(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111460506 A
(43)申请公布日 2020.07.28

(21)申请号 202010257974.3

(22)申请日 2020.04.03

(71)申请人 中国工商银行股份有限公司
地址 100140 北京市西城区复兴门内大街55号

(72)发明人 张文翰 孙丽娜 彭金胜 沈梦婷

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 刘熔 王涛

(51)Int.Cl.
G06F 21/62(2013.01)

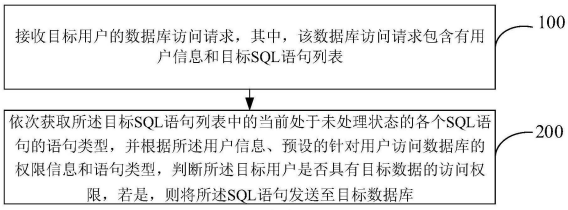
权利要求书2页 说明书12页 附图4页

(54)发明名称

数据访问控制方法及装置

(57)摘要

本申请提供了一种数据访问控制方法及装置，其中，该方法包括：接收目标用户的数据库访问请求，其中，该数据库访问请求包括用户信息和目标SQL语句列表；依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型，并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型，判断所述目标用户是否具有目标数据的访问权限，若是，则将所述SQL语句发送至目标数据库。本申请能够提高数据访问控制的可靠性和灵活性，同时能够提高应用场景的广泛性。



CN 111460506 A

1.一种数据访问控制方法,其特征在于,包括:

接收目标用户的数据库访问请求,其中,该数据库访问请求包括用户信息和目标SQL语句列表;

依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型,并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型,判断所述目标用户是否具有目标数据的访问权限,若是,则将所述SQL语句发送至目标数据库。

2.根据权利要求1所述的数据访问控制方法,其特征在于,所述语句类型包括:查询类型和操作类型;

相对应的,所述判断所述目标用户是否具有目标数据的访问权限,包括:

若所述语句类型为查询类型,则判断所述目标用户是否具有目标数据表和字段的数据查询权限;

若所述语句类型为操作类型,则判断所述目标用户是否具有目标数据表的数据操作权限。

3.根据权利要求2所述的数据访问控制方法,其特征在于,在所述判断所述目标用户是否具有目标数据的访问权限之后,还包括:

若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数,并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

4.根据权利要求2所述的数据访问控制方法,其特征在于,在所述判断所述目标用户是否具有目标数据的访问权限之后,还包括:

若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件,并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

5.根据权利要求2所述的数据访问控制方法,其特征在于,在所述判断所述目标用户是否具有目标数据的访问权限之后,还包括;

若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型,则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数,并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

6.根据权利要求2所述的数据访问控制方法,其特征在于,在所述判断所述目标用户是否具有目标数据的访问权限之后,还包括:

若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型,则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件,并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

7.一种数据访问控制装置,其特征在于,包括:

接收模块,用于接收目标用户的数据库访问请求,其中,该数据库访问请求包括用户信息和目标SQL语句列表;

访问权限控制模块,用于依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型,并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型,判断所述目标用户是否具有目标数据的访问权限,若是,则将所述SQL语句发送

至目标数据库。

8.根据权利要求7所述的数据访问控制装置,其特征在于,所述语句类型包括:查询类型和操作类型;

相对应的,所述访问权限控制模块包括:

判断数据查询权限单元,用于若所述语句类型为查询类型,则判断所述目标用户是否具有目标数据表和字段的数据查询权限;

判断数据操作权限单元,用于若所述语句类型为操作类型,则判断所述目标用户是否具有目标数据表的数据操作权限。

9.根据权利要求8所述的数据访问控制装置,其特征在于,还包括:

第一屏蔽模块,用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数,并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

10.根据权利要求8所述的数据访问控制装置,其特征在于,还包括:

第一隔离模块,用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件,并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

11.根据权利要求8所述的数据访问控制装置,其特征在于,还包括;

第二屏蔽模块,用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型,则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数,并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

12.根据权利要求8所述的数据访问控制装置,其特征在于,还包括:

第二隔离模块,用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型,则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件,并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

13.一种电子设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现权利要求1至6任一项所述的数据访问控制方法。

14.一种计算机可读存储介质,其上存储有计算机指令,其特征在于,所述指令被执行时实现权利要求1至6任一项所述的数据访问控制方法。

数据访问控制方法及装置

技术领域

[0001] 本申请涉及信息安全技术领域,尤其涉及一种数据访问控制方法及装置。

背景技术

[0002] 在数据为本的时代背景下,大量的数据集中存储在数据库中,在多种应用场景中,例如客户营销、经营分析和企业管理等,通过SQL语句对数据库中的数据进行多样化的处理与分析,因此,如何在确保数据信息安全的前提下,将数据快速地在不同的业务部门实现共享,对提高数据利用率和处理时效性具有重要的意义。

[0003] 目前,大多数企业都是采用基于数据库用户来实现对数据访问的管控,即分配数据库账号在指定数据库实例进行增删改查操作。这种方式,一方面过度依赖数据库自身的权限管理机制,数据库账户存在数量限制无法满足用户数量的增长,数据库粒度的权限需要创建视图实现数据表级、特定范围访问控制和敏感信息屏蔽,维护成本高且管理审计困难;另一方面,数据库的权限信息仅在单个数据库集群有效,每个集群需要单独配置并且需要通过应用版本发布,审批流程复杂、实施周期长,严重影响数据的整体处理效率。

发明内容

[0004] 针对现有技术中的问题,本申请提出了一种数据访问控制方法及装置,能够提高数据访问控制的可靠性和灵活性,同时能够提高应用场景的广泛性。

[0005] 为了解决上述技术问题,本申请提供以下技术方案:

[0006] 第一方面,本申请提供一种数据访问控制方法,包括:

[0007] 接收目标用户的数据库访问请求,其中,该数据库访问请求包括用户信息和目标SQL语句列表;

[0008] 依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型,并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型,判断所述目标用户是否具有目标数据的访问权限,若是,则将所述SQL语句发送至目标数据库。

[0009] 进一步地,所述语句类型包括:查询类型和操作类型;相对应的,所述判断所述目标用户是否具有目标数据的访问权限,包括:若所述语句类型为查询类型,则判断所述目标用户是否具有目标数据表和字段的数据查询权限;若所述语句类型为操作类型,则判断所述目标用户是否具有目标数据表的数据操作权限。

[0010] 进一步地,在所述判断所述目标用户是否具有目标数据的访问权限之后,还包括:若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数,并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

[0011] 进一步地,在所述判断所述目标用户是否具有目标数据的访问权限之后,还包括:若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制

条件，并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

[0012] 进一步地，在所述判断所述目标用户是否具有目标数据的访问权限之后，还包括：若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型，则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数，并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

[0013] 进一步地，在所述判断所述目标用户是否具有目标数据的访问权限之后，还包括：若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型，则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件，并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

