文信息中的子集。

25 可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：登录服务器接收登录请求，生成发起登录请求的账户的完整上下文信息，将完整上下文信息的其中一个子集返回给客户端；并将完整上下文信息发送给第一服务器和/或上下文信息服务器。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：第一服务器接收账户发起的数据访问请求；第一服务器验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验；第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三
30 方系统。

系统，使得第三方系统根据数据访问请求访问数据源。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：第一服务器在确定数据访问请求中携带上下文信息之后，读取数据访问请求中携带的上下文信息；第一服务器将上下文信息与预存的完整上下文信息进行匹配，在匹配成功的情况下，确定账户的上下文信息为合法信息；第一服务器生成账户的合法访问标识信息，其中，合法访问标识信息用于表征发起数据访问请求的账户为合法账户。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：第一服务器在确定数据访问请求中携带上下文信息之后，发送上下文信息至上下文信息服务器；第一服务器接收上下文信息服务器验证上下文信息的验证结果；在验证结果为账户的上下文信息为合法信息的情况下，第一服务器接收上下文信息服务器生成的账户的合法访问标识信息，其中，合法访问标识信息用于表征发起的数据访问请求的账户为合法账户；其中，上下文信息服务器将上下文信息与预存在本地的完整上下文信息进行匹配，在匹配成功的情况下，验证结果为账户的上下文信息为合法信息。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：数据源服务器接收第三方系统转发的数据访问请求；数据源服务器访问第一服务器或上下文信息服务器，如果查询得到账户的合法访问标识信息，则确定合法账户发起的数据访问请求为安全访问请求；数据源服务器向第三方系统返回数据访问请求所要访问的数据。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：数据源服务器验证上下文信息中是否包含账户的在线信息；当上下文信息中包含账户的在线信息时，数据源服务器执行向第三方系统返回数据访问请求所要访问的数据的步骤。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：数据源服务器根据安全隐私等级信息生成对应的第一访问数据，并将第一访问数据返回至第三方系统。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：数据源服务器安全风险状态信息生成对应的第二访问数据，并将第二访问数据返回至第三方系统。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：第一服务器在确定数据访问请求中没有包含账户的上下文信息，或在账户的上下文信息校验失败的情况下，第一服务器发送数据访问请求至第三方系统，或者第一服务器禁止发送数据访问请求至第三方系统，并发出报警信息。

此处需要说明的是，上述计算机终端群中的任意一个可以与网站服务器和扫描器建立通信关系，扫描器可以扫描计算机终端上 php 执行的 web 应用程序的值命令。

实施例十三

本申请的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以用于保存上述实施例三所提供的用户数据的访问控制方法所执行的程序代码。

可选地，在本实施例中，上述存储介质可以位于计算机网络中计算机终端群中的任意一个计算机终端中，或者位于移动终端群中的任意一个移动终端中。

可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第三方系统接收第一服务器发送的数据访问请求，其中，数据访问请求为由账户发起的包含了账户的上下文信息的请求；第三方系统转发数据访问请求至数据源服务器；第三方系统接收数据源服务器返回的数据访问请求所要访问的数据，其中，当数据源服务器根据数据访问请求中包含的上下文信息，确定发起数据访问请求的账户为安全访问账户，且数据访问请求为安全访问请求时，允许第三方系统根据数据访问请求访问数据源。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：在第一服务器确定数据访问请求中携带账户的上下文信息，且账户的上下文信息为合法信息的情况下，生成账户的合法访问标识信息，其中，合法访问标识信息用于表征发起的数据访问请求的账户为合法账户。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：第一服务器验证数据访问请求中是否携带账户的上下文信息，和/或对账户的上下文信息进行校验；第一服务器在确定数据访问请求中包含账户的上下文信息，和/或在账户的上下文信息校验通过的情况下，允许发送数据访问请求至第三方系统，使得第三方系统根据数据访问请求访问数据源；第一服务器在确定数据访问请求中没有包含账户的上下文信息，和/或在账户的上下文信息校验失败的情况下，第一服务器仍旧发送数据访问请求至第三方系统，或者第一服务器禁止发送数据访问请求至第三方系统，并发出报警信息。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：数据源服务器接收第三方系统转发的数据访问请求；数据源服务器读取数据访问请求中携带的上下文信息；在数据源服务器验证上下文信息为合法信息时，确定发起数据访问请求的账户为安全访问账户，且在查询得到账户具有合法访问标识信息时，确定数据访问请求为安全访问请求。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：第一服务器将接收到的数据访问请求转发至第三方系统，其中，向第一服务器发送数据访问请求的具体实施步骤包括：账户登录客户端之后，向登录服务器发起登录请求；客户端接收登录服

务器返回的上下文信息，其中，上下文信息为登录服务器根据登录请求生成的完整上下文信息中的子集；客户端获取账户的上下文信息；客户端发送账户触发的数据访问请求至第一服务器，其中，数据访问请求至少包括上下文信息。

