(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 110222531 A
(43)申请公布日 2019.09.10

(21)申请号 201910467315.X

(22)申请日 2019.05.31

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 肖磊 张园超 姚兴 李婷婷

(74)专利代理机构 北京晋德允升知识产权代理有限公司 11623
代理人 黎飞鸿

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)
G06F 21/31(2013.01)

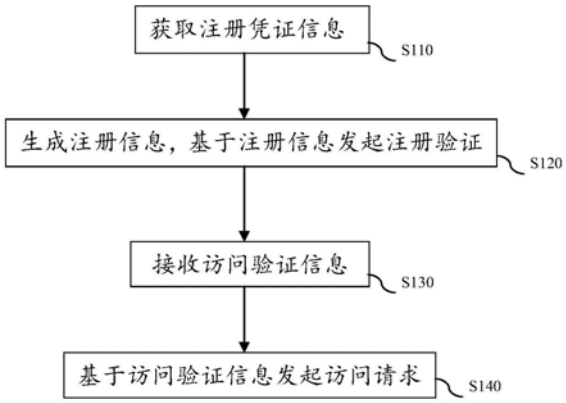
权利要求书3页 说明书12页 附图6页

(54)发明名称

一种访问数据库的方法、系统及设备

(57)摘要

本申请公开了一种访问数据库的方法、系统及设备。在本说明书一实施例的方法中，访问数据库的方法包括：获取来自部署平台的注册凭证信息；根据所述注册凭证信息生成注册信息，基于所述注册信息向访问控制平台发起注册验证；接收来自所述访问控制平台的访问验证信息，其中，所述访问验证信息在所述注册验证成功后才能获取，所述访问验证信息包含有权访问的数据库实例信息，所述数据库实例信息包含对应的数据库口令；基于所述访问验证信息向数据库主机发起访问请求，所述访问请求包括所述数据库口令。



CN 110222531 A

1.一种访问数据库的方法,所述方法包括:

获取来自部署平台的注册凭证信息;

根据所述注册凭证信息生成注册信息,基于所述注册信息向访问控制平台发起注册验证;

接收来自所述访问控制平台的访问验证信息,其中,所述访问验证信息在所述注册验证成功后才能获取,所述访问验证信息包含有权访问的数据库实例信息,所述数据库实例信息包含对应的数据库口令;

基于所述访问验证信息向数据库主机发起访问请求,所述访问请求包括所述数据库口令。

2.根据权利要求1所述的方法:

获取所述注册凭证信息,其中,所述注册凭证信息包括与第一合法身份信息绑定的注册凭证;

根据所述注册凭证信息生成注册信息,其中,所述注册信息包括所述注册凭证。

3.根据权利要求1或2所述的方法,所述访问验证信息还包括与第二合法身份信息绑定的身份验证信息。

4.根据权利要求1～3中任一项所述的方法,利用与数据库访问请求方的业务进程相独立的数据库访问模块实现生成所述注册信息、和/或发起所述注册验证、和/或发起所述访问请求。

5.根据权利要求4所述的方法,获取注册凭证信息,包括:

利用所述数据库访问模块接收来自部署平台的加密信息,其中,所述加密信息的解密密钥内置在所述数据库访问模块中;

利用所述数据库访问模块解密所述加密信息,获取所述注册凭证信息。

6.根据权利要求5或6所述的方法,所述方法还包括:

启动所述数据库访问模块,其中,所述数据库访问模块由所述部署平台以独立容器或进程启动。

7.根据权利要求4～6中任一项所述的方法,基于所述访问验证信息向数据库主机发起访问请求,包括:

将所述数据库访问模块视作数据库本地代理,由业务进程向所述数据库访问模块发起SQL连接;

由所述数据库访问模块向所述数据库主机发起TLS数据库连接。

8.根据权利要求4～7中任一项所述的方法,利用数据库Sidecar模块构建所述数据库访问模块。

9.根据权利要求1～8中任一项所述的方法,基于所述访问验证信息向数据库主机发起访问请求,其中,基于最新接收到的访问验证信息向所述数据库主机发起访问请求。

10.一种部署数据库访问权限的方法,所述方法包括:

进行注册验证,其中,接收如权利要求1～9中任一项所述的注册信息并验证所述注册信息;

当注册验证成功时,创建如权利要求1～9中任一项所述的访问验证信息,所述访问验证信息与注册验证发起方的身份匹配;

向所述注册验证发起方发送所述访问验证信息。

11.根据权利要求10所述的方法，接收如权利要求1～9中任一项所述的注册信息并验证所述注册信息，其中：

接收与第一合法身份信息绑定的所述注册信息；

验证所述第一合法身份信息与所述注册验证发起方是否匹配。

12.根据权利要求10或11所述的方法，所述方法还包括：

接收来自数据库主机的核实请求，所述核实请求包含访问请求发起方的身份标识；

将可访问数据库列表返回给所述数据库主机，其中，所述可访问数据库列表为所述访问请求发起方可访问的数据库列表。

13.根据权利要求10～12中任一项所述的方法，所述方法还包括：

将拦截策略发送到数据库主机。

14.根据权利要求10～13中任一项所述的方法，所述方法还包括：

更新已创建的访问验证信息，其中，更新数据库口令；

将更新后的访问验证信息发送到对应的所述注册验证发起方；

监控当前正在被使用的数据库访问连接；

在当前正在被使用的数据库访问连接中存在基于更新前的访问验证信息建立的数据库访问连接时，维持更新前的访问验证信息有效；

在当前正在被使用的数据库访问连接中不存在基于更新前的访问验证信息建立的数据库访问连接时，销毁更新前的访问验证信息。

15.一种验证数据库访问权限的方法，所述方法包括：

接收如权力要求1～9任一项所述的访问请求；

验证所述访问请求；

当所述访问请求通过验证时，容许访问请求发起方访问数据库。

16.根据权利要求15所述的方法：

接收所述访问请求，其中，所述访问请求包括与第二合法身份信息绑定的身份验证信息；

验证所述访问请求，包括，验证所述第二合法身份信息与所述访问请求发起方是否匹配。

17.根据权利要求15或16所述的方法，验证所述访问请求，还包括：

生成核实请求，所述核实请求包含所述访问请求发起方的身份标识；

将所述核实请求发送到访问控制平台；

接收来自所述访问控制平台的可访问数据库列表，其中，所述可访问数据库列表为所述访问请求发起方可访问的数据库列表；

根据所述可访问数据库列表验证所述访问请求，其中，验证所述访问请求对应的目标数据库是否在所述可访问数据库列表中。

18.一种访问数据库的系统，所述系统包括：

部署信息获取模块，其用于获取来自部署平台的注册凭证信息；

注册验证发起模块，其用于根据所述注册凭证信息生成注册信息，基于所述注册信息向访问控制平台发起注册验证；

访问验证信息获取模块，其用于接收来自所述访问控制平台的访问验证信息，其中，所述访问验证信息在所述注册验证成功后才能获取，所述访问验证信息包含有权访问的数据库实例信息，所述数据库实例信息包含对应的数据库口令；