[0014] 第二方面，本申请提供一种数据访问控制装置，包括：

[0015] 接收模块，用于接收目标用户的数据库访问请求，其中，该数据库访问请求包括用户信息和目标SQL语句列表；

[0016] 访问权限控制模块，用于依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型，并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型，判断所述目标用户是否具有目标数据的访问权限，若是，则将所述SQL语句发送至目标数据库。

[0017] 进一步地，所述语句类型包括：查询类型和操作类型；相对应的，所述访问权限控制模块包括：判断数据查询权限单元，用于若所述语句类型为查询类型，则判断所述目标用户是否具有目标数据表和字段的数据查询权限；判断数据操作权限单元，用于若所述语句类型为操作类型，则判断所述目标用户是否具有目标数据表的数据操作权限。

[0018] 进一步地，所述的数据访问控制装置还包括：第一屏蔽模块，用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询，则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数，并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

[0019] 进一步地，所述的数据访问控制装置还包括：第一隔离模块，用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询，则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件，并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

[0020] 进一步地，所述的数据访问控制装置还包括；第二屏蔽模块，用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型，则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数，并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

[0021] 进一步地，所述的数据访问控制装置还包括：第二隔离模块，用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型，则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件，并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

[0022] 第三方面，本申请提供一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现所述的数据访问控制方法。

[0023] 第四方面，本申请提供一种计算机可读存储介质，其上存储有计算机指令，所述指令被执行时实现所述的数据访问控制方法。

[0024] 由上述技术方案可知，本申请提供一种数据访问控制方法及装置。其中，该方法包括：接收目标用户的数据库访问请求，其中，该数据库访问请求包括用户信息和目标SQL语句列表；依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型，并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型，判断所述目标用户是否具有目标数据的访问权限，若是，则将所述SQL语句发送至目标数据库，能够提高数据访问控制的可靠性和灵活性，同时能够提高应用场景的广泛性；具体地，能够有效地解决数据库用户数量限制、权限管理场景单一和配置生效周期长的问题，主要体现在如下两方面：1)使用SQL语句解析和修改的方式，动态控制用户查询的数据表、字段和数据范围，能够丰富用户权限管理场景，提高数据利用率和系统服务能力；2)通过系统授权的用户查询请求和响应均被记录至数据库，可以作为热点数据检测权限审计需求。

附图说明

[0025] 为了更清楚地说明本申请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申请的一些实施例，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。

[0026] 图1是本申请实施例中数据访问控制方法的流程示意图；

[0027] 图2是本申请实施例中数据访问控制方法步骤201和步骤202的流程示意图；

[0028] 图3是本申请实施例中数据访问控制装置的结构示意图；

[0029] 图4是本申请具体应用实例中数据访问控制系统的结构示意图；

[0030] 图5是本申请具体应用实例中SQL语句解析单元的结构示意图；

[0031] 图6是本申请具体应用实例中用户权限验证单元的处理流程示意图；

[0032] 图7是本申请具体应用实例中SQL语句修改单元的结构示意图；

[0033] 图8是本申请具体应用实例中SQL语句字段血缘分析模块的处理流程示意图；

[0034] 图9为本申请实施例的电子设备9600的系统构成示意框图。

具体实施方式

[0035] 为了使本技术领域的人员更好地理解本说明书中的技术方案，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，都属于本申请保护的范围。

[0036] 基于此，为了提高数据访问控制的可靠性和灵活性，同时能够提高应用场景的广泛性，本申请实施例提供一种数据访问控制装置，该装置可以是一服务器或客户端设备，所述客户端设备可以包括智能手机、平板电子设备、网络机顶盒、便携式计算机、台式电脑、个人数字助理(PDA)、车载设备和智能穿戴设备等。其中，所述智能穿戴设备可以包括智能眼镜、智能手表和智能手环等。

[0037] 在实际应用中，进行数据访问控制的部分可以在如上述内容所述的服务器侧执行，也可以所有的操作都在所述客户端设备中完成。具体可以根据所述客户端设备的处理能力，以及用户使用场景的限制等进行选择。本申请对此不作限定。若所有的操作都在所述客户端设备中完成，所述客户端设备还可以包括处理器。

[0038] 上述的客户端设备可以具有通信模块(即通信单元)，可以与远程的服务器进行通信连接，实现与所述服务器的数据传输。所述服务器可以包括任务调度中心一侧的服务器，其他的实施场景中也可以包括中间平台的服务器，例如与任务调度中心服务器有通信链接的第三方服务器平台的服务器。所述的服务器可以包括单台计算机设备，也可以包括多个服务器组成的服务器集群，或者分布式装置的服务器结构。

[0039] 所述服务器与所述客户端设备之间可以使用任何合适的网络协议进行通信，包括在本申请提交日尚未开发出的网络协议。所述网络协议例如可以包括TCP/IP协议、UDP/IP协议、HTTP协议、HTTPS协议等。当然，所述网络协议例如还可以包括在上述协议之上使用的RPC协议(Remote Procedure Call Protocol，远程过程调用协议)、REST协议(Representational State Transfer，表述性状态转移协议)等。

[0040] 具体通过下述各个实施例进行说明。

[0041] 如图1所示，为了提高数据访问控制的可靠性和灵活性，同时能够提高应用场景的广泛性，本实施例提供一种执行主体是数据访问控制装置的数据访问控制方法，具体包含有如下内容：

[0042] 步骤100：接收目标用户的数据库访问请求，其中，该数据库访问请求包含有用户信息和目标SQL语句列表。

[0043] 具体地，所述用户信息包含有：用户唯一标识，如用户编码；所述目标SQL语句列表中包含有多个SQL语句。

[0044] 步骤200：依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型，并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型，判断所述目标用户是否具有目标数据的访问权限，若是，则将所述SQL语句发送至目标数据库。

[0045] 具体地，所述针对用户访问数据库的权限信息可以存储在本地权限信息中或外部权限信息中，可根据实际情况进行设置。可根据目标SQL语句列表中的各个SQL语句确定所述目标数据。

[0046] 在一种举例中，在步骤200之前还包含有：对所述目标SQL语句列表进行解析，生成已解析的目标SQL语句列表，具体地，将所述目标SQL语句列表中的各个SQL语句分别转换为对应的标识对象组；根据预设的SQL语句语法规范，将各组标识对象分别转化为对应的语法树节点，各个语法树节点组成所述已解析的目标SQL语句列表。

[0047] 为了进一步提高数据访问控制的可靠性和灵活性，在本申请一个实施例中，所述语句类型包含有：查询类型和操作类型；相对应的，参见图2，步骤200所述的判断所述目标用户是否具有目标数据的访问权限包含有：

