(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116155565 B
(45)授权公告日 2023.10.10

(21)申请号 202310008006.2

(22)申请日 2023.01.04

(65)同一申请的已公布的文献号
申请公布号 CN 116155565 A

(43)申请公布日 2023.05.23

(73)专利权人 北京夏石科技有限责任公司
地址 100020 北京市朝阳区北苑东路19号院3号楼2层212

(72)发明人 范鹏 陈岌 李文军

(74)专利代理机构 北京细软智谷知识产权代理有限责任公司 11471
专利代理师 葛钟

(51)Int.Cl.
H04L 9/40(2022.01)
G06F 21/31(2013.01)
G06F 21/60(2013.01)
G06F 21/64(2013.01)

(56)对比文件
CN 113849789 A,2021.12.28
CN 113067797 A,2021.07.02
CN 115062211 A,2022.09.16
CN 115277207 A,2022.11.01
CN 114237625 A,2022.03.25
CN 112769735 A,2021.05.07
US 2020358615 A1,2020.11.12
CN 111030828 A,2020.04.17
张锐;张建林;孙国忠.多业务系统的统一认证授权研究与设计.计算机工程与设计.2009,(08),第1826-1828页.
杨薪燕.基于Spring的Acegi安全框架在Web系统中的应用与分析.中国西部科技.2009,(05),第54-56页.

审查员 魏慧慧

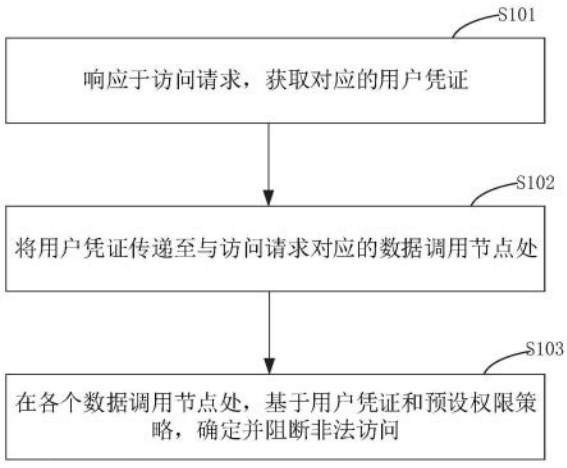
权利要求书2页 说明书8页 附图3页

(54)发明名称

数据访问控制方法和装置

(57)摘要

本发明涉及安全技术领域,具体涉及一种数据访问控制方法和装置,该方法包括:首先在各个数据调用节点中,基于用户信息和该调用节点内的数据,进行权限管理,得到权限策略;在当收到数据访问请求后,将用户凭证发送至对应的各个数据调用节点处,从而在各个数据调用节点处,基于用户凭证和权限策略,确定非法访问,并及时阻断,从而在根本上解决了涉及数据调用的安全问题。



CN 116155565 B

1.一种数据访问控制方法,其特征在于,包括:

响应于访问请求,通过预设微代理,基于安全平行切面技术,获取对应的用户凭证;

获取所述访问请求的上下文数据,其中,所述上下文数据包括上下文线程、请求环境和执行时间;

基于所述上下文数据,确定目标数据调用节点;

将所述用户凭证转换为opentracing标准协议数据,并传递至所述目标数据调用节点处;

在各个所述数据调用节点处,基于所述用户凭证和预设权限策略,确定并阻断非法访问;

其中,所述预设权限策略基于待测系统中用户信息和各个所述数据调用节点内的数据生成的,且所述权限策略与各个数据调用节点一一对应,所述数据调用节点内的数据包括数据库中的库表和字段。

2.根据权利要求1所述的数据访问控制方法,其特征在于,所述预设权限策略的生成过程,包括:

基于所述用户信息和所述数据调用节点内的数据,通过预设属性授权引擎,生成所述权限策略。

3.根据权利要求2所述的数据访问控制方法,其特征在于,所述将所述用户凭证传递至与所述访问请求对应的数据调用节点处,还包括:

在调用系统发送所述opentracing标准协议数据和所述上下文数据之前,进行签名和加密处理;

和在被调用系统接收所述opentracing标准协议数据和所述上下文数据之后,进行解密和校验处理。

4.根据权利要求1所述的数据访问控制方法,其特征在于,还包括:

基于所述用户凭证和所述预设权限策略,确定对应用户的访问权限;

基于所述访问权限,确定对应用户的可访问数据;

基于所述访问请求,对所述可访问数据进行操作。

5.根据权利要求1所述的数据访问控制方法,其特征在于,还包括:

对所述访问请求对应的访问行为和流转数据进行跟踪记录;

基于所述跟踪记录结果,分析确定权限策略优化方案。

6.根据权利要求1所述的数据访问控制方法,其特征在于,还包括:

基于接口调用策略,进行接口权限验证;