数据库访问模块，其用于基于所述访问验证信息向数据库主机发起访问请求，所述访问请求包括所述数据库口令。

19.一种部署数据库访问权限的系统，所述系统包括：

注册验证模块，其用于进行注册验证，其中，接收如权利要求1～9中任一项所述的注册信息并验证所述注册信息；

访问验证信息创建模块，其用于当注册验证成功时，创建如权利要求1～9中任一项所述的访问验证信息，所述访问验证信息与注册验证发起方的身份匹配；

访问验证信息发送模块，其用于向所述注册验证发起方发送所述访问验证信息。

20.一种验证数据库访问权限的系统，所述系统包括：

访问请求获取模块，其用于接收如权力要求1～9任一项所述的访问请求；

访问请求验证模块，其用于验证所述访问请求，当所述访问请求通过验证时，容许访问请求发起方访问数据库。

21.一种用于在用户设备端信息处理的设备，该设备包括用于存储计算机程序指令的存储器和用于执行程序指令的处理器，其中，当该计算机程序指令被该处理器执行时，触发该设备执行权利要求1至17中任一项所述的方法。

一种访问数据库的方法、系统及设备

技术领域

[0001] 本说明书涉及计算机技术领域，尤其涉及一种访问数据库的方法、系统及设备。

背景技术

[0002] 数据库是按照数据结构来组织、存储和管理数据的仓库。一般的，数据库中存放的数据并不是针对所有人开放的。因此，在用户访问数据库时，需要对用户进行鉴权，确认用户有权访问的数据库实例，阻止非法访问。

[0003] 在现有技术中，通常基于数据库口令实现对数据库访问者的鉴权。即，为具有访问权限的访问者颁发对应的数据库口令。在访问者访问数据库时，验证其具备的数据库口令，从而确定其是否具备访问权限。然而，随着企业生长，数据库系统规模和复杂性增大，这使得数据库口令的管理变得异常困难，从而导致数据库口令颁发错误、数据库口令泄露的发生几率大大增加，进而使得数据库被拖库的风险显著提升。

发明内容

[0004] 有鉴于此，本说明书实施例提供了一种访问数据库的方法、系统及设备，用于解决现有技术中数据库口令管理过程中存在的问题。

[0005] 本说明书实施例采用下述技术方案：

[0006] 本说明书实施例提供一种访问数据库的方法，所述方法包括：

[0007] 获取来自部署平台的注册凭证信息；

[0008] 根据所述注册凭证信息生成注册信息，基于所述注册信息向访问控制平台发起注册验证；

[0009] 接收来自所述访问控制平台的访问验证信息，其中，所述访问验证信息在所述注册验证成功后才能获取，所述访问验证信息包含有权访问的数据库实例信息，所述数据库实例信息包含对应的数据库口令；