[0048] 步骤201：若所述语句类型为查询类型，则判断所述目标用户是否具有目标数据表和字段的数据查询权限。

[0049] 其中，所述查询类型为SELECT查询类型。

[0050] 步骤202:若所述语句类型为操作类型,则判断所述目标用户是否具有目标数据表的数据操作权限。

[0051] 举例来说,操作类型包含有CREATE、DROP、ALTER、INSERT、DELETE和TRUNCATE类型。

[0052] 为了进一步提高数据权限控制的灵活性和准确性,在本申请一个实施例中,在步骤200所述的判断所述目标用户是否具有目标数据的访问权限之后,还包含有:

[0053] 步骤210:若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数,并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

[0054] 具体地,所述敏感字段包含有:姓名、地址、电话、身份证、邮箱、证书和IP地址等信息。根据血缘关系从最里层往外逐层处理,如果存在用户不可见的敏感字段,当用户对该字段使用非汇聚类型的函数或二元操作时,则在使用前添加屏蔽函数,否则将在最外层添加。这样的处理方式可以支持用户使用敏感字段作为关联条件且保证敏感信息不泄露。但需要注意的是,当字段被用户使用函数处理后,就无法在父查询中作为关联条件。

[0055] 在一个举例中,在步骤002之前还包含有:确定所述SQL语句的血缘关系,其具体包含有:

[0056] S1:获取查询语句所有查询字段,需要按照查询层次由里往外进行排序,以保证在处理父字段时子字段信息已经被创建。

[0057] S2:判断所有查询字段是否均被处理,如果是则结束处理流程。

[0058] S3:从所有查询字段中提取一个未处理的字段,创建字段信息并存入分析结果集合。

[0059] S4:判断字段对应数据源类型,数据源类型包含有:物理表、子查询(Sub Query)、联合查询(Union Query)。

[0060] S5:判断所有联合查询的子查询是否均被处理,如果是则进行设置字段辅助信息。

[0061] S6:提取子查询的字段名称和别名与父字段进行比对,如果匹配成功则设置父子关系。涉及多个联合子查询块时,进行使用递归或循环的方式直至所有子查询都完成处理。

[0062] S7:设置字段辅助信息,例如是否使用汇聚函数、是否处于UNION查询块、是否使用二元操作等。

[0063] 为了进一步提高数据权限控制的灵活性和准确性,在本申请一个实施例中,在步骤200所述的判断所述目标用户是否具有目标数据的访问权限之后,还包含有:

[0064] 步骤220:若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件,并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

[0065] 具体地,所述预设的数据隔离信息表包含有用户信息,控制字段和控制条件之间的对应关系,根据所述预设的数据隔离信息表确定所述用户信息对应的控制字段和控制条件,并基于所述控制字段和控制条件将数据范围访问权限添加至所述SQL语句。

[0066] 举例来说:所述SQL语句为“SELECT*FROM USER_INFO u”;所述数据隔离表DATA_CTRL包含有,用户编号USER_ID,控制字段CTRL_FIELD和控制条件CONDITION之间的对应关系;其中,用户信息表USER_INFO包含:用户机构编号字段BRANCHNO;则已添加数据范围访问

限制条件的SQL语句为“SELECT*FROM(SELECT*FROM USER_INFO u,DATA_CTRL c WHERE u.BRANCHNO＝c.CONDITION and c.CTRL_FIELD＝‘BRANCHNO’and c.USER_ID＝‘当前用户的编号’)”。

[0067] 为了提高数据访问控制的灵活性和准确性,在本申请一个实施例中,在步骤200所述的判断所述目标用户是否具有目标数据的访问权限之后,包含有:

[0068] 步骤230:若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型,则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数,并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

[0069] 为了提高数据访问控制的灵活性和准确性,在本申请一个实施例中,在步骤200所述的判断所述目标用户是否具有目标数据的访问权限之后,包含有:

[0070] 步骤240:若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型,则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件,并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

[0071] 从软件层面来说,为了提高数据访问控制的可靠性和灵活性,同时能够提高应用场景的广泛性,本申请提供一种用于实现所述数据访问控制方法中全部或部分内容的数据访问控制装置的实施例,参见图3,所述数据访问控制装置具体包含有如下内容:

[0072] 接收模块10,用于接收目标用户的数据库访问请求,其中,该数据库访问请求包含有用户信息和目标SQL语句列表。

[0073] 访问权限控制模块20,用于依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型,并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型,判断所述目标用户是否具有目标数据的访问权限,若是,则将所述SQL语句发送至目标数据库。

[0074] 在本申请一个实施例中,所述语句类型包含有:查询类型和操作类型;相对应的,所述访问权限控制模块包含有:

[0075] 判断数据查询权限单元,用于若所述语句类型为查询类型,则判断所述目标用户是否具有目标数据表和字段的数据查询权限。

[0076] 判断数据操作权限单元,用于若所述语句类型为操作类型,则判断所述目标用户是否具有目标数据表的数据操作权限。

[0077] 在本申请一个实施例中,所述的数据访问控制装置还包含有:

[0078] 第一屏蔽模块,用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数,并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

[0079] 在本申请一个实施例中,所述的数据访问控制装置还包含有:

[0080] 第一隔离模块,用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述SQL语句包含有子查询,则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件,并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

[0081] 在本申请一个实施例中,所述的数据访问控制装置还包含有:

[0082] 第二屏蔽模块，用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型，则根据所述SQL语句的血缘关系向所述SQL语句添加敏感字段屏蔽函数，并将已添加敏感字段屏蔽函数的SQL语句发送至所述目标数据库。

[0083] 在本申请一个实施例中，所述的数据访问控制装置还包含有：

[0084] 第二隔离模块，用于若经判断得到所述目标用户具有目标数据表的数据操作权限且所述语句类型为查询类型，则根据预设的数据隔离信息表和所述用户信息向所述SQL语句添加数据范围访问限制条件，并将已添加数据范围访问限制条件的SQL语句发送至所述目标数据库。

[0085] 本说明书提供的数据访问控制装置的实施例具体可以用于执行上述数据访问控制方法的实施例的处理流程，其功能在此不再赘述，可以参照上述数据访问控制方法实施例的详细描述。

[0086] 为了进一步说明本方案，本申请还提供一种数据访问控制系统与方法的具体应用实例，该数据访问控制系统实现的功能相当于上述数据访问控制装置实现的功能，在本应用实例中，权限控制基于数据库实现，数据应用软件在执行SQL语句之前，通过客户端或服务端调用权限服务判断是否允许执行，验证成功后获取更新的语句，发送至数据库服务器执行。权限服务包含SQL语句鉴权与SQL执行状态记录两部分处理逻辑，SQL语句鉴权主要负责对语句解析、权限验证和修改，SQL执行状态记录一方面用于审计信息记录，另一方面对于DDL语句执行成功时，需要在权限管理系统中注册或撤销用户自定义数据表信息。

[0087] 下面将对照附图，对本具体应用实例的技术方案进行详细说明。

[0088] 图4为系统的结构示意图，包含有：请求处理单元1、SQL语句解析单元2、用户权限验证单元3、SQL语句修改单元4、用户数据表处理单元5、审计信息记录单元6和响应处理单元7。