上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。

- 5 在本申请的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中未详述的部分，可以参见其他实施例的相关描述。

10 在本申请所提供的几个实施例中，应该理解到，所揭露的客户端，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

15 所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。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

20 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，可以存储在一个计算机可读取存储介质中。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介质中，包括若干指令用以使得一台计算机设备（可为个人计算机、服务器或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：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。

25

30 以上所述仅是本申请的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本申请的保护范围。

权 利 要 求 书

1、一种用户数据的访问控制方法，其特征在于，包括：

第一服务器接收账户发起的数据访问请求；

5 所述第一服务器验证所述数据访问请求中是否携带所述账户的上下文信息，和/或对所述账户的上下文信息进行校验；

所述第一服务器在确定所述数据访问请求中包含所述账户的上下文信息，和/或在所述账户的上下文信息校验通过的情况下，允许发送所述数据访问请求至第三方系统，使得所述第三方系统根据所述数据访问请求访问数据源。

2、根据权利要求 1 所述的方法，其特征在于，在第一服务器接收账户发起的数据访问请求之前，所述方法还包括：

所述账户登录客户端之后，向登录服务器发起登录请求；

所述客户端接收所述登录服务器返回的所述上下文信息，其中，所述上下文信息为所述登录服务器根据所述登录请求生成的完整上下文信息中的子集；

所述客户端发送携带有所述上下文信息的所述数据访问请求至所述第一服务器。

15 3、根据权利要求 2 所述的方法，其特征在于，对所述账户的上下文信息进行校验，包括：

所述第一服务器在确定所述数据访问请求中携带所述上下文信息之后，读取所述数据访问请求中携带的所述上下文信息；

20 所述第一服务器将所述上下文信息与预存的所述完整上下文信息进行匹配，在匹配成功的情况下，确定所述账户的上下文信息为合法信息；

所述第一服务器生成所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起所述数据访问请求的所述账户为合法账户。

4、根据权利要求 2 所述的方法，其特征在于，对所述账户的上下文信息进行校验，包括：

25 所述第一服务器在确定所述数据访问请求中携带所述上下文信息之后，发送所述上下文信息至上下文信息服务器；

所述第一服务器接收所述上下文信息服务器验证所述上下文信息的验证结果；

30 在所述验证结果为所述账户的上下文信息为合法信息的情况下，所述第一服务器接收所述上下文信息服务器生成的所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起的所述数据访问请求的所述账户为合法账户；

其中,所述上下文信息服务器将所述上下文信息与预存在本地的所述完整上下文信息进行匹配,在匹配成功的情况下,所述验证结果为所述账户的上下文信息为所述合法信息。

5 5、根据权利要求 3 或 4 所述的方法,其特征在于,在允许发送所述数据访问请求至第三方系统之后,所述方法还包括:

数据源服务器接收所述第三方系统转发的所述数据访问请求;

所述数据源服务器访问所述第一服务器或所述上下文信息服务器,如果查询得到所述账户的所述合法访问标识信息,则确定所述合法账户发起的所述数据访问请求为安全访问请求;

10 所述数据源服务器向所述第三方系统返回所述数据访问请求所要访问的数据。

6、根据权利要求 5 所述的方法,其特征在于,在确定发起所述数据访问请求的所述账户为安全访问账户之后,所述方法还包括:

所述数据源服务器验证所述上下文信息中是否包含所述账户的在线信息;

15 当所述上下文信息中包含所述账户的在线信息时,所述数据源服务器执行向所述第三方系统返回所述数据访问请求所要访问的数据的步骤。

7、根据权利要求 5 所述的方法,其特征在于,当所述上下文信息中还包括所述账户的安全隐私等级信息时,所述数据源服务器向所述第三方系统返回所述数据访问请求所要访问的数据的步骤包括:所述数据源服务器根据所述安全隐私等级信息生成对应的第一访问数据,并将所述第一访问数据返回至所述第三方系统。

20 8、根据权利要求 5 所述的方法,其特征在于,当所述上下文信息中还包括所述账户的安全风险状态信息时,所述数据源服务器向所述第三方系统返回所述数据访问请求所要访问的数据的步骤包括:所述数据源服务器所述安全风险状态信息生成对应的第二访问数据,并将所述第二访问数据返回至所述第三方系统。

25 9、根据权利要求 1 所述的方法,其特征在于,所述第一服务器在确定所述数据访问请求中没有包含所述账户的上下文信息,或在所述账户的上下文信息校验失败的情况下,所述第一服务器发送所述数据访问请求至所述第三方系统,或者所述第一服务器禁止发送所述数据访问请求至所述第三方系统,并发出报警信息。

10、一种用户数据的访问控制方法,其特征在于,包括:

客户端获取账户的上下文信息;