并在所述接口权限验证通过后,且基于所述用户凭证和所述预设权限策略,确定所述用户凭证对应的权限后,基于所述预设权限策略,进行数据调用。

7.根据权利要求1所述的数据访问控制方法,其特征在于,所述数据调用节点包括前端应用、业务服务层应用和数据库服务。

8.一种数据访问控制装置,其特征在于,包括:

通讯模块,用于响应于访问请求,通过预设微代理,基于安全平行切面技术,获取对应的用户凭证;

所述通讯模块,还用于获取所述访问请求的上下文数据,其中,所述上下文数据包括上

下文线程、请求环境和执行时间;基于所述上下文数据,确定目标数据调用节点;将所述用户凭证转换为opentracing标准协议数据,并传递至所述目标数据调用节点处;计算模块,用于在各个所述数据调用节点处,基于所述用户凭证和预设权限策略,确定并阻断非法访问;其中,所述预设权限策略基于待测系统中用户信息和各个所述数据调用节点内的数据生成的,且所述权限策略与各个数据调用节点一一对应,所述数据调用节点内的数据包括数据库中的库表和字段。

数据访问控制方法和装置

技术领域

[0001] 本发明涉及数据安全技术领域，具体涉及一种数据访问控制方法和装置。

背景技术

[0002] 随着网络技术的不断发展，各种应用的功能也越来越强大，其中，在包括微服务架构等中，某一个功能的实现往往需要依赖多个服务，例如应用入口处的系统或服务需要通过接口调用其他系统或服务内的数据，所以，如何保证数据在各个系统或服务之间调用流转过程中的安全，对于应用或系统的安全尤为重要。

[0003] 现有技术中，一般是在入口处的系统或服务中对用户身份进行验证，以及在入口处的系统或服务在通过接口调用其他系统或服务的数据过程中，对调用系统或服务的接口权限进行验证，若其有该接口的权限，则可以获取该接口返回的数据，在一定程度上能够保证数据安全。

[0004] 但是，当攻击者绕过入口处的系统服务的访问控制机制时，后面各个系统或服务均无法对攻击进行有效防护，数据安全仍然存在较大的安全隐患。

发明内容

[0005] 有鉴于此，本发明的目的在于提供一种数据访问控制方法和装置，以克服目前数据调用过程中安全性差的问题。

[0006] 为实现以上目的，本发明采用如下技术方案：

[0007] 第一方面，本申请提供一种数据访问控制方法，包括：

[0008] 响应于访问请求，获取对应的用户凭证；

[0009] 将所述用户凭证传递至与所述访问请求对应的数据调用节点处；

[0010] 在各个所述数据调用节点处，基于所述用户凭证和预设权限策略，确定并阻断非法访问；

[0011] 其中，所述预设权限策略基于待测系统中用户信息和各个所述数据调用节点内的数据生成的。

[0012] 可选地，所述预设权限策略的生成过程，包括：

[0013] 基于所述用户信息和所述数据调用节点内的数据，通过预设属性授权引擎，生成所述权限策略；

[0014] 其中，所述权限策略与各个数据调用节点一一对应，所述数据调用节点内的数据包括数据库中的库表和字段。

[0015] 可选地，所述获取对应的用户凭证，包括：

[0016] 通过预设微代理，基于安全平行界面技术，获取用户凭证。

[0017] 可选地，所述将所述用户凭证传递至与所述访问请求对应的数据调用节点处，包括：

[0018] 获取所述访问请求的上下文数据，其中，所述上下文数据包括上下文线程、请求环

境和执行时间；

[0019] 基于所述上下文数据，确定目标数据调用节点；

[0020] 将所述用户凭证转换为opentracing标准协议数据，并传递至所述目标数据调用节点处。

[0021] 可选地，所述将所述用户凭证传递至与所述访问请求对应的数据调用节点处，还包括：

[0022] 在调用系统发送所述opentracing标准协议数据和所述上下文数据之前，进行签名和加密处理；

[0023] 和在被调用系统接收所述opentracing标准协议数据和所述上下文数据之后，进行解密和校验处理。

[0024] 可选地，还包括：

[0025] 基于所述用户凭证和所述预设权限策略，确定对应用户的访问权限；

[0026] 基于所述访问权限，确定对应用户的可访问数据；

[0027] 基于所述访问请求，对所述可访问数据进行操作。

[0028] 可选地，还包括：

[0029] 对所述访问请求对应的访问行为和流转数据进行跟踪记录；

[0030] 基于所述跟踪记录结果，分析确定权限策略优化方案。

[0031] 可选地，还包括：

[0032] 基于接口调用策略，进行接口权限验证；

[0033] 并在所述接口权限验证通过后，且基于所述用户凭证和所述预设权限策略，确定所述用户凭证对应的权限后，基于所述预设权限策略，进行数据调用。

[0034] 可选地，所述数据调用节点包括前端应用、业务服务层应用和数据库服务。

[0035] 第二方面，本申请还提供一种数据访问控制装置，包括：

[0036] 通讯模块，用于响应于访问请求，获取对应的用户凭证；

[0037] 所述通讯模块，还用于将所述用户凭证传递至与所述访问请求对应的数据调用节点处；

[0038] 计算模块，用于在各个所述数据调用节点处，基于所述用户凭证和预设权限策略，确定并阻断非法访问；其中，所述预设权限策略基于待测系统中用户信息和各个所述数据调用节点内的数据生成的。