[0089] 请求处理单元1负责解析输入参数和校验参数合法性，然后根据请求类型将SQL语句鉴权请求传入SQL语句解析单元2，将SQL执行状态记录请求传入用户数据表处理单元5。SQL语句鉴权的输入参数包含有：用户唯一标识、数据库类型、数据库集群和SQL语句段落。通常情况下，数据分析师使用多条SQL语句对数据进行一系列处理后获取输出结果，其中包含创建删除临时数据表等操作，这些操作需要作为同一个事务，所以必须支持单次请求的SQL语句段落鉴权，每条语句可以使用分号隔开。SQL执行状态记录请求输入参数包含有：SQL语句鉴权操作编号、执行状态、执行开始时间、执行结束时间和数据集行数大小等。

[0090] QL语句解析单元2将SQL语句文本解析为抽象语法树对象后传入用户权限验证单元3。图5为本具体应用实例中，SQL语句解析单元2的结构示意图，包含有词法分析单元21、语法分析单元22和语法节点遍历单元23。词法分析单元21包含一组词汇表，通过对SQL语句每个单词逐一匹配，将文本转换为标识对象。语法分析单元22，根据各数据库SQL语法规范将一组标识对象识别为抽象语法树节点，节点类型包含有SQL对象、SQL表达式和SQL声明等。语法节点遍历单元23使用访问者设计模式对所有语法节点的遍历，可以通过预设或自定义方式实现访问的数据表和列提取、SQL语句内容修改和输出SQL语句文本等功能。

[0091] 用户权限验证单元3使用本地权限信息8和外部权限信息9对提取的访问数据表和列进行验证，验证成功将SQL抽象语法对象与权限信息传入SQL语句修改单元4，验证失败则将错误信息传入审计信息记录单元7。外部权限信息9的实现形式可以是外部权限管理系

统，也可以是权限信息数据库。通常情况下，系统允许数据分析师创建、删除、使用和共享自定义数据表，所以当涉及用户自定义数据表操作时，还需要将这些信息传入用户数据表处理单元5处理。

[0092] 图6为本具体应用实例中用户权限验证单元3的处理流程示意图，具体步骤如下：

[0093] S11：接收输入参数；输入参数包含有用户信息和已解析的SQL语句列表。

[0094] S12：判断所有SQL语句是否均被处理，若否，则执行步骤S13；若是，则结束处理流程。

[0095] S13：提取单条SQL语句；从已解析的SQL语句列表中按顺序提取单条未处理的语句。

[0096] S14：判断是否为SELECT查询语句；若是，则执行步骤S18；若否，则执行步骤S15。

[0097] 具体地，SQL语句类型包含有操作类型和查询类型，如果为用户数据表操作，例如CREATE、DROP、ALTER、INSERT、DELETE和TRUNCATE等，则首先提取用户数据表信息；如果仅为SELECT查询操作，则进行提取查询的数据表和字段信息。

[0098] S15：提取用户数据表信息；具体地，获取语法节点遍历单元23提取操作的用户数据表信息。

[0099] S16：判断用户是否有操作权限；具体地，从本地存储和外部权限管理系统获取权限信息，判断用户是否拥有对用户数据表操作权限，若是，则执行步骤S17；若否，则结束处理流程。

[0100] S17：判断是否包含子查询；具体地，判断用户数据表操作是否包含子查询，例如CREATE...AS SELECT...，INSERT INTO...SELECT等语法，若是，则执行步骤S18；若否，则执行步骤S112。

[0101] S18：提取查询的用户数据表和字段信息；具体地，获取语法节点遍历单元23提取的用户数据表和字段信息。

[0102] S19：判断用户是否有访问权限；具体地，从本地存储和外部权限管理系统获取权限信息，判断用户是否拥有对用户数据表访问权限，若是，执行步骤S110，若否，则结束处理流程。

[0103] S110：SQL语句修改；具体地，根据用户权限为SQL语句添加数据范围访问限制条件和敏感字段屏蔽函数。

[0104] S111：判断是否对用户数据表进行DDL操作；判断是否涉及用户数据表创建、删除和重命名操作，若是，则执行步骤S112，若否，则再次执行步骤S12，进行下一轮语句处理。

[0105] S112：用户数据表处理；具体地，用户数据表的DDL操作需要更新本地权限信息，待接收到SQL语句成功执行通知后，推送至外部权限管理系统。

[0106] SQL语句修改单元4为SQL语句添加敏感信息屏蔽函数和数据隔离条件，然后将输出的语句文本和用户信息传入审计信息记录单元6。敏感字段主要包含有姓名、地址、电话、身份证、邮箱、证书和IP地址等信息，数据分析师查询这些字段时系统需要根据权限等级进行显示，例如某级别权限，姓名字段仅显示姓氏而名字以*代替。另外，系统需要支持使用敏感信息字段作为查询条件和关联条件。为了满足以上的需求，在涉及多层子查询嵌套、字段汇聚函数、字段处理函数等应用场景中，首先需要对语句的查询字段进行血缘分析，然后动态地在不同子查询中添加敏感屏蔽函数。

[0107] 图7为本具体应用实例中SQL语句修改单元4的结构示意图，主要包含有：SELECT*语法处理模块401，字段血缘分析模块402，敏感信息屏蔽处理模块403，数据隔离条件处理模块404。

[0108] SELECT*语法处理模块401，检查语句是否存在SELECT*语法、查询的数据表是否存在敏感字段，如果存在则获取元数据信息后使用列名替换*。

[0109] 字段血缘分析模块402通过分析SQL语句结构，生成查询字段引用父子关联信息，同时设置字段辅助信息。图8为本具体应用实例中SQL语句字段血缘分析模块402的处理流程示意图，具体步骤如下：

[0110] S21：获取语句所有查询字段列表；需要按照查询层次由里往外进行排序，这样能确保在处理父字段时子字段信息已经被创建。

[0111] S22：判断所有查询字段是否均被处理，若是则结束处理流程；若否，则执行步骤S23。

[0112] S23：提取单个未处理的查询字段并创建字段信息存入分析结果合集；具体地，从所有查询字段列表中提取一个未处理的字段，创建字段信息存入分析结果集合。

[0113] S24：判断字段对应数据源类型；数据源类型包含有：物理表、子查询(Sub Query)和联合查询(Union Query)。

[0114] S25：判断所有联合查询的子查询是否均被处理；若是，则执行步骤S28；若否，则执行步骤S26。

[0115] S26：处理单个联合子查询块；具体地，提取子查询的字段名称和别名与父字段进行比对，如果匹配成功则设置父子关系。涉及多个联合子查询块时，进行使用递归或循环的方式直至所有子查询都完成处理。