30 所述客户端发送所述账户触发的数据访问请求至第一服务器,其中,所述数据访问

请求至少包括所述上下文信息；

所述客户端接收所述第一服务器根据所述数据访问请求获取到的访问数据；

其中，在所述第一服务器确定所述数据访问请求中包含所述账户的上下文信息，和/或在所述账户的上下文信息校验通过的情况下，允许发送所述数据访问请求至第三方系统，使得所述第三方系统根据所述数据访问请求访问数据源。

11、根据权利要求 10 所述的方法，其特征在于，客户端获取登录账户的上下文信息，包括：

所述账户登录所述客户端之后，向登录服务器发起登录请求；

所述客户端接收所述登录服务器返回的所述上下文信息，其中，所述上下文信息为所述登录服务器根据所述登录请求生成的完整上下文信息中的子集。

12、一种用户数据的访问控制方法，其特征在于，包括：

第三方系统接收第一服务器发送的数据访问请求，其中，所述数据访问请求为由账户发起的包含了所述账户的上下文信息的请求；

所述第三方系统转发所述数据访问请求至数据源服务器；

所述第三方系统接收所述数据源服务器返回的所述数据访问请求所要访问的数据，其中，当所述数据源服务器根据所述数据访问请求中包含的所述上下文信息，确定发起所述数据访问请求的所述账户为安全访问账户，且所述数据访问请求为安全访问请求时，允许所述第三方系统根据所述数据访问请求访问数据源。

13、根据权利要求 12 所述的方法，其特征在于，在第三方系统接收第一服务器发送的数据访问请求之前，所述方法还包括：

在所述第一服务器确定所述数据访问请求中携带所述账户的上下文信息，且所述账户的上下文信息为合法信息的情况下，生成所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起的所述数据访问请求的所述账户为合法账户。

14、根据权利要求 13 所述的方法，其特征在于，所述数据源服务器根据所述数据访问请求中包含的所述上下文信息，确定发起所述数据访问请求的所述账户为安全访问账户，且所述数据访问请求为安全访问请求包括：

所述数据源服务器接收所述第三方系统转发的所述数据访问请求；

所述数据源服务器读取所述数据访问请求中携带的所述上下文信息；

在所述数据源服务器验证所述上下文信息为合法信息时，确定发起所述数据访问请求的所述账户为安全访问账户，且在查询得到所述账户具有所述合法访问标识信息时，

确定所述数据访问请求为所述安全访问请求。

15、根据权利要求 12 所述的方法，其特征在于，在第三方系统接收第一服务器发送的所述数据访问请求之前，所述方法还包括：

所述第一服务器验证所述数据访问请求中是否携带所述账户的上下文信息，和/或对
5 所述账户的上下文信息进行校验；

所述第一服务器在确定所述数据访问请求中包含所述账户的上下文信息，和/或在所述账户的上下文信息校验通过的情况下，允许发送所述数据访问请求至第三方系统，使得所述第三方系统根据所述数据访问请求访问数据源；

所述第一服务器在确定所述数据访问请求中没有包含所述账户的上下文信息，和/或
10 或在所述账户的上下文信息校验失败的情况下，所述第一服务器仍旧发送所述数据访问请求至所述第三方系统，或者所述第一服务器禁止发送所述数据访问请求至所述第三方系统，并发出报警信息。

16、一种用户数据的访问控制装置，其特征在于，包括：

接收模块，用于接收账户发起的数据访问请求；

15 校验模块，包含第一校验单元和/或第二校验单元，其中，所述第一校验单元用于验证所述数据访问请求中是否携带所述账户的上下文信息，所述第二校验单元对所述账户的上下文信息进行校验；

控制模块，用于在校验模块校验通过的情况下，允许发送所述数据访问请求至第三方系统，使得所述第三方系统根据所述数据访问请求访问数据源。

20 17、根据权利要求 16 所述的装置，其特征在于，所述第二校验单元包括：

读取子单元，用于在确定所述数据访问请求中携带所述上下文信息之后，读取所述数据访问请求中携带的所述上下文信息；

匹配子单元，用于将所述上下文信息与预存的完整上下文信息进行匹配，在匹配成功的情况下，确定所述账户的上下文信息为合法信息；

25 生成子单元，用于生成所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起所述数据访问请求的所述账户为合法账户。

18、根据权利要求 16 所述的装置，其特征在于，所述第二校验单元包括：

发送子单元，用于在确定所述数据访问请求中携带所述上下文信息之后，发送所述上下文信息至上下文信息服务器；

30 第一接收子单元，用于接收所述上下文信息服务器验证所述上下文信息的验证结

果；

第二接收子单元，用于在所述验证结果为所述账户的上下文信息为合法信息的情况下，接收所述上下文信息服务器生成的所述账户的合法访问标识信息，其中，所述合法访问标识信息用于表征发起的所述数据访问请求的所述账户为合法账户；所述上下文信息服务器将所述上下文信息与预存在本地的完整上下文信息进行匹配，在匹配成功的情况下，所述验证结果为所述账户的上下文信息为所述合法信息。