[0039] 本申请提供的数据访问控制策略，首先在各个数据调用节点中，基于用户信息和该调用节点内的数据，进行权限管理，得到权限策略；在当收到数据访问请求时，将对应的用户凭证发送至对应的各个数据调用节点处，从而在各个数据调用节点处，基于用户凭证和权限策略，确定非法访问，并及时阻断，从而在根本上解决了涉及数据调用时的安全问题。

附图说明

[0040] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以

根据这些附图获得其他的附图。

[0041] 图1是本申请实施例提供的数据访问控制方法的流程示意图；

[0042] 图2是本申请实施例提供的数据访问控制方法的具体流程图；

[0043] 图3为本申请实施例提供的数据访问控制方法中用户凭证透转的流程示意图；

[0044] 图4为本申请实施例提供的数据访问控制方法中用户凭证透转的实现结构示意图；

[0045] 图5为本申请实施例提供的数据访问控制方法中权限策略的应用流程图；

[0046] 图6为本申请实施例提供的数据访问控制方法中的数据流转图；

[0047] 图7为本申请实施例提供的数据访问控制装置的应用流程图。

具体实施方式

[0048] 为使本发明的目的、技术方案和优点更加清楚，下面将对本发明的技术方案进行详细的描述。显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所得到的所有其它实施方式，都属于本发明所保护的范围。

[0049] 申请概述：

[0050] 目前应用系统身份验证都是在应用系统的入口处(如MVC模型的控制或模型层里)进行用户身份验证的，如果验证不通过则用户被拒绝登陆或拒绝访问系统的数据资源，如果验证通过用户即可具备对应身份的角色，从而可以访问系统数据。

[0051] 随着应用功能的不断强大，以及各种架构的产生，例如在一些微服务架构中，某一个应用以及某一个功能往往需要依赖多个系统或服务配合来完成，此时，入口处的系统或服务会调用其它系统或服务接口完成响应的业务逻辑操作。现有技术中，一般由入口出的系统或服务获取用户的身份凭证，进行验证，在该处验证通过后，后续入口出的系统或服务与其他系统或服务之间调用数据时，只需要检测进行接口调用的内容，例如包括验证调用者(其它系统)是否被授权、调用通道是否被加密、以及调用者所在机器的黑白名单设置等。这种后端系统服务接口权限控制方式是粗粒度的资源权限控制，有该接口的权限即可获取该接口返回的所有数据，而不论在最初系统服务入口处登陆的用户的身份凭证如何，即不对登陆用户身份进行验证或数据访问鉴权，因此，一旦应用程序遭受攻击，攻击者绕过入口处应用系统正常的访问控制机制，即可发生非授权访问，后续的系统或服务无能为力，存在较大的安全隐患。

[0052] 另外，现有系统在数据库调用过程中，包括对于个人隐私数据查询访问和检测过程中，也仅是在应用系统处对操作用户进行身份验证，而后数据库只能看到应用系统ID，应用系统ID校验成功即可通过接口调用数据库，以查询个人隐私数据。

[0053] 因此，上述方案存在无法判断调用行为是否由用户发起，应用系统通过接口访问数据库，但是该调用行为是否存在风险，应用系统自身无法判断，因为该访问行为可由用户正常业务使用触发，也可在应用系统所在主机上人为异常触发。而且，从应用所在主机直接访问数据库接口时，应用系统无法判断是否正常，无法快速地针对查询数据内容进行检测，进一步判断查询行为是否正常。

[0054] 本申请提供的数据访问控制方法和装置，首先通过用户凭证透传及转发技术，将

系统服务入口处已经鉴权完成的用户身份凭证，在之后所有的接口调用链路上进行透传转发，所有被调用的接口都可以获得用户身份凭证，接口被哪个用户使用，接口数据被哪个用户访问，可以清清楚楚地跟踪及控制。同时，预先对所有接口里的数据进行细粒度的权限管控，即对该接口里的逻辑代码访问的数据库表和字段进行权限策略管理，针对透传转发过来的用户凭证里的用户标识进行关联授权管理，对未授权用户的非法访问进行及时判断并及时阻断，大大提高了数据的安全性。下面将以实施例的方式对本申请方案进行详细阐述。

[0055] 方法实施例：

[0056] 图1是本申请实施例提供的数据访问控制方法的流程示意图，图2是本申请实施例提供的数据访问控制方法的具体流程图，请参阅图1和图2，本实施例可以包括以下步骤：