[0116] S27：处理子查询块；具体地，提取子查询的字段名称和别名与父字段进行比对，如果匹配成功则设置父子关系。

[0117] S28：设置字段辅助信息；具体地。供敏感信息屏蔽处理模块403应用，例如是否使用汇聚函数、是否处于UNION查询块和是否使用二元操作等。

[0118] 敏感信息屏蔽处理模块403根据血缘关系从最里层往外逐层处理，如果存在用户不可见的敏感字段，当用户对该字段使用非汇聚类型的函数或二元操作时，则在使用前添加屏蔽函数，否则将在最外层添加。这样的处理方式可以支持用户使用敏感字段作为关联条件且保证敏感信息不泄露。但需要注意的是，当字段被用户使用函数处理后，就无法在父查询中作为关联条件。

[0119] 数据隔离条件处理模块404实现限制分析师访问数据表指定的部分数据，例如用户信息表存放所有机构的用户数据，对于不同机构的数据分析师仅可以查询本人所属机构的用户。系统增加数据隔离信息表，通过将查询语句中的表名替换为与隔离信息表关联的子查询。

[0120] 用户数据表处理单元5将在本地权限信息8新增或删除用户数据表记录，若接收到语句执行成功通知，则将本地权限推送外部权限信息9更新，更新后本地相应的权限信息将被清除。

[0121] 审计信息记录单元6记录请求的用户、请求的原始SQL语句和更新的SQL语句，然后将这些信息传入响应处理单元7。使用异步方式可以极大地提高了接口处理响应速度。

[0122] 响应处理单元7对输出参数进行按预定格式封装后传回调用方。

[0123] 由上述描述可知，本申请提供的数据访问控制方法及装置，能够提高数据访问控制的可靠性和灵活性，同时能够提高应用场景的广泛性；具体地，本申请能够克服现有数据库自身权限管理系统存在账户数量限制、无法应对多样化权限配置和管理审计困难的缺陷，提供一种基于用户粒度、个性化定制场景、跨数据集群和配置实时生效的数据访问权限控制方法及装置。

[0124] 从硬件层面来说，为了提高数据访问控制的可靠性和灵活性，同时能够提高应用场景的广泛性，本申请提供一种用于实现所述数据访问控制方法中的全部或部分内容的电子设备的实施例所述电子设备具体包含有如下内容：

[0125] 处理器(processor)、存储器(memory)、通信接口(Communications Interface)和总线；其中，所述处理器、存储器、通信接口通过所述总线完成相互间的通信；所述通信接口用于实现所述数据访问控制装置以及用户终端等相关设备之间的信息传输；该电子设备可以是台式计算机、平板电脑及移动终端等，本实施例不限于此。在本实施例中，该电子设备可以参照实施例用于实现所述数据访问控制方法的实施例及用于实现所述数据访问控制装置的实施例进行实施，其内容被合并于此，重复之处不再赘述。

[0126] 图9为本申请实施例的电子设备9600的系统构成的示意框图。如图9所示，该电子设备9600可以包括中央处理器9100和存储器9140；存储器9140耦合到中央处理器9100。值得注意的是，该图9是示例性的；还可以使用其他类型的结构，来补充或代替该结构，以实现电信功能或其他功能。

[0127] 在本申请一个或多个实施例中，数据访问控制功能可以被集成到中央处理器9100中。其中，中央处理器9100可以被配置为进行如下控制：

[0128] 步骤100：接收目标用户的数据库访问请求，其中，该数据库访问请求包含有用户信息和目标SQL语句列表。

[0129] 步骤200：依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型，并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型，判断所述目标用户是否具有目标数据的访问权限，若是，则将所述SQL语句发送至目标数据库。

[0130] 从上述描述可知，本申请的实施例提供的电子设备，能够提高数据访问控制的可靠性和灵活性，同时能够提高应用场景的广泛性。

[0131] 在另一个实施方式中，数据访问控制装置可以与中央处理器9100分开配置，例如可以将数据访问控制装置配置为与中央处理器9100连接的芯片，通过中央处理器的控制来实现数据访问控制功能。

[0132] 如图9所示，该电子设备9600还可以包括：通信模块9110、输入单元9120、音频处理器9130、显示器9160、电源9170。值得注意的是，电子设备9600也并不是必须要包括图9中所示的所有部件；此外，电子设备9600还可以包括图9中没有示出的部件，可以参考现有技术。

[0133] 如图9所示，中央处理器9100有时也称为控制器或操作控件，可以包括微处理器或其他处理器装置和/或逻辑装置，该中央处理器9100接收输入并控制电子设备9600的各个部件的操作。

[0134] 其中，存储器9140，例如可以是缓存器、闪存、硬驱、可移动介质、易失性存储器、非

易失性存储器或其它合适装置中的一种或更多种。可储存上述与失败有关的信息，此外还可存储执行有关信息的程序。并且中央处理器9100可执行该存储器9140存储的该程序，以实现信息存储或处理等。

[0135] 输入单元9120向中央处理器9100提供输入。该输入单元9120例如为按键或触摸输入装置。电源9170用于向电子设备9600提供电力。显示器9160用于进行图像和文字等显示对象的显示。该显示器例如可为LCD显示器，但并不限于此。

[0136] 该存储器9140可以是固态存储器，例如，只读存储器(ROM)、随机存取存储器(RAM)、SIM卡等。还可以是这样的存储器，其即使在断电时也保存信息，可被选择性地擦除且设有更多数据，该存储器的示例有时被称为EPROM等。存储器9140还可以是某种其它类型的装置。存储器9140包括缓冲存储器9141(有时被称为缓冲器)。存储器9140可以包括应用/功能存储部9142，该应用/功能存储部9142用于存储应用程序和功能程序或用于通过中央处理器9100执行电子设备9600的操作的流程。

[0137] 存储器9140还可以包括数据存储部9143，该数据存储部9143用于存储数据，例如联系人、数字数据、图片、声音和/或任何其他由电子设备使用的数据。存储器9140的驱动程序存储部9144可以包括电子设备的用于通信功能和/或用于执行电子设备的其他功能(如消息传送应用、通讯录应用等)的各种驱动程序。

[0138] 通信模块9110即为经由天线9111发送和接收信号的发送机/接收机9110。通信模块(发送机/接收机)9110耦合到中央处理器9100，以提供输入信号和接收输出信号，这可以和常规移动通信终端的情况相同。

[0139] 基于不同的通信技术，在同一电子设备中，可以设置有多个通信模块9110，如蜂窝网络模块、蓝牙模块和/或无线局域网模块等。通信模块(发送机/接收机)9110还经由音频处理器9130耦合到扬声器9131和麦克风9132，以经由扬声器9131提供音频输出，并接收来自麦克风9132的音频输入，从而实现通常的电信功能。音频处理器9130可以包括任何合适的缓冲器、解码器、放大器等。另外，音频处理器9130还耦合到中央处理器9100，从而使得可以通过麦克风9132能够在本机上录音，且使得可以通过扬声器9131来播放本机上存储的声音。