19、根据权利要求 16 所述的装置，其特征在于，所述控制模块还用于在校验模块校验不通过的情况下，发送所述数据访问请求至所述第三方系统，或者禁止发送所述数据访问请求至所述第三方系统，并发出报警信息。

10 20、一种用户数据的访问控制装置，其特征在于，包括：

获取模块，用于获取账户的上下文信息；

发送模块，用于发送所述账户触发的数据访问请求至第一服务器，其中，所述数据访问请求至少包括所述上下文信息；

接收模块，用于接收所述第一服务器根据所述数据访问请求获取到的访问数据；

15 其中，在所述第一服务器确定所述数据访问请求中包含所述账户的上下文信息，和/或在所述账户的上下文信息校验通过的情况下，允许发送所述数据访问请求至第三方系统，使得所述第三方系统根据所述数据访问请求访问数据源。

21、根据权利要求 20 所述的装置，其特征在于，获取模块包括：

发送单元，用于向登录服务器发起登录请求；

20 接收单元，用于接收所述登录服务器返回的所述上下文信息，其中，所述上下文信息为所述登录服务器根据所述登录请求生成的完整上下文信息中的子集。

22、一种用户数据的访问控制装置，其特征在于，包括：

第一接收模块，用于接收第一服务器发送的数据访问请求，其中，所述数据访问请求为由账户发起的包含了所述账户的上下文信息的请求；

25 转发模块，用于转发所述数据访问请求至数据源服务器；

第二接收模块，用于接收所述数据源服务器返回的所述数据访问请求所要访问的数据，

其中，当所述数据源服务器根据所述数据访问请求中包含的所述上下文信息，确定发起所述数据访问请求的所述账户为安全访问账户，且所述数据访问请求为安全访问请求时，允许第三方系统根据所述数据访问请求访问数据源。

30

23、一种用户数据的访问控制系统，其特征在于，包括：

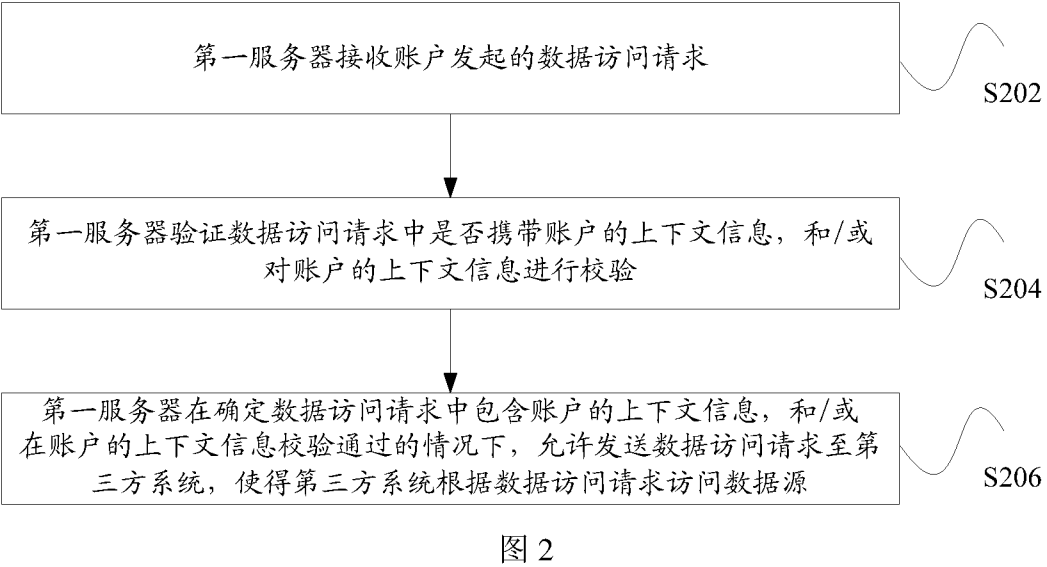
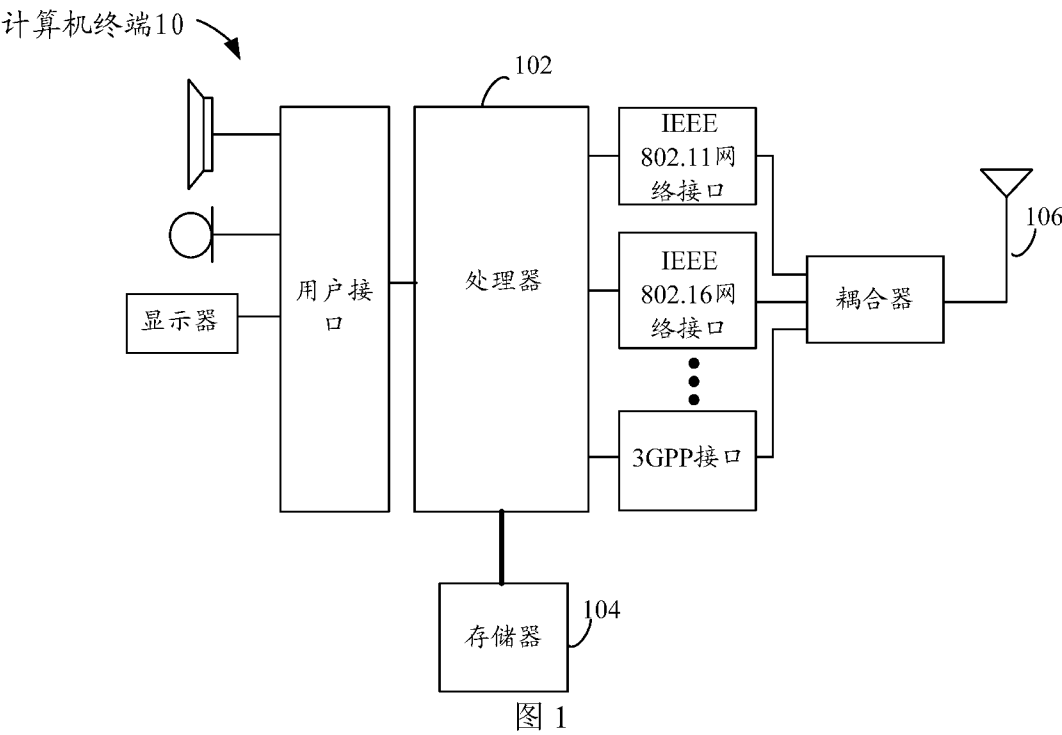
客户终端，用于在账户登录之后，发起数据访问请求；