[0057] S101、响应于访问请求，获取对应的用户凭证。

[0058] 具体的，访问请求可以是访问者在业务表现层/MVC层，例如应用前端生成的，当检测到存在访问请求时，获取包括用户信息的用户凭证。

[0059] 可以理解的是，在获取用户信息时，还可以在该层对用户信息进行验证。如果用户没有通过验证，则直接阻断访问或登录，若用户通过验证，继续后面的流程。

[0060] 需要说明的是，用户凭证可是用户个人信息，也可以是入口处的系统或服务例如前端应用基于用户个人信息检测生成的用户凭证。

[0061] S102、将用户凭证传递至与访问请求对应的数据调用节点处。

[0062] 具体的，因为访问可能涉及多个数据调用节点，例如图2中的多个应用、服务和对应的数据库，此时将用户凭证传递至上述访问请求对应的数据调用节点处，即将用户凭证在前端应用、业务服务层应用和数据库服务之间转发，具体转发过程如图2所示。

[0063] S103、在各个数据调用节点处，基于用户凭证和预设权限策略，确定并阻断非法访问。

[0064] 其中，预设权限策略基于待测系统中用户信息和各个数据调用节点内的数据生成的。

[0065] 具体的，在待检测系统数据安全运营期间，即进行访问控制之前，基于系统中用户信息和数据调用节点内的数据生成权限策略，例如，对所有数据库的表、字段分别进行了安全级别属性的定义，同时对各个用户能够访问哪些安全级别的表和字段进行授权。

[0066] 在实际检测和访问控制时，因为各层的应用服务(包括图2中的业务表现层/MVC层、业务服务层和数据持久层)里均有存在被转发的用户凭证，因此，各层的应用服务均可以对用户凭证进行合法性校验，根据用户凭证里的用户标识信息，进行数据库表、字段的访问权限校验，判断该用户是否有访问或操作该数据的权限，以及具体可以访问那些数据，当访问用户的权限与其访问的数据不匹配时，及时判决为非法访问，并及时阻断访问。如此，当正常用户访问时，可以顺利完成访问，而攻击者即使绕过了应用前端的检验，在后续的流程中也会被发现和阻断。

[0067] 本申请提供的数据访问控制方法，首先基于用户信息将各个接口对应的数据调用节点内的数据进行细粒度的权限管控，在实际应用时，将用户凭证透传至各个数据调用节点处，在各个数据调用节点处进行身份验证，从而可以在系统服务的调用链路中，及时发现并阻断非法用户、没有得到已授权用户凭证的访问，以及访问用户凭证授权以外的数据。从而避免了现有技术中，攻击者绕过入口处的系统服务即可访问各种数据，实现应用系统非

法数据访问的实时判决和阻断，大大提高了系统的安全性。

[0068] 进一步的，在本申请提供的数据访问控制方法，预设权限策略的生成过程可以包括：基于用户信息和数据调用节点内的数据，通过预设属性授权引擎，生成权限策略；其中，权限策略与各个数据调用节点一一对应，数据调用节点内的数据包括数据库中的库表和字段。

[0069] 具体的，如图2所示，各个数据调用节点均对应各自的数据库，各个数据库中具体到库表和字段的内容，可以通过预设的权限管理平台中的属性授权引擎即ABAC授权引擎，在后端进行权限策略管理。以及在实际检测过程中，通过agent微代理获取各个数据调用节点处的用户凭证，通过权限管理平台，完成分布式系统调用的全链路用户鉴权，即在微服务的分布式链路调用过程中的任何节点，都进行用户访问数据资源的权限校验，从而提高系统安全性。

[0070] 在本申请一些实施例中，可以在第三方业务系统(进行访问控制的业务系统)或服务所在的机器上，例如对应的服务器上任意位置部署agent微代理，通过预设agent微代理，基于安全平行切面技术获取用户凭证，从而避免部署实施时给客户带来任何额外开发成本的增加。其中，安全平行切面技术是AOP思想在安全领域的创新应用，通过该技术可以实现业务系统零耦合安全逻辑，通过切面的方式保障系统的安全性，避免对第三方业务系统的改造，大大提高用户体验。

[0071] 图3为本申请实施例提供的数据访问控制方法中用户凭证透转的流程示意图，图4为本申请实施例提供的数据访问控制方法中用户凭证透转的实现结构示意图，如图3和图4所示，该过程可以包括：

[0072] S301、获取访问请求的上下文数据。

[0073] S302、基于上下文数据，确定目标数据调用节点。

[0074] 其中，上下文数据包括上下文线程、请求环境和执行时间等。

[0075] 具体的，上下文数据可以包括访问请求对应的上下文线程、请求环境和执行时间等信息，用于确定访问请求的访问情况，包括涉及的数据调用节点等信息。

[0076] 在通过agent基于切面技术获取用户凭证后以及上述上下文数据后，可以通过在切面构建的安全沙箱，来保障用户凭证以及其他上述数据的安全性、有效性以及不被篡改。其中，安全沙箱可以包括线程安全管理器11、请求环境安全管理器12、执行时间安全管理器13和用户凭证实时异步重校验服务14。