[0010] 基于所述访问验证信息向数据库主机发起访问请求，所述访问请求包括所述数据库口令。

[0011] 在本说明书一实施例中：

[0012] 获取所述注册凭证信息，其中，所述注册凭证信息包括与第一合法身份信息绑定的注册凭证；

[0013] 根据所述注册凭证信息生成注册信息，其中，所述注册信息包括所述注册凭证。

[0014] 在本说明书一实施例中，所述访问验证信息还包括与第二合法身份信息绑定的身份验证信息。

[0015] 在本说明书一实施例中，利用与数据库访问请求方的业务进程相独立的数据库访问模块实现生成所述注册信息、和/或发起所述注册验证、和/或发起所述访问请求。

[0016] 在本说明书一实施例中，获取注册凭证信息，包括：

[0017] 利用所述数据库访问模块接收来自部署平台的加密信息，其中，所述加密信息的

解密密钥内置在所述数据库访问模块中；

[0018] 利用所述数据库访问模块解密所述加密信息，获取所述注册凭证信息。

[0019] 在本说明书一实施例中，所述方法还包括：

[0020] 启动所述数据库访问模块，其中，所述数据库访问模块由所述部署平台以独立容器或进程启动。

[0021] 在本说明书一实施例中，基于所述访问验证信息向数据库主机发起访问请求，包括：

[0022] 将所述数据库访问模块视作数据库本地代理，由业务进程向所述数据库访问模块发起SQL连接；

[0023] 由所述数据库访问模块向所述数据库主机发起TLS数据库连接。

[0024] 在本说明书一实施例中，利用数据库Sidecar模块构建所述数据库访问模块。

[0025] 在本说明书一实施例中，基于所述访问验证信息向数据库主机发起访问请求，其中，基于最新接收到的访问验证信息向所述数据库主机发起访问请求。

[0026] 本说明书实施例还提供一种部署数据库访问权限的方法，所述方法包括：

[0027] 进行注册验证，其中，接收如本说明书实施例所述的注册信息并验证所述注册信息；

[0028] 当注册验证成功时，创建如本说明书实施例所述的访问验证信息，所述访问验证信息与注册验证发起方的身份匹配；

[0029] 向所述注册验证发起方发送所述访问验证信息。

[0030] 在本说明书一实施例中，接收如本说明书实施例所述的注册信息并验证所述注册信息，其中：

[0031] 接收与第一合法身份信息绑定的所述注册信息；

[0032] 验证所述第一合法身份信息与所述注册验证发起方是否匹配。

[0033] 在本说明书一实施例中，所述方法还包括：

[0034] 接收来自数据库主机的核实请求，所述核实请求包含访问请求发起方的身份标识；

[0035] 将可访问数据库列表返回给所述数据库主机，其中，所述可访问数据库列表为所述访问请求发起方可访问的数据库列表。

[0036] 在本说明书一实施例中，所述方法还包括：

[0037] 将拦截策略发送到数据库主机。

[0038] 在本说明书一实施例中，所述方法还包括：

[0039] 更新已创建的访问验证信息，其中，更新数据库口令；

[0040] 将更新后的访问验证信息发送到对应的所述注册验证发起方；

[0041] 监控当前正在被使用的数据库访问连接；

[0042] 在当前正在被使用的数据库访问连接中存在基于更新前的访问验证信息建立的数据库访问连接时，维持更新前的访问验证信息有效；

[0043] 在当前正在被使用的数据库访问连接中不存在基于更新前的访问验证信息建立的数据库访问连接时，销毁更新前的访问验证信息。

[0044] 本说明书实施例还提供一种验证数据库访问权限的方法，所述方法包括：

[0045] 接收如本说明书实施例所述的访问请求；

[0046] 验证所述访问请求；

[0047] 当所述访问请求通过验证时，容许访问请求发起方访问数据库。

[0048] 在本说明书一实施例中：

[0049] 接收所述访问请求，其中，所述访问请求包括与第二合法身份信息绑定的身份验证信息；

[0050] 验证所述访问请求，包括，验证所述第二合法身份信息与所述访问请求发起方是否匹配。

[0051] 在本说明书一实施例中，验证所述访问请求，还包括：

[0052] 生成核实请求，所述核实请求包含所述访问请求发起方的身份标识；

[0053] 将所述核实请求发送到访问控制平台；

[0054] 接收来自所述访问控制平台的可访问数据库列表，其中，所述可访问数据库列表为所述访问请求发起方可访问的数据库列表；

[0055] 根据所述可访问数据库列表验证所述访问请求，其中，验证所述访问请求对应的目标数据库是否在所述可访问数据库列表中。

[0056] 本说明书实施例还提供一种访问数据库的系统，所述系统包括：

[0057] 部署信息获取模块，其用于获取来自部署平台的注册凭证信息；

[0058] 注册验证发起模块，其用于根据所述注册凭证信息生成注册信息，基于所述注册信息向访问控制平台发起注册验证；

[0059] 访问验证信息获取模块，其用于接收来自所述访问控制平台的访问验证信息，其中，所述访问验证信息在所述注册验证成功后才能获取，所述访问验证信息包含有权访问的数据库实例信息，所述数据库实例信息包含对应的数据库口令；

[0060] 数据库访问模块，其用于基于所述访问验证信息向数据库主机发起访问请求，所述访问请求包括所述数据库口令。

[0061] 本说明书实施例还提供一种部署数据库访问权限的系统，所述系统包括：

[0062] 注册验证模块，其用于进行注册验证，其中，接收如本说明书实施例所述的注册信息并验证所述注册信息；

[0063] 访问验证信息创建模块，其用于当注册验证成功时，创建如本说明书实施例所述的访问验证信息，所述访问验证信息与注册验证发起方的身份匹配；

[0064] 访问验证信息发送模块，其用于向所述注册验证发起方发送所述访问验证信息。

[0065] 本说明书实施例还提供一种验证数据库访问权限的系统，所述系统包括：

[0066] 访问请求获取模块，其用于接收如本说明书实施例所述的访问请求；

[0067] 访问请求验证模块，其用于验证所述访问请求，当所述访问请求通过验证时，容许访问请求发起方访问数据库。

[0068] 本申请还提出了一种用于在用户设备端信息处理的设备，该设备包括用于存储计算机程序指令的存储器和用于执行程序指令的处理器，其中，当该计算机程序指令被该处理器执行时，触发该设备执行本说明书实施例所述系统所述的方法。

[0069] 本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果：根据本说明书实施例的方法，部署平台不直接颁发数据库口令，而是颁发用于标识访问者合法性的

注册凭证信息，在访问控制平台颁发数据库口令时首先要验证注册凭证信息，验证通过后再颁发数据库口令；相较于现有技术，根据本说明书实施例的方法可以大大降低了数据库口令错发、泄露的可能性，提高了数据库系统的安全性，大大降低了数据库被拖库的风险。

附图说明

[0070] 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：

[0071] 图1、图3、图5以及图9为本说明书实施例中应用程序的运行方法的流程图；

[0072] 图7以及图8为本说明书实施例中应用程序的运行方法的部分流程图；

[0073] 图2、图4、图6、图8以及图10～12为本说明书实施例中系统的结构框图。

具体实施方式

[0074] 为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例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。

[0075] 在现有技术中，通常基于数据库口令实现对数据库访问者的鉴权。即，为具有访问权限的访问者颁发对应的数据库口令。在访问者访问数据库时，验证其具备的数据库口令，从而确定其是否具备访问权限。然而，随着企业生长，数据库系统规模和复杂性增大，这使得数据库口令的管理变得异常困难，从而导致数据库口令颁发错误、数据库口令泄露的发生几率大大增加，进而使得数据库被拖库的风险显著提升。

[0076] 针对上述问题，本说明书实施例提出了一种访问数据库的方法。根据本说明书实施例的方法，部署平台不直接颁发数据库口令，而是颁发用于标识访问者合法性的注册凭证信息，在访问控制平台颁发数据库口令时首先要验证注册凭证信息，验证通过后再颁发数据库口令；相较于现有技术，根据本说明书实施例的方法可以大大降低了数据库口令错发、泄露的可能性，提高了数据库系统的安全性，大大降低了数据库被拖库的风险。

[0077] 以下结合附图，详细说明本说明书各实施例提供的技术方案。

[0078] 在本说明书一实施例中，如图1所示，访问数据库的方法包括：

[0079] S110，获取来自部署平台的注册凭证信息；

[0080] S120，根据注册凭证信息生成注册信息，基于注册信息向访问控制平台发起注册验证；

[0081] S130，接收来自访问控制平台的访问验证信息，其中，访问验证信息在注册验证成功后才能获取，访问验证信息包含有权访问的数据库实例信息，该数据库实例信息包含对应的数据库口令；