第一服务器，与所述客户终端通信，用于在验证所述数据访问请求中包含了所述账户的上下文信息，和/或验证所述上下文信息为合法信息之后，透传所述数据访问请求；

5 第三方系统服务器，与所述第一服务器通信，用于接收所述第一服务器透传的所述数据访问请求；

数据源服务器，与所述第三方系统服务器通信，用于接收所述第三方系统服务器通信转发的所述数据访问请求，在根据所述数据访问请求中包含的所述上下文信息，确定发起所述数据访问请求的所述账户为安全访问账户，且所述数据访问请求为安全访问请求时，返回所述数据访问请求对应的访问数据至所述第三方系统服务器。

10



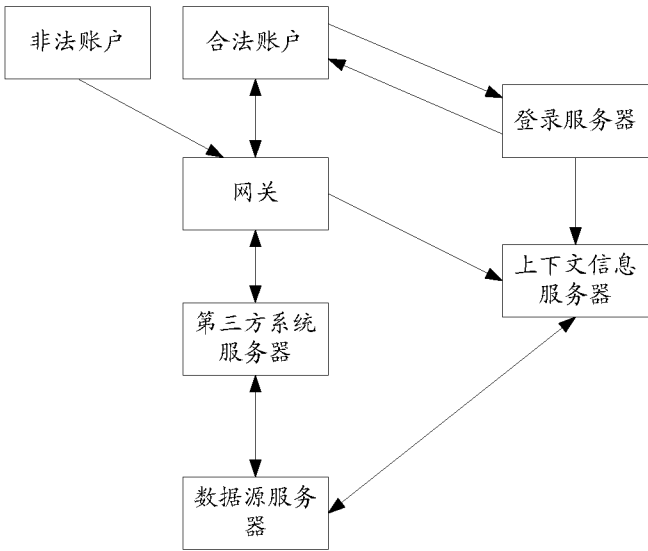


图 3

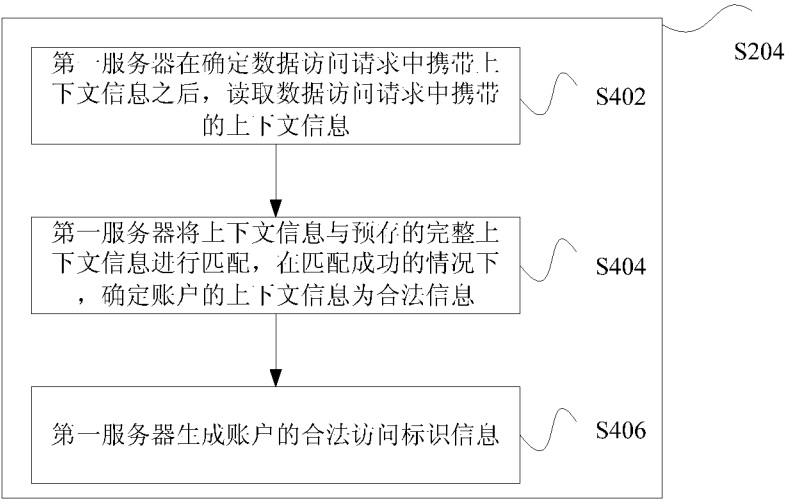


图 4

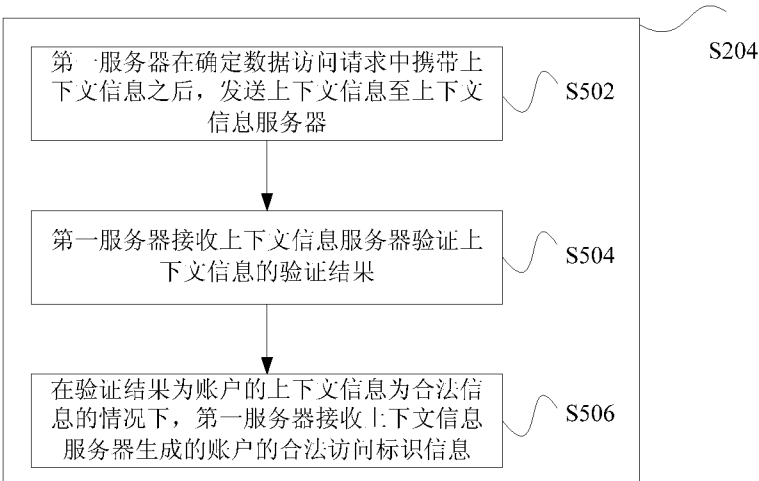


图 5

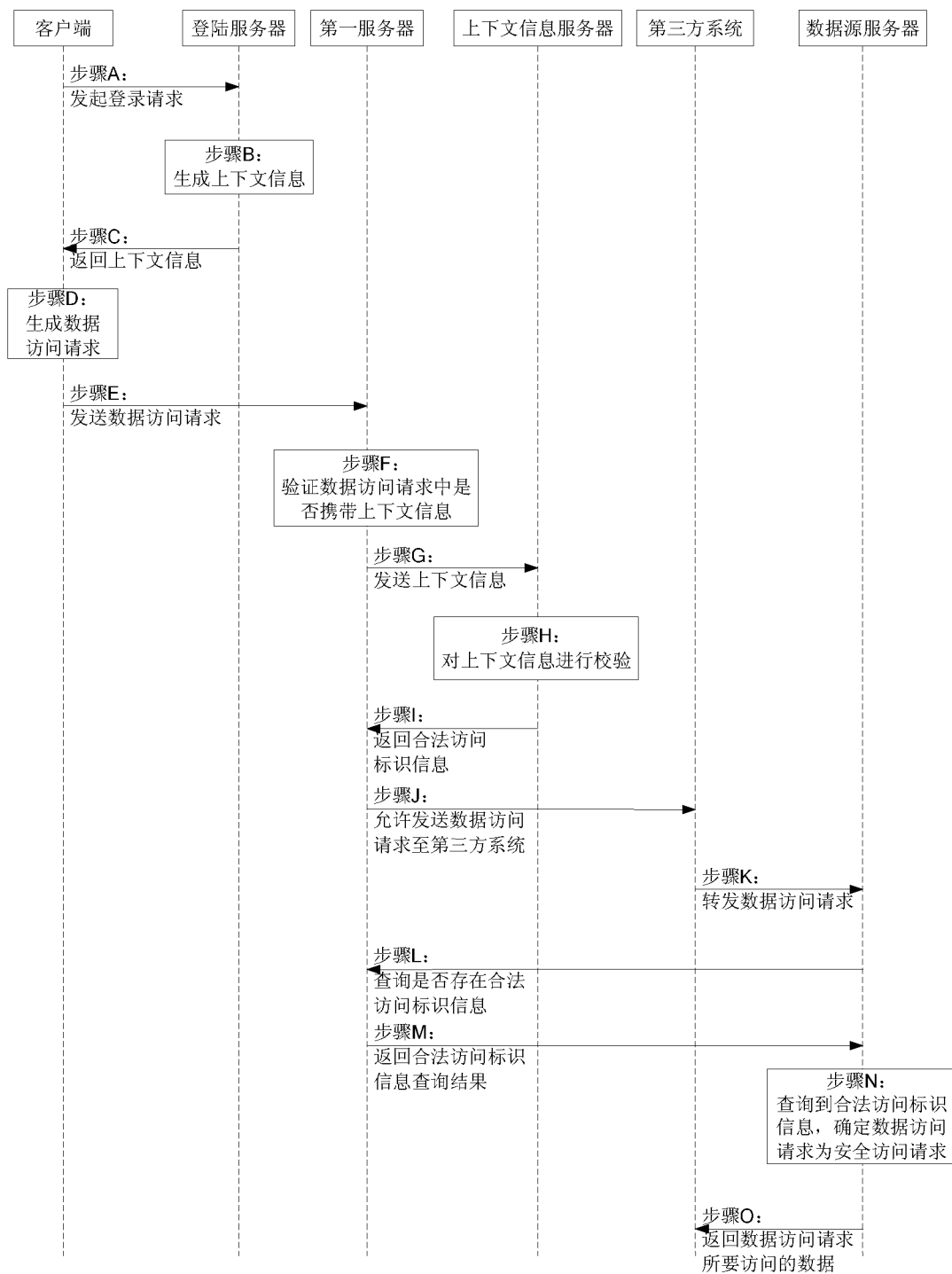


图 6

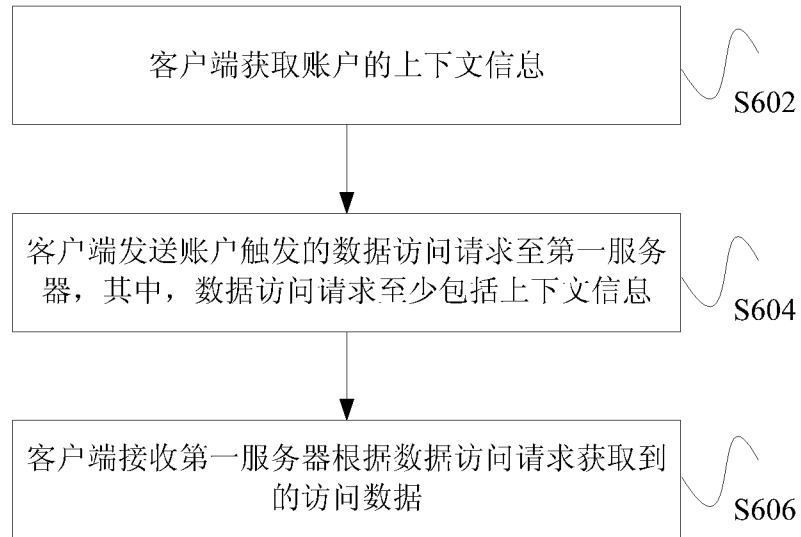


图 7

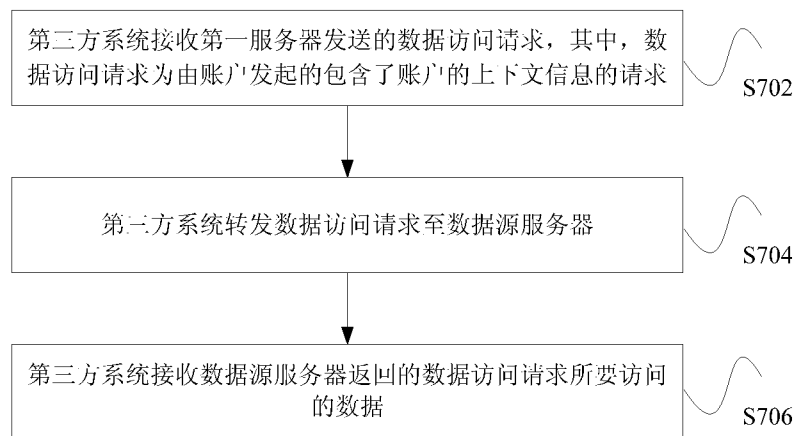


图 8



图 9

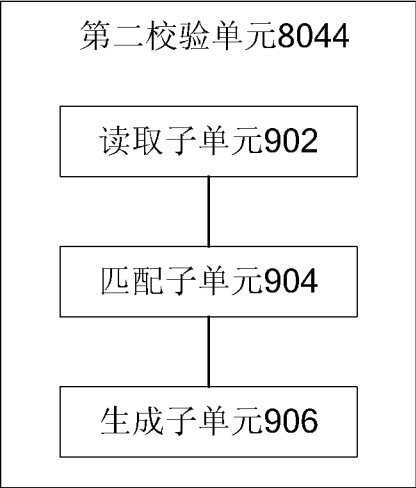


图 10

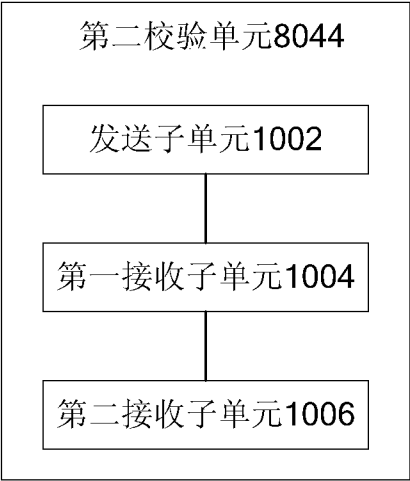


图 11



图 12



图 13

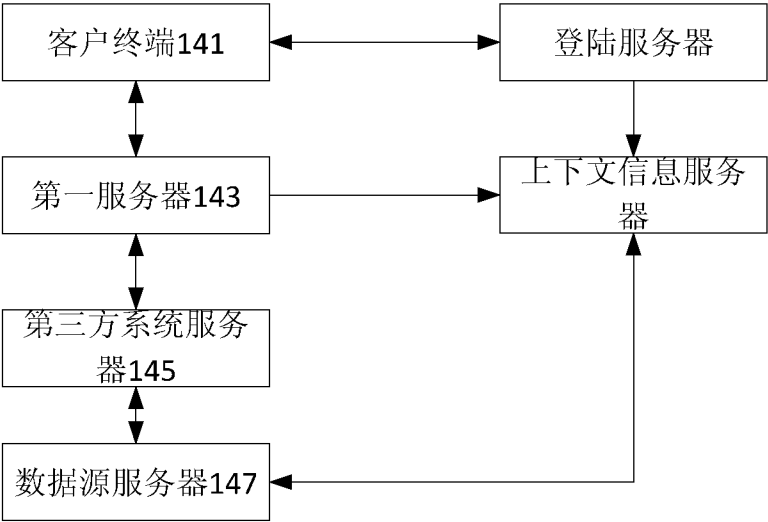


图 14

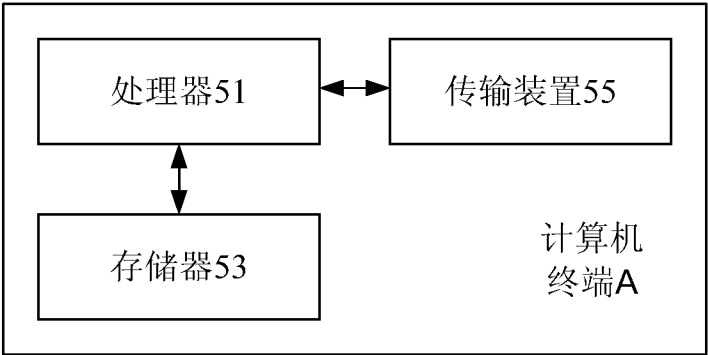


图 15

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/082162

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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)