[0077] 其中，线程安全管理器11，用于保证线程信息的安全，请求环境安全管理器12用于保证请求环境信息的安全，执行时间安全管理器13用于保证执行时间数据的安全性，用户凭证实时异步重校验服务14用于将获取的用户凭证与预设权限管理平台中的用户信息进行检验，确定用户凭证正常。

[0078] S303、将用户凭证转换为opentracing标准协议数据，并传递至目标数据调用节点处。

[0079] 具体的，在对用户凭证进行在各个数据调用节点之间传递时，可以将用户凭证转换为opentracing标准协议数据，以opentracing标准协议数据的格式在各个节点之间传递，以保证传递过程中的安全以及传递效率。

[0080] 本申请提供的数据访问控制方法中，通过在切面探测到的上下文线程，以及通过

opentracing标准协议，保障经过权限验证后的用户凭证可以在该请求上下文中透传。而且，切面安全沙箱通过绑定线程标识、请求来源环境属性(IP、token创建时间等)、请求方式、时间序列及关键切面执行点之间的时间差、用户凭证重新校验机制等核心功能，实现了用户凭证在当前请求上下文环境的不同执行点的透传。

[0081] 在本申请一些实施例中，在通过Agent微代理基于安全平行切面技术实现了用户身份凭证的探测的基础上，通过opentracing标准库进行在多个系统间(或分布式服务间)传递。其中，还可以在数据透传过程中，通过对opentracing标准协议数据和所述上下文数据进行签名和加密，以及后续解密和校验，进一步保证数据透传的安全性。

[0082] 具体的，在传递过程中，通过预设权限管理平台中的tracing标准数据加解密校验服务，对opentracing标准协议数据和上述提到的上下文数据一起进行签名，然后对全部数据进行RSA加密。当下游被调用的接口服务或系统收到转发过来的用户凭证后，通过预设权限管理平台中的第三方业务系统秘钥管理服务，对签名和加密后的opentracing标准协议数据内容和用户上下文数据进行合法性校验，若没有被篡改，数据没有丢失，则完成用户凭证转发。具体如图4所示。

[0083] 现有技术中，在市面上所有其它安全类产品的实现中，只对接口的调用方进行了权限校验，这种权限校验是粗粒度的接口使用安全验证，没有细化的数据资产的细节，也就是只要拥有获取接口的访问令牌key，并且在接口的白名单中，即可对接口发起调用，造成较大安全隐患，而且当拥有上述条件时，可以针对该接口所有数据进行检索和操作，计算量也较大。

[0084] 在本申请一些实施例中，可以限制服务或系统之间的数据访问，并支持访问控制的全局分析。例如包括基于用户凭证和预设权限策略，确定对应用户的访问权限；再基于访问权限，确定对应用户的可访问数据；最后基于访问请求，对可访问数据进行操作。

[0085] 具体的，可以通过对数据库表和字段的安全属性的权限策略配置，限制接口数据访问方式，并授予所需要的最小界别的访问权限，即基于权限策略，确定用户可以访问的数据，进行只对允许该用户访问的数据进行检索和其他操作。如此，根据透传转发过来的用户凭证，在用户可访问的数据权限范围内进行数据的检索和操作，而不是扩大到接口所执行的更大的数据范围，最细力度保障了数据的安全性。

[0086] 另外，在本申请另一些实施例中，还可以在预设权限管理平台中设置审计行为分析服务或模块，通过该功能对访问行为轨迹和数据流转轨迹进行跟踪记录，和对所有接口数据访问或操作情况，以及数据流转情况进行管理，同时进行行为数据汇总分析，以在安全访问控制全局分析功能模块进行智能化的全链路分析和风险分析，为安全运营提供强有力的指导方案，如分析得到安全漏洞风险和完善方案。

[0087] 图5为本申请实施例提供的数据访问控制方法中权限策略的应用流程图，图6为本申请实施例提供的数据访问控制方法中的数据流转图，如图5和图6所示：

[0088] 首先可以通过预设权限管理平台中的ABAC授权引擎管理第三方系统(待检测控制系统)中的元数据及安全属性进行权限策略。在实际检测控制时，可以在基于agent检测各个服务或系统中的用户凭证的基础上，通过权限管理平台进行鉴权等，判断以及下发实时判决结果以及阻断访问指令等。其中，所有在第三方业务系统执行的数据操作都由其下发的权限策略进行控制。

[0089] 而且，业务系统接口里执行的所有操作关键执行点都可以由agent微代理探测到并进行权限策略执行的控制，从而实现根据访问用户的用户凭证的数据权限策略配置情况进行权限管控。

[0090] 进一步的，本申请实施例提供的数据访问控制方法，还包括：基于接口调用策略，进行接口权限验证；并在接口权限验证通过后，且基于用户凭证和预设权限策略，确定用户凭证对应的用户具有权限后，基于预设权限策略，进行数据调用。