[0082] S140，基于访问验证信息向数据库主机发起访问请求，该访问请求包括数据库口令。

[0083] 进一步的，基于本说明书实施例的访问数据库的方法，本说明书实施例还提出了一种访问数据库的系统。如图2所示，访问数据库的系统包括：

[0084] 部署信息获取模块210，其用于获取来自部署平台的注册凭证信息；

[0085] 注册验证发起模块220，其用于根据注册凭证信息生成注册信息，基于注册信息向访问控制平台发起注册验证；

[0086] 访问验证信息获取模块230，其用于接收来自访问控制平台的访问验证信息，其中，访问验证信息在注册验证成功后才能获取，访问验证信息包含有权访问的数据库实例信息，数据库实例信息包含对应的数据库口令；

[0087] 数据库访问模块240，其用于基于访问验证信息向数据库主机发起访问请求，访问请求包括所述数据库口令。

[0088] 具体的，在本说明书一实施例中，访问数据库的系统被构造在业务系统中。

[0089] 进一步的，基于本说明书实施例的访问数据库的方法，本说明书实施例还提出了一种部署数据库访问权限的方法。如图3所示，在本说明书一实施例中，部署数据库访问权限的方法包括：

[0090] S310，进行注册验证，其中，接收本说明书实施例所述的注册信息并验证该注册信息；

[0091] S320，当注册验证成功时，创建如本说明书实施例所述的访问验证信息，该访问验证信息与注册验证发起方的身份匹配；

[0092] S330，向注册验证发起方发送访问验证信息。

[0093] 进一步的，在本说明书一实施例的部署数据库访问权限的方法中，在创建如本说明书实施例所述的访问验证信息后，还将访问验证信息的相关数据(例如，数据库口令)发送到数据库主机。

[0094] 具体的，在本说明书一实施例的部署数据库访问权限的方法中，在创建针对注册验证发起方(业务系统)的访问验证信息时，针对注册验证发起方(业务系统)有权访问的数据库实例创建数据库账号(数据库账号包含数据库口令)。在向注册验证发起方(业务系统)发送访问验证信息时，发送其有权访问的数据库实例的数据库账号。

[0095] 进一步的，基于本说明书实施例的部署数据库访问权限的方法，本说明书实施例还提出了一种部署数据库访问权限的系统(访问控制平台)。如图4所示，部署数据库访问权限的系统包括：

[0096] 注册验证模块410，其用于进行注册验证，其中，接收如本说明书实施例所述的注册信息并验证所述注册信息；

[0097] 访问验证信息创建模块420，其用于当注册验证成功时，创建如本说明书实施例所述的访问验证信息，访问验证信息与注册验证发起方的身份匹配；

[0098] 访问验证信息发送模块430，其用于向注册验证发起方发送访问验证信息。

[0099] 进一步的，基于本说明书实施例的访问数据库的方法，本说明书实施例还提出了一种验证数据库访问权限的方法。如图5所示，在本说明书一实施例中，验证数据库访问权限的方法包括：

[0100] S510，接收如本说明书实施例所述的访问请求；

[0101] S520，验证所述访问请求；

[0102] S530，当访问请求通过验证时，容许访问请求发起方访问数据库。

[0103] 进一步的，基于本说明书实施例的验证数据库访问权限的方法，本说明书实施例还提出了一种验证数据库访问权限的系统。如图6所示，验证数据库访问权限的系统包括：

[0104] 访问请求获取模块610，其用于接收如本说明书实施例所述的访问请求；

[0105] 访问请求验证模块620，其用于验证访问请求，当访问请求通过验证时，容许访问请求发起方访问数据库。

[0106] 具体的，在本说明书一实施例中，验证数据库访问权限的系统被构造在数据库主机中。

[0107] 进一步的，为了降低数据库口令错发、泄露的可能性，在本说明书一实施例中，在颁发数据库口令时，采用了注册凭证以及注册者身份双重验证的方案。

[0108] 具体的，在本说明书一实施例的访问数据库的方法中，在获取所述注册凭证信息时，获取的注册凭证信息包括与第一合法身份信息绑定的注册凭证；在根据注册凭证信息生成注册信息的过程中，注册信息包括与第一合法身份信息绑定的注册凭证。

[0109] 对应的，在本说明书一实施例的部署数据库访问权限的方法中，在接收注册信息时，接收与第一合法身份信息绑定的注册信息；在验证注册信息的过程中，验证第一合法身份信息与注册验证发起方是否匹配。

[0110] 具体的，在本说明书一实施例中，部署系统向注册验证发起方发送应用私钥凭证，该凭证和合法访问者身份(第一合法身份信息)绑定。注册验证发起方向访问控制平台发起注册验证时，使用来自部署系统的应用私钥凭证签名注册请求。访问控制平台进行注册验证时，验证注册请求的签名并同时校验注册请求的来源是否与其绑定的合法访问者身份一致。

[0111] 进一步的，为了避免由数据库口令泄露带来的数据库非法访问情况的发生，在本说明书一实施例中，在验证包含是数据库口令的访问请求时，采用了数据库口令与访问者身份双重验证的方案。

[0112] 具体的，在本说明书一实施例的部署数据库访问权限的方法中，创建的访问验证信息还包括与第二合法身份信息绑定的身份验证信息，第二合法身份信息为访问验证信息所对应的访问者的身份信息。

[0113] 对应的，在本说明书一实施例的访问数据库的方法中，接收到的来自访问控制平台的访问验证信息还包括与第二合法身份信息绑定的身份验证信息。

[0114] 对应的，在本说明书一实施例的验证数据库访问权限的方法中，在接收访问请求时，该访问请求包括与第二合法身份信息绑定的身份验证信息；在验证访问请求的过程中，验证第二合法身份信息与访问请求发起方是否匹配。

[0115] 具体的，在本说明书一实施例中，当访问控制平台进行注册验证并验证成功时，访问控制平台向注册验证发起方返回应用有权访问的数据库实例信息(包括数据库口令)以及标识应用身份的证书和私钥(该证书和应用身份绑定，且证书包含应用名称)。当注册验证发起方向数据库主机发起访问请求时，其使用访问控制平台返回的应用身份证书和数据库口令向数据库主机发起建立数据库访问连接。数据库主机在验证数据库口令的同时还验证应用身份证书所绑定的应用身份与发起建立数据库访问连接的来源方是否匹配。