[0140] 上述描述可知，本申请的实施例提供的电子设备，能够提高数据访问控制的可靠性和灵活性，同时能够提高应用场景的广泛性。

[0141] 本申请的实施例还提供能够实现上述实施例中的数据访问控制方法中全部步骤的一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时实现上述实施例中的数据访问控制方法的全部步骤，例如，所述处理器执行所述计算机程序时实现下述步骤：

[0142] 步骤100：接收目标用户的数据库访问请求，其中，该数据库访问请求包含有用户信息和目标SQL语句列表。

[0143] 步骤200：依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型，并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型，判断所述目标用户是否具有目标数据的访问权限，若是，则将所述SQL语句发送至目标数据库。

[0144] 从上述描述可知，本申请实施例提供的计算机可读存储介质，能够提高数据访问

控制的可靠性和灵活性,同时能够提高应用场景的广泛性。

[0145] 本申请中上述方法的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。相关之处参见方法实施例的部分说明即可。

[0146] 本领域内的技术人员应明白,本申请的实施例可提供为方法、系统、或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0147] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0148] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0149] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0150] 本申请中应用了具体实施例对本申请的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本申请的方法及其核心思想;同时,对于本领域的一般技术人员,依据本申请的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本申请的限制。

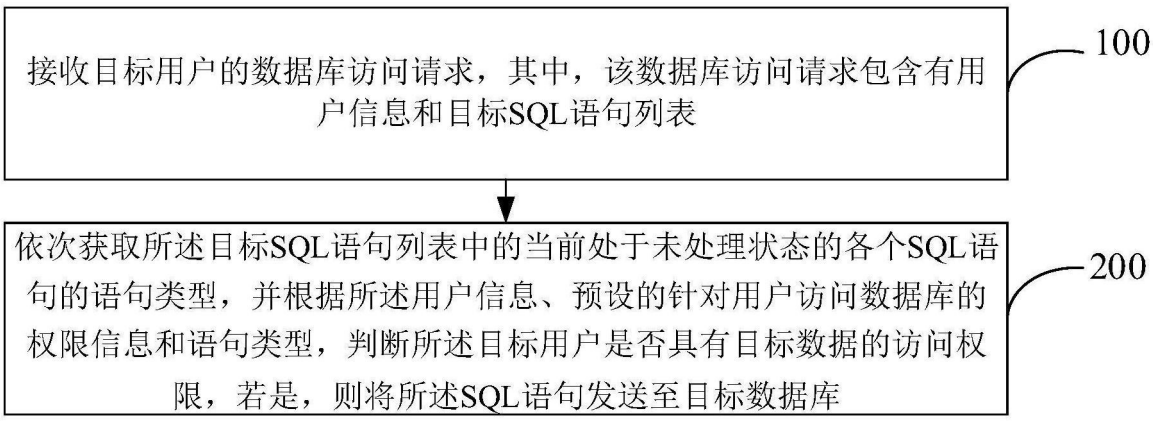

接收目标用户的数据库访问请求，其中，该数据库访问请求包含有用户信息和目标SQL语句列表
100
依次获取所述目标SQL语句列表中的当前处于未处理状态的各个SQL语句的语句类型，并根据所述用户信息、预设的针对用户访问数据库的权限信息和语句类型，判断所述目标用户是否具有目标数据的访问权限，若是，则将所述SQL语句发送至目标数据库
200

图1

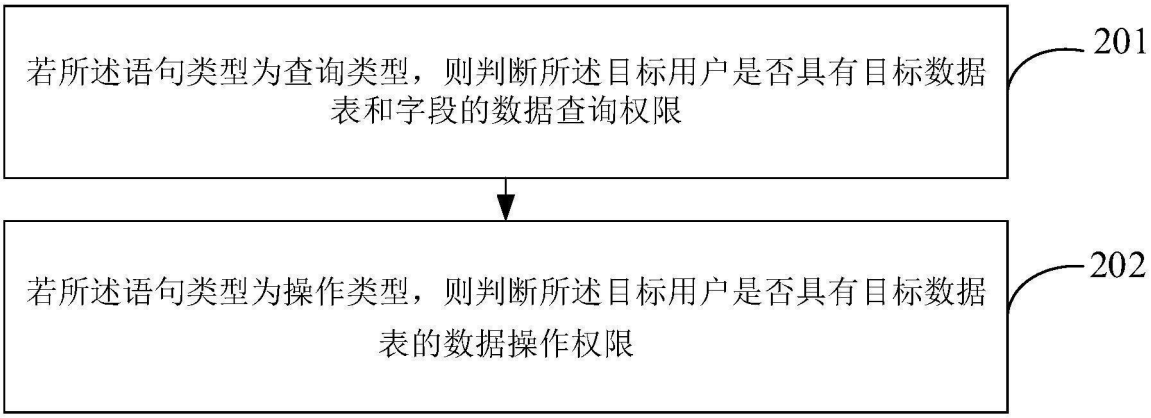

若所述语句类型为查询类型，则判断所述目标用户是否具有目标数据表和字段的数据查询权限
201
若所述语句类型为操作类型，则判断所述目标用户是否具有目标数据表的数据操作权限
202