[0091] 具体的，对于服务间的鉴权，不仅仅进行接口间权限验证，还要对终端用户身份进行鉴权，这正基于可转发的用户凭证和服务间数据访问限制的功能。这个功能就是利用用户凭证转发透传技术，将用户上线文数据带到请求全链路中，针对下游服务的数据访问，增加了终端用户身份权限校验，即该用户是否有访问该安全级别的数据权限。实现基于终端用户的身份控制服务间的授权。

[0092] 本申请提供的数据访问控制方法和装置，首先通过用户凭证透传及转发技术，将系统服务入口处已经鉴权完成的用户身份凭证，在之后所有的接口调用链路上进行透传转发，所有被调用的接口都可以获得用户身份凭证，接口被哪个用户使用，接口数据被哪个用户访问，可以清清楚楚地跟踪及控制。同时，预先对所有接口里的数据进行细粒度的权限管控，即对该接口里的逻辑代码访问的数据库表和字段进行权限策略管理，针对透传转发过来的用户凭证里的用户标识进行关联授权管理，对未授权用户的非法访问进行及时判断并及时阻断，大大提高了数据的安全性。

[0093] 装置实施例：

[0094] 基于同一个发明构思，本申请实施例提供的一种数据访问控制装置，如图7所示，该装置包括：

[0095] 通讯模块71，用于获取待测信息中的检测特征；

[0096] 计算模块72，用于分别计算检测特征与预设正常特征的第一相似度，和检测特征与预设异常特征的第二相似度；其中，异常特征从预设异常样本中提取得到，用于表征样本异常，正常特征从正常样本中提取得到；并基于第一相似度的倒数和第二相似度，确定待测信息的异常评分；

[0097] 计算模块72，还用于若异常评分大于预设阈值，则确定待测信息为异常信息。

[0098] 其中，通讯模块71可以通过agent微代理和opentracing标准库实现，以及计算模块72可以通过预设权限管理平台实现。关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

[0099] 本申请提供的数据访问控制装置，首先通过用户凭证透传及转发技术，将系统服务入口处已经鉴权完成的用户身份凭证，在之后所有的接口调用链路上进行透传转发，所有被调用的接口都可以获得用户身份凭证，接口被哪个用户使用，接口数据被哪个用户访问，可以清清楚楚地跟踪及控制。同时，预先对所有接口里的数据进行细粒度的权限管控，即对该接口里的逻辑代码访问的数据库表和字段进行权限策略管理，针对透传转发过来的用户凭证里的用户标识进行关联授权管理，对未授权用户的非法访问进行及时判断并及时阻断，大大提高了数据的安全性。

[0100] 可以理解的是，上述各实施例中相同或相似部分可以相互参考，在一些实施例中未详细说明的内容可以参见其他实施例中相同或相似的内容。

[0101] 需要说明的是，在本发明的描述中，术语“第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相对重要性。此外，在本发明的描述中，除非另有说明，“多个”的含义是指至少两个。

[0102] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0103] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0104] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0105] 此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，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模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

[0106] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0107] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0108] 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