[0116] 进一步的，为了进一步避免由数据库口令泄露带来的数据库非法访问情况的发生，还直接验证访问者身份对应的访问权限。具体的，根据访问者身份，确认其有权访问的数据库列表，验证当前访问请求的访问对象是否被包含在该数据库列表中。

[0117] 具体的，在本说明书一实施例的验证数据库访问权限的方法中，如图7所示，在验

证访问请求的过程中：

[0118] S710，生成核实请求，该核实请求包含访问请求发起方的身份标识；

[0119] S720，将核实请求发送到访问控制平台；

[0120] S730，接收来自访问控制平台的可访问数据库列表，其中，可访问数据库列表为访问请求发起方可访问的数据库列表；

[0121] S740，根据可访问数据库列表验证访问请求，其中，验证访问请求对应的目标数据库是否在可访问数据库列表中。

[0122] 对应的，在本说明书一实施例的部署数据库访问权限的方法中，如图8所示，方法还包括：

[0123] S810，接收来自数据库主机的核实请求，该核实请求包含访问请求发起方的身份标识；

[0124] S820，将可访问数据库列表返回给数据库主机，其中，该可访问数据库列表为对应核实请求的访问请求发起方可访问的数据库列表。

[0125] 具体的，在本说明书一实施例的应用场景中，如图9所示：

[0126] S900，部署平台向业务系统(注册验证发起方/数据库访问请求发起方)发布和业务应用身份绑定的应用私钥凭证；

[0127] S911，业务系统接收绑定了业务应用身份的应用私钥凭证；

[0128] S912，使用应用私钥凭证签名注册请求；

[0129] S913，向访问控制平台发起注册验证；

[0130] S921，访问控制平台验证注册请求的签名并同时验证与签名绑定的业务应用身份与业务系统的身份是否匹配；

[0131] S922，注册验证通过后，访问控制平台针向业务系统返回其有权访问的数据库实例信息(包括数据库口令)以及标识应用身份的证书和私钥(证书和应用身份绑定，且证书包含应用名称)；

[0132] S914，业务系统接收其有权访问的数据库实例信息以及标识应用身份的证书和私钥；

[0133] S915，当业务系统需要访问数据库时，基于应用身份证书以及数据库口令向数据库主机发起访问请求；

[0134] S931，数据库主机接收访问请求；

[0135] S932，数据库主机验证应用身份证书所绑定的应用身份与访问请求的发起方是否一致；

[0136] S933，数据库主机向访问控制平台发送访问请求的发起方的应用名称；

[0137] S923，访问控制平台向数据库主机返回访问请求的发起方有权访问的数据库列表；

[0138] S934，数据库主机验证访问请求对应的目标数据库是否在访问请求的发起方有权访问的数据库列表中；

[0139] S935，数据库主机验证数据库口令。

[0140] 进一步的，为了进一步提高数据库访问的安全性，在本说明书一实施例的部署数据库访问权限的方法中，方法还包括：将拦截策略发送到数据库主机。这样，数据库主机在

发现非法访问请求时，就可以根据接收到的拦截策略做出有效的拦截操作，避免非法用户访问数据库。

[0141] 进一步的，考虑到长期使用相同的数据库口令，会加大数据库口令被泄露的风险。因此，在本说明书一实施例的部署数据库访问权限的方法中，方法还包括：更新已创建的访问验证信息，其中，更新数据库口令；将更新后的访问验证信息发送到对应的注册验证发起方(业务系统)。

[0142] 进一步的，在本说明书一实施例的部署数据库访问权限的方法中，在更新访问验证信息后，还将更新后的访问验证信息的相关数据(例如，更新后的数据库口令)发送到数据库主机。

[0143] 进一步的，在访问验证信息被更新后，如果更新前的访问验证信息仍然有效，那就失去了更新访问验证信息的意义。但是，如果直接销毁(无效)更新前的访问验证信息，就可能出现正在使用的数据库访问连接被中途中断的情况，导致业务系统运行错误或者数据丢失。因此，在本说明书一实施例的部署数据库访问权限的方法中，在更新访问验证信息后：监控当前正在被使用的数据库访问连接；在当前正在被使用的数据库访问连接中存在基于更新前的访问验证信息建立的数据库访问连接时，维持更新前的访问验证信息有效；在当前正在被使用的数据库访问连接中不存在基于更新前的访问验证信息建立的数据库访问连接时，销毁(无效)更新前的访问验证信息。

[0144] 对应的，在本说明书一实施例的访问数据库的方法中，基于最新接收到的访问验证信息向数据库主机发起访问请求。

[0145] 具体的，在本说明书一实施例的部署数据库访问权限的方法中，在创建针对注册验证发起方(业务系统)的访问验证信息时，针对注册验证发起方(业务系统)有权访问的数据库实例创建数据库账号(数据库账号包含数据库口令)。在向注册验证发起方(业务系统)发送访问验证信息时，发送其有权访问的数据库实例的数据库账号。在更新访问验证信息时，对指定的数据库实例创建新的数据库帐号(不同于老帐号的口令)，然后将新帐号和口令推送给有权限访问该数据库实例的注册验证发起方(业务系统)并将新账号发送给数据库主机。令注册验证发起方(业务系统)创建新数据库连接时，使用新的帐号创建连接(数据库主机也基于新账号进行合法性验证)。监控数据库中老帐号创建的数据库连接数，连接数降为0时，无效老帐号(销毁数据库主机上的老帐号)。

[0146] 具体的，在本说明书一实施例中，如图10所示，(1)访问控制平台101创建新数据库账号，将新数据库账号发送到数据库主机102；(2)访问控制平台101向业务系统100推送新数据库账号；(3)业务系统100使用新数据库账号新建数据库连接到数据库主机102；(4)访问控制平台101监控数据库主机102，监控老帐号连接数量，当老帐号连接数量降为0时，销毁数据库主机102上的老帐号。

[0147] 进一步的，为了避免业务系统被破解，从而导致数据库口令和/或其他验证凭证泄露，在本说明书一实施例的访问数据库的方法中，利用与数据库访问请求方的业务进程相独立的数据库访问模块(访问数据库的系统)实现生成注册信息、和/或发起注册验证、和/或发起访问请求。