图2

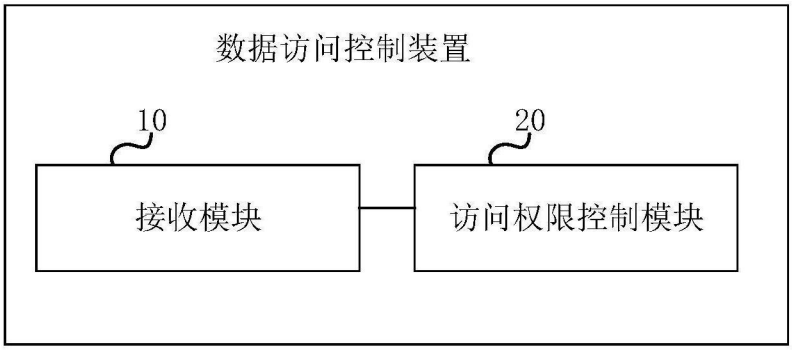

数据访问控制装置
10
20
接收模块
访问权限控制模块

图3

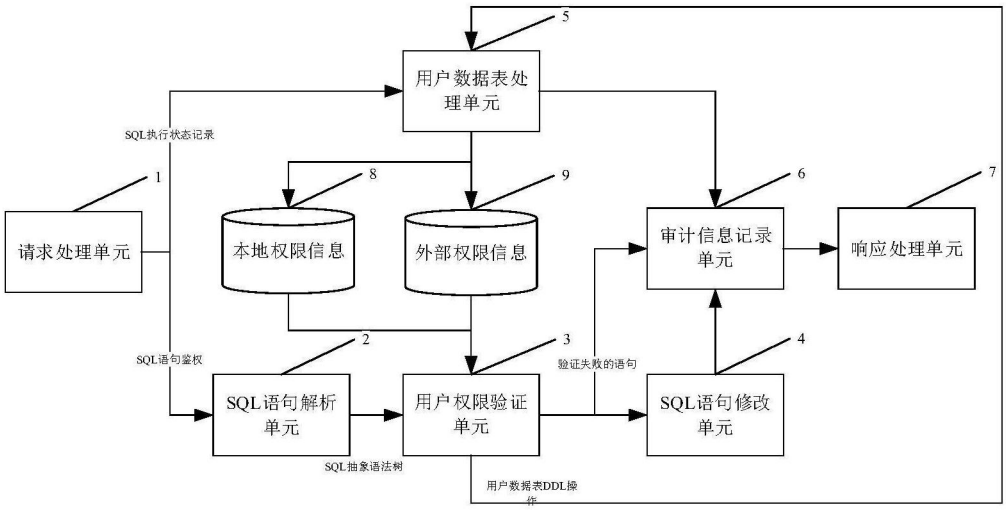

5
用户数据表处理单元
SQL执行状态记录
1
8
9
6
7
请求处理单元
本地权限信息
外部权限信息
审计信息记录单元
响应处理单元
2
3
4
SQL语句鉴权
验证失败的语句
SQL语句解析单元
用户权限验证单元
SQL语句修改单元
SQL抽象语法树
用户数据表DDL操作

图4

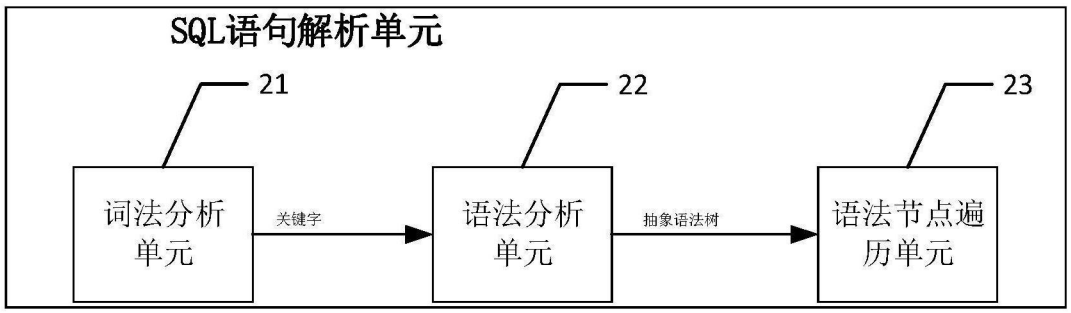

SQL语句解析单元
21
22
23
词法分析单元
关键字
语法分析单元
抽象语法树
语法节点遍历单元

图5

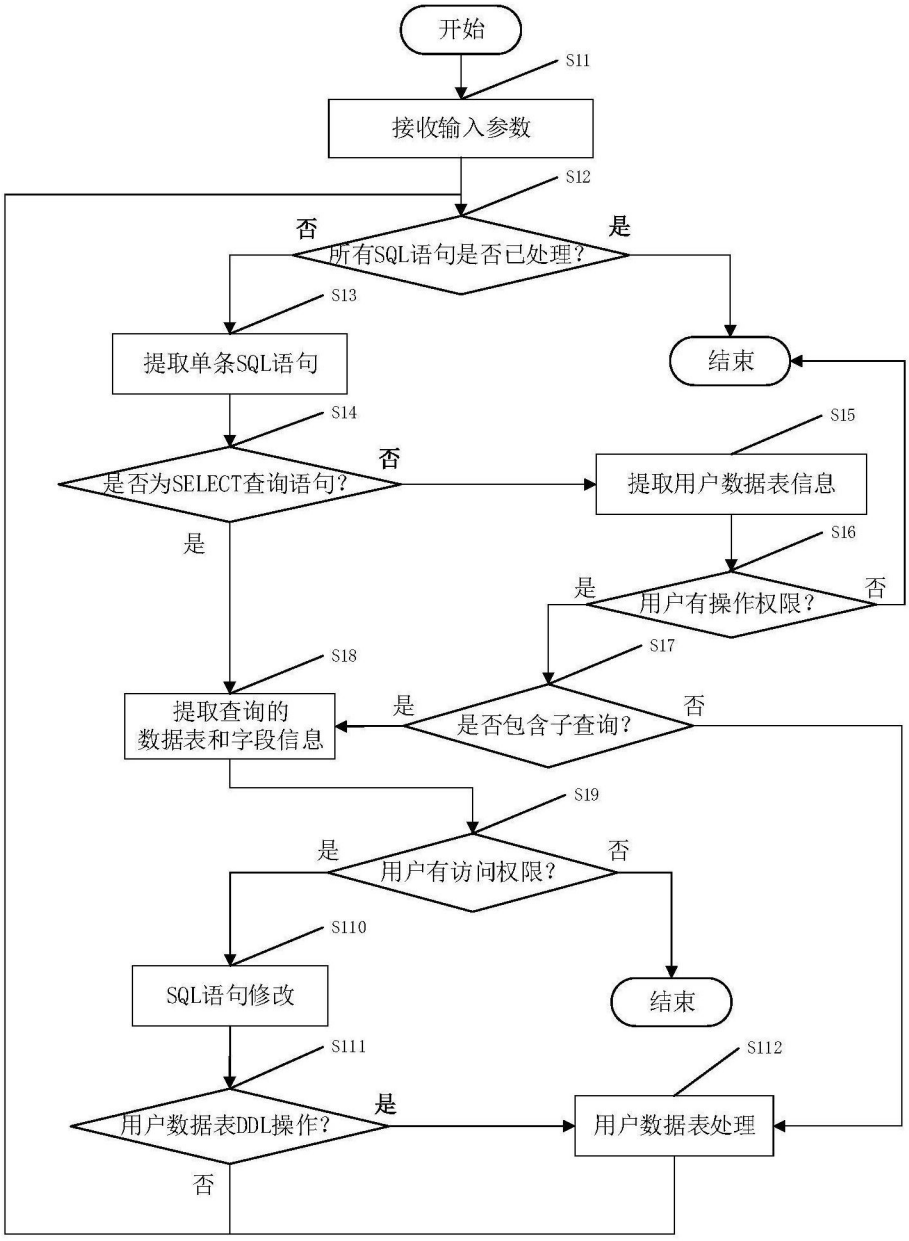

开始
S11
接收输入参数
S12
否
所有SQL语句是否已处理?
是
S13
提取单条SQL语句
结束
S14
是否为SELECT查询语句?
否
S15
提取用户数据表信息
是
S16
是
用户有操作权限?
否
S17
S18
提取查询的
数据表和字段信息
是
是否包含子查询?
否
S19
是
用户有访问权限?
否
S110
SQL语句修改
结束
S111
用户数据表DDL操作?
是
S112
用户数据表处理
否