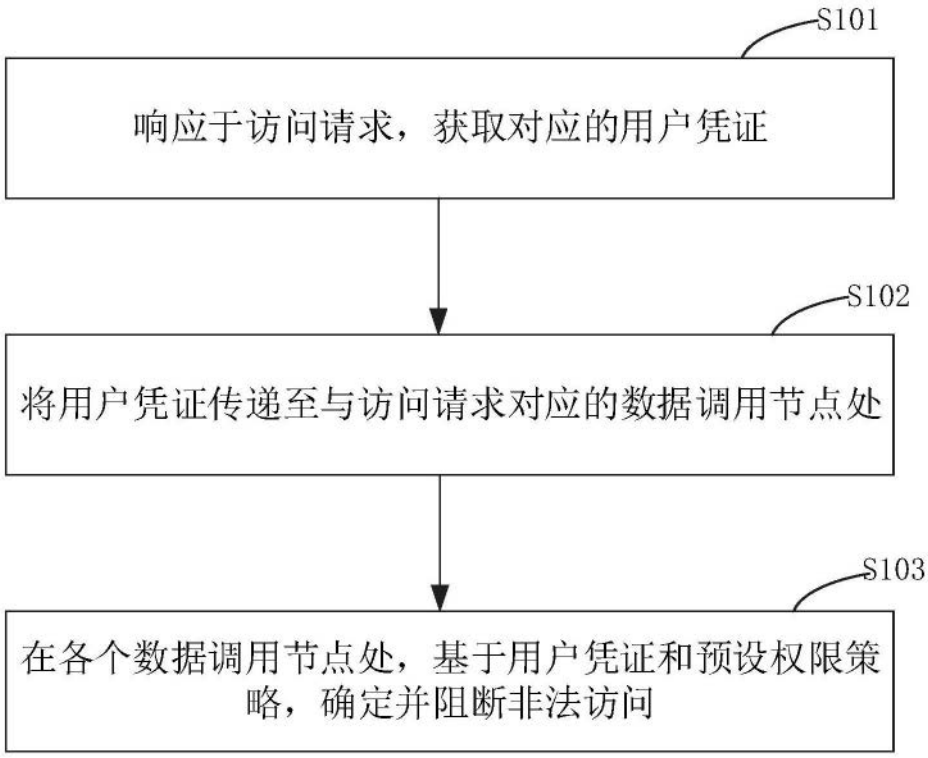

S101
响应于访问请求，获取对应的用户凭证
S102
将用户凭证传递至与访问请求对应的数据调用节点处
S103
在各个数据调用节点处，基于用户凭证和预设权限策略，确定并阻断非法访问

图1

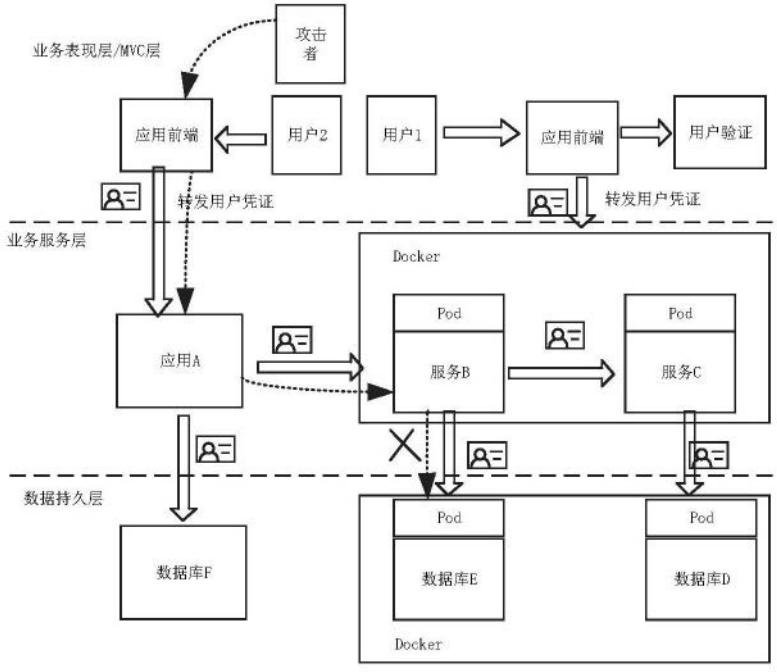

业务表现层/MVC层
攻击者
应用前端
用户2
用户1
应用前端
用户验证
转发用户凭证
转发用户凭证
业务服务层
Docker
Pod
Pod
应用A
服务B
服务C
数据持久层
Pod
Pod
数据库F
数据库E
数据库D
Docker

图2

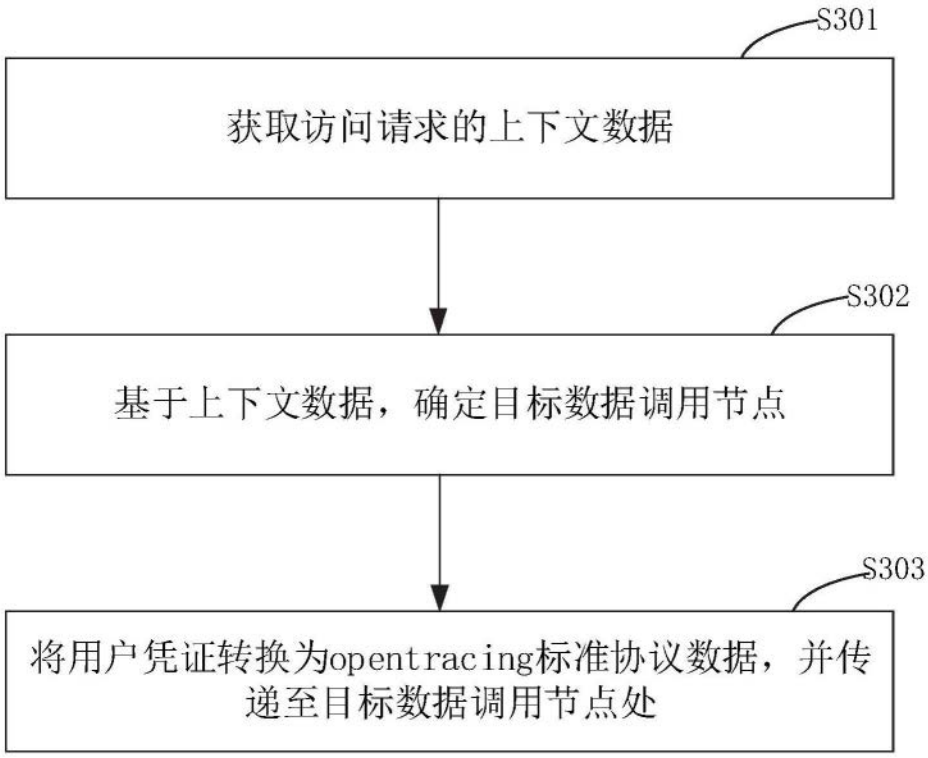

S301
获取访问请求的上下文数据
S302
基于上下文数据，确定目标数据调用节点
S303
将用户凭证转换为opentracing标准协议数据，并传递至目标数据调用节点处