[0148] 具体的，在本说明书一实施例的访问数据库的方法中，利用与数据库访问请求方的业务进程相独立的数据库访问模块(访问数据库的系统)实现与部署平台、访问控制平

台、数据库主机以及数据库访问请求方(业务系统)的业务进程间的数据交互。

[0149] 具体的,在本说明书一实施例中,如图11所示,业务系统110包含数据库访问模块111,数据库访问模块111与业务系统110的业务进程112相互独立。数据库访问模块111连接到部署平台120、访问控制平台130以及数据库主机140。

[0150] 进一步的,在本说明书一实施例的访问数据库的方法中,在获取注册凭证信息的过程中:利用数据库访问模块接收来自部署平台的加密信息,其中,该加密信息的解密密钥内置在数据库访问模块中;利用数据库访问模块解密加密信息,获取注册凭证信息。

[0151] 进一步的,在本说明书一实施例的访问数据库的方法中,加密信息的解密密钥仅内置在数据库访问模块中。

[0152] 进一步的,在本说明书一实施例的访问数据库的方法中,方法还包括:启动数据库访问模块,其中,数据库访问模块由部署平台以独立容器或进程启动。

[0153] 进一步的,在本说明书一实施例的访问数据库的方法中,在基于所述访问验证信息向数据库主机发起访问请求的过程中:将数据库访问模块视作数据库本地代理,由业务进程向数据库访问模块发起SQL连接;由数据库访问模块向数据库主机发起TLS数据库连接。具体的,当业务系统需要访问数据库时,业务系统的业务进程将数据库访问模块视作数据库本地代理,向数据库访问模块发起SQL连接;数据库访问模块向数据库主机发起TLS数据库连接。

[0154] 进一步的,在本说明书一实施例的访问数据库的方法中,利用数据库Sidecar模块构建数据库访问模块。对应的,在本说明书一实施例的部署数据库访问权限的方法中,利用数据库Sidecar模块构建访问控制平台(部署数据库访问权限的系统)。对应的,在本说明书一实施例的验证数据库访问权限的方法中,利用数据库Sidecar模块构建数据库主机的访问请求验证模块(验证数据库访问权限的系统)。

[0155] 具体的,在本说明书一实施例中,如图12所示,业务主机1210包含业务进程1211以及Sidecar模块1212(数据库访问模块)。部署平台1220发布业务系统时会以独立容器或进程启动Sidecar模块1212,同时传递只有Sidecar模块1212内置密钥才能解密的应用私钥凭证,该凭证和业务应用身份绑定。

[0156] Sidecar模块1212启动时向Sidecar控制平台1230注册(https请求),用获取的应用私钥凭证签名访问请求。Sidecar控制平台1230检验签名同时附加校验签名来源IP是否为签名声称的业务应用。当校验通过时,Sidecar控制平台1230向Sidecar模块1212返回应用有权访问的数据库实例信息(包括数据库口令)以及标识应用身份的证书和私钥(该证书和应用身份绑定,且证书包含应用名称)。

[0157] 业务进程1211运行时将Sidecar模块1212视作数据库本地代理,发起SQL连接。Sidecar模块1212使用Sidecar控制平台1230返回的应用身份证书和数据库口令向数据库主机1240的Sidecar模块1241建立TLS数据库连接。

[0158] 数据库的Sidecar模块1241从对端TLS请求(来自Sidecar模块1212)的证书识别请求来源应用名称,调用Sidecar控制平台1230获取来源应用可访问的数据库列表,如果访问请求对应的数据库连接的目标数据库不在可访问列表中,断开连接。数据库的Sidecar模块1241在访问请求合法时,向数据库进程1242发起SQL连接。

[0159] 进一步的,Sidecar控制平台1230推送给数据库的Sidecar模块1241拦截策略,细

粒度对入侵拖库行为拦截止血。

[0160] 进一步的，基于本发明的方法，本发明还提出了一种用于在用户设备端信息处理的设备，该设备包括用于存储计算机程序指令的存储器和用于执行程序指令的处理器，其中，当该计算机程序指令被该处理器执行时，触发该设备执行本发明所述的方法。

[0161] 在20世纪90年代，对于一个技术的改进可以很明显地区分是硬件上的改进(例如，对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件(Programmable Logic Device,PLD)(例如现场可编程门阵列(Field Programmable Gate Array,FPGA))就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言(Hardware Description Language,HDL)，而HDL也并非仅有一种，而是有许多种，如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等，目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[0162] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit,ASIC)、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器:ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20以及Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0163] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[0164] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0165] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明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，本发明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。

[0166] 本发明是参照根据本发明实施例的方法、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。

[0167] 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。

[0168] 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。

[0169] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0170] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0171] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0172] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0173] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0174] 本说明书中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。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0175] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