H04L; H04W; H04Q

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)

WPI; EPODOC; CNKI; CNPAT: time, common, data source, user, account, data, request, control, context, address, location, state, verify, authenticate, server, legal, third party, source, gateway

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103297437 A (CHINA NATIONAL SOFTWARE & SERVICE CO., LTD.), 11 September 2013 (11.09.2013), description, paragraphs 0035-0047 and 0060-0073, and figures 1-4	1-23
A	CN 104518876 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.), 15 April 2015 (15.04.2015), the whole document	1-23
A	US 2008134305 A1 (HINTON, H.M. et al.), 05 June 2008 (05.06.2008), the whole document	1-23

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 16 July 2016 (16.07.2016)	Date of mailing of the international search report 10 August 2016 (10.08.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LIU, Qingfeng Telephone No.: (86-10) 62413279

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/082162

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103297437 A	11 September 2013	None	
CN 104518876 A	15 April 2015	WO 2015043224 A1	02 April 2015
		US 2015096004 A1	02 April 2015
US 2008134305 A1	05 June 2008	EP 1964360 A1	03 September 2008
		JP 2009519529 A	14 May 2009
		CN 101331735 A	24 December 2008
		TW 200810458 A	16 February 2008
		WO 2007068715 A1	21 June 2007

国际检索报告

国际申请号

PCT/CN2016/082162

A. 主题的分类

H04L 29/06(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)

H04L; H04W; H04Q

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))

WPI; EPODOC; CNKI; CNPAT: 数据, 请求, 控制, 上下文, 地址, 时间, 常用, 状态, 校验, 验证, 服务器, 合法, 第三方, 数据源, 用户, 账户, 网关, data, request, control, context, address, location, state, verify, authenticate, server, legal, third party, source, gateway

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 103297437 A (中国软件与技术服务股份有限公司) 2013年 9月 11日 (2013 - 09 - 11) 说明书第0035-0047、0060-0073段, 图1-4	1-23
A	CN 104518876 A (腾讯科技深圳有限公司) 2015年 4月 15日 (2015 - 04 - 15) 全文	1-23
A	US 2008134305 A1 (HINTON, HEATHER M. 等) 2008年 6月 5日 (2008 - 06 - 05) 全文	1-23

☐ 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

2016年 7月 16日

国际检索报告邮寄日期

2016年 8月 10日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(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

授权官员

刘庆峰

电话号码 (86-10)62413279

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/082162

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	103297437	A	2013年 9月 11日	无			
CN	104518876	A	2015年 4月 15日	WO	2015043224	A1	2015年 4月 2日
				US	2015096004	A1	2015年 4月 2日
US	2008134305	A1	2008年 6月 5日	EP	1964360	A1	2008年 9月 3日
				JP	2009519529	A	2009年 5月 14日
				CN	101331735	A	2008年 12月 24日
				TW	200810458	A	2008年 2月 16日
				WO	2007068715	A1	2007年 6月 21日

表 PCT/ISA/210 (同族专利附件) (2009年7月)