图3

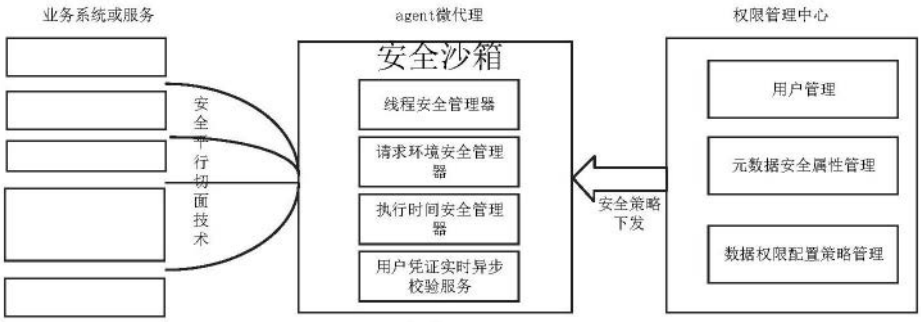

业务系统或服务
agent微代理
权限管理中心
安全沙箱
线程安全管理器
请求环境安全管理器
执行时间安全管理器
用户凭证实时异步校验服务
安全平行切面技术
安全策略下发
用户管理
元数据安全属性管理
数据权限配置策略管理

图4

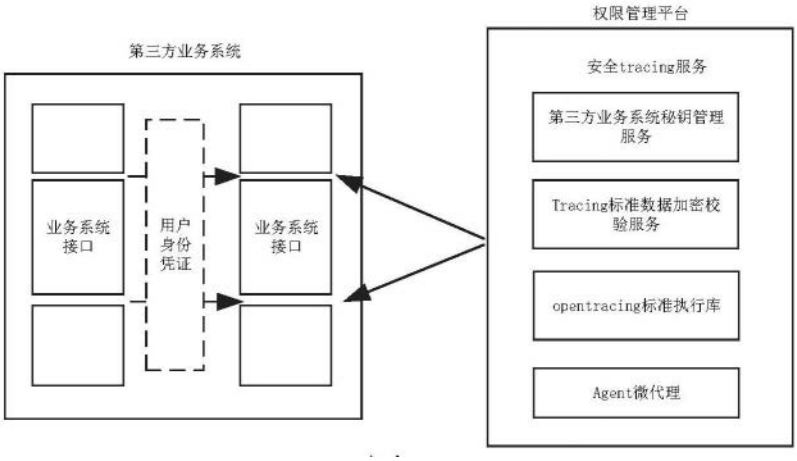

权限管理平台
第三方业务系统
安全tracing服务
第三方业务系统秘钥管理服务
业务系统接口
用户身份凭证
业务系统接口
Tracing标准数据加密校验服务
opentracing标准执行库
Agent微代理

图5

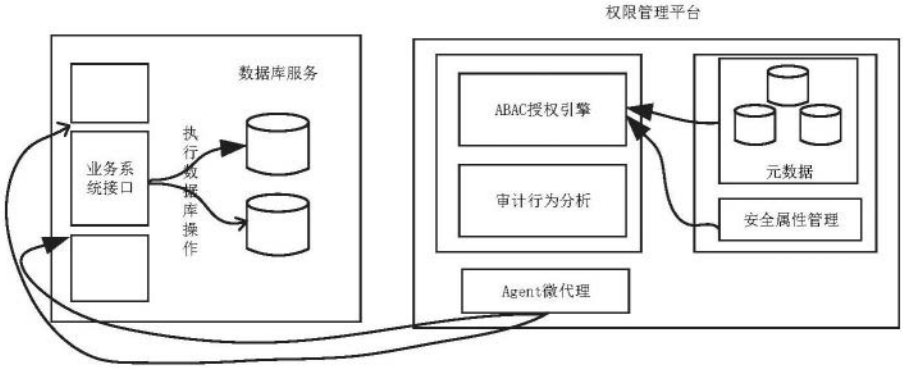

权限管理平台
数据库服务
ABAC授权引擎
业务系统接口
执行数据库操作
审计行为分析
元数据
安全属性管理
Agent微代理

图6

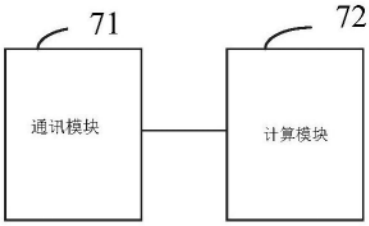

71
72
通讯模块
计算模块

图7