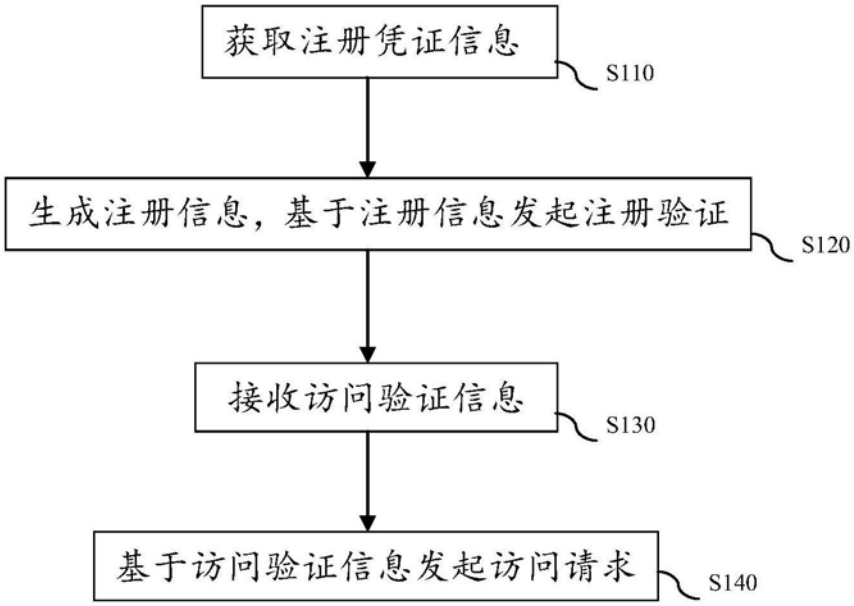

获取注册凭证信息
S110
生成注册信息，基于注册信息发起注册验证
S120
接收访问验证信息
S130
基于访问验证信息发起访问请求
S140

图1

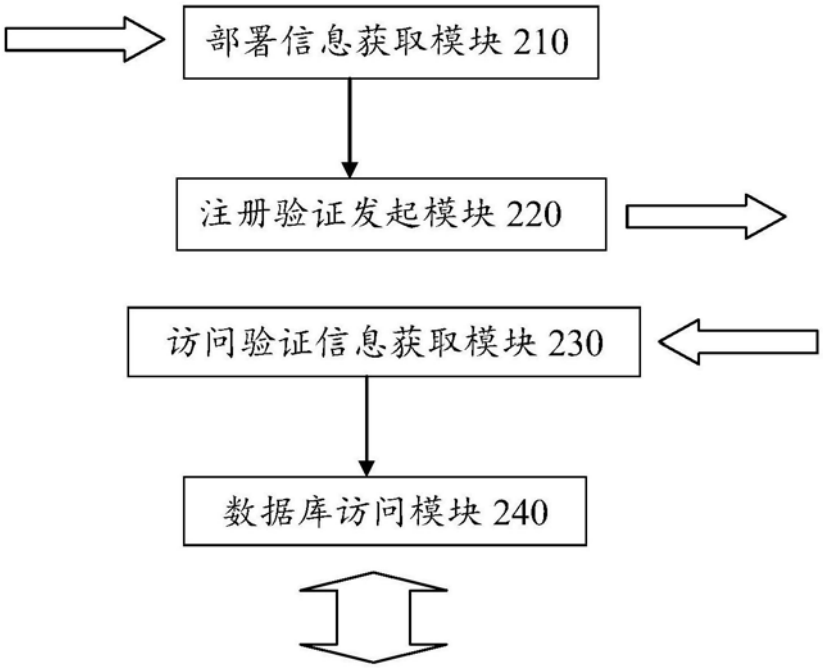

部署信息获取模块 210
注册验证发起模块 220
访问验证信息获取模块 230
数据库访问模块 240

图2

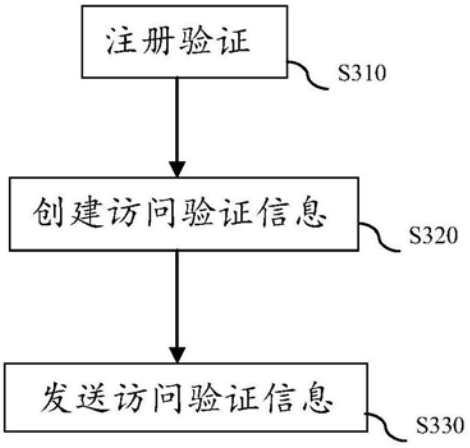

注册验证
S310
创建访问验证信息
S320
发送访问验证信息
S330

图3

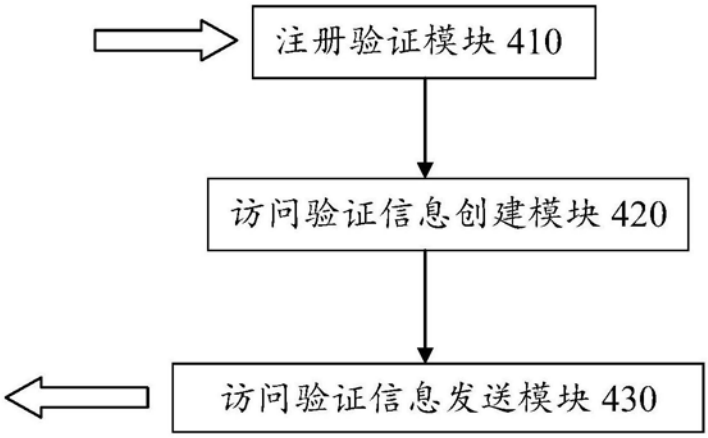

注册验证模块 410
访问验证信息创建模块 420
访问验证信息发送模块 430

图4

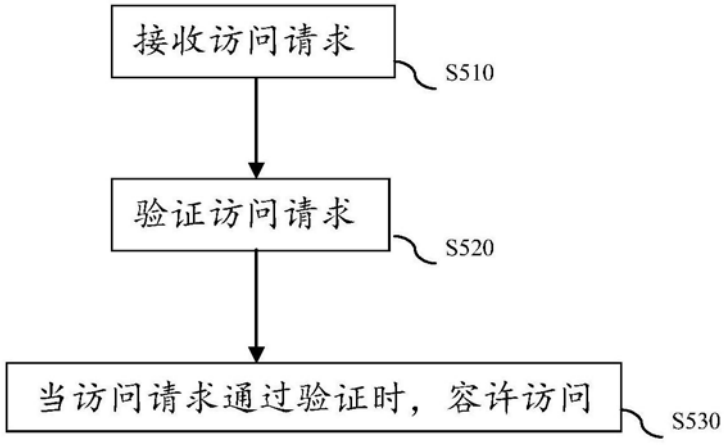

接收访问请求