图6

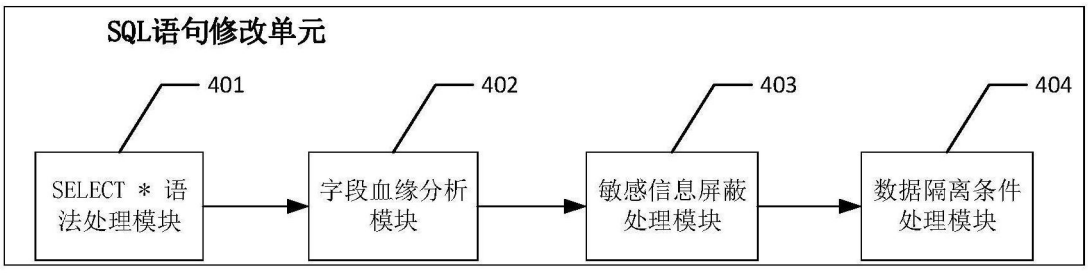

SQL语句修改单元
401
SELECT * 语
法处理模块
402
字段血缘分析
模块
403
敏感信息屏蔽
处理模块
404
数据隔离条件
处理模块

图7

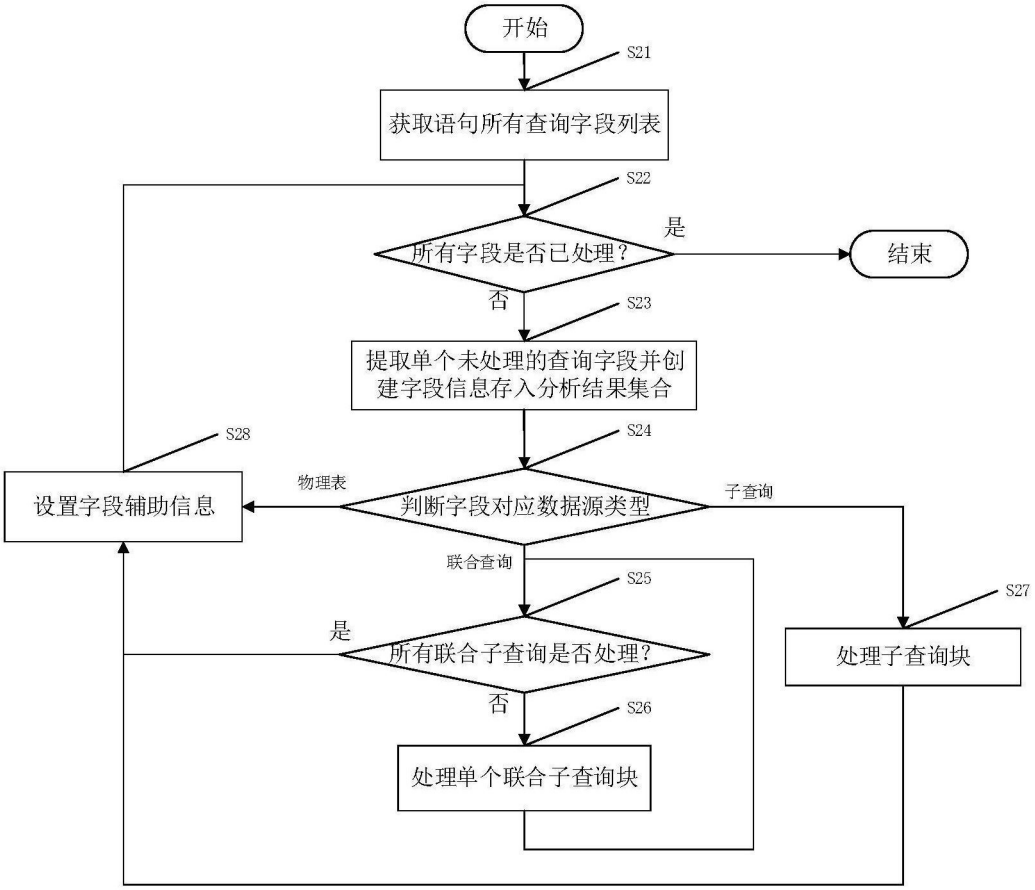

开始
S21
获取语句所有查询字段列表
S22
所有字段是否已处理?
是
结束
否
S23
提取单个未处理的查询字段并创建字段信息存入分析结果集合
S24
判断字段对应数据源类型
物理表
子查询
联合查询
S28
设置字段辅助信息
S25
所有联合子查询是否处理?
是
否
S26
处理单个联合子查询块
S27
处理子查询块

图8

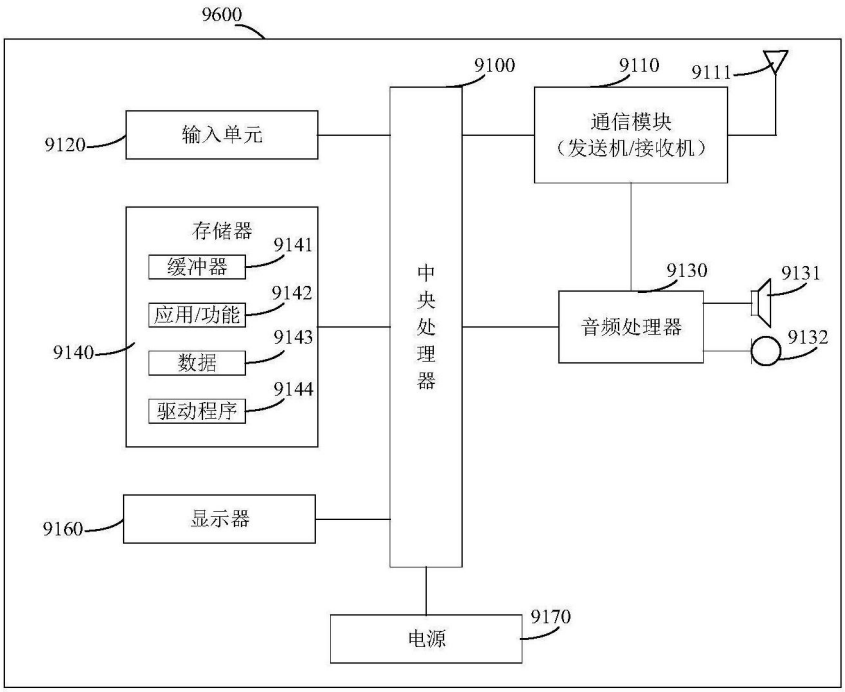

9600
9100
9110
9111
9120
输入单元
通信模块
（发送机/接收机）
存储器
9141
缓冲器
9142
应用/功能
9143
数据
9144
驱动程序
9140
中央处理器
9130
9131
音频处理器
9132
9160
显示器
9170
电源

图9