S510
验证访问请求
S520
当访问请求通过验证时，容许访问
S530

图5

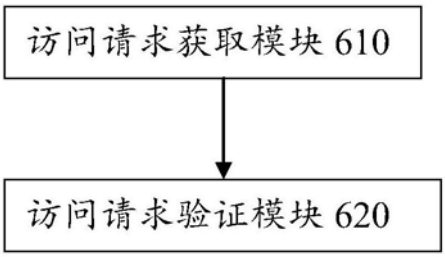

访问请求获取模块 610
访问请求验证模块 620

图6

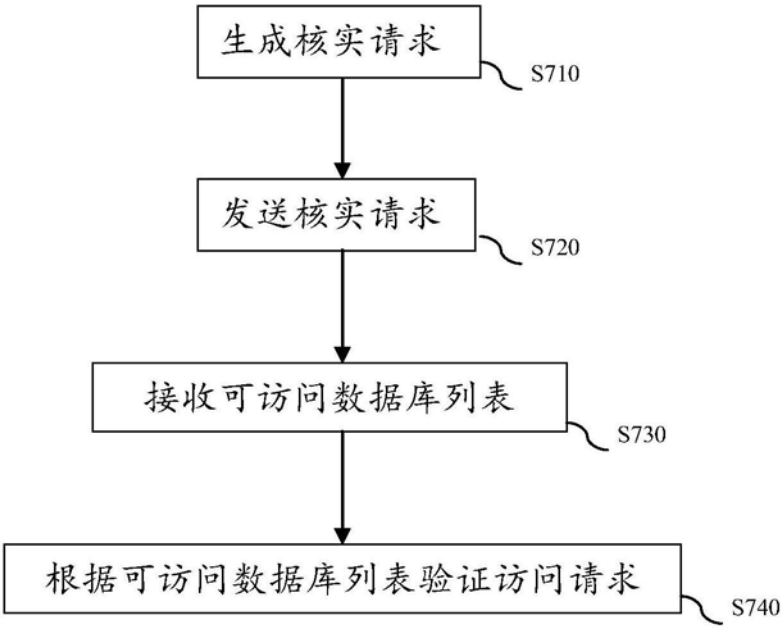

生成核实请求
S710
发送核实请求
S720
接收可访问数据库列表
S730
根据可访问数据库列表验证访问请求
S740

图7

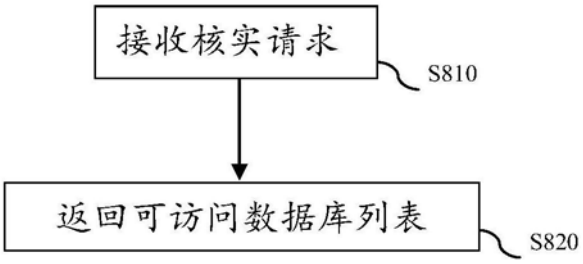

接收核实请求
S810
返回可访问数据库列表
S820

图8

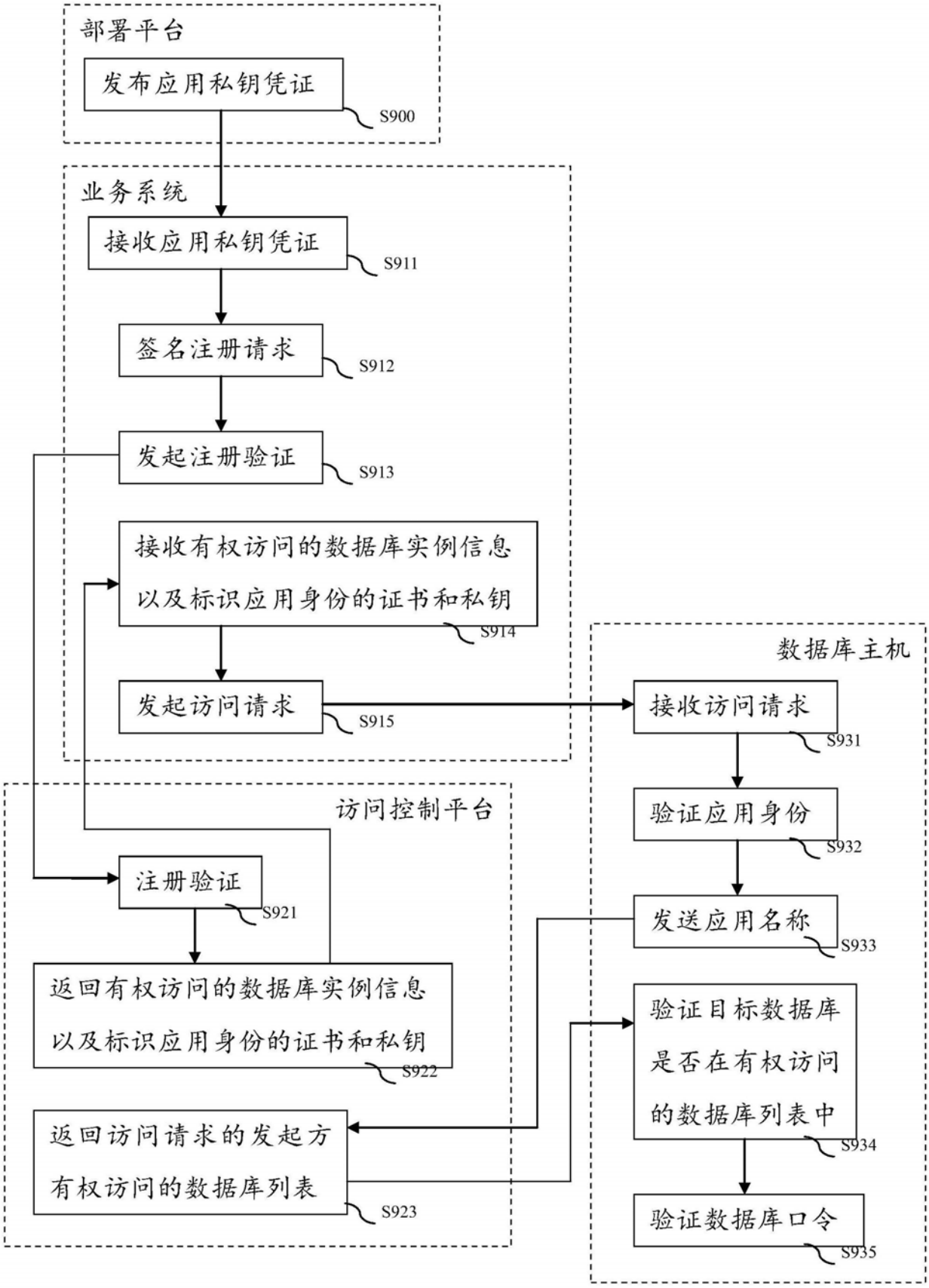

部署平台
发布应用私钥凭证
S900
业务系统
接收应用私钥凭证
S911
签名注册请求
S912
发起注册验证
S913
接收有权访问的数据库实例信息
以及标识应用身份的证书和私钥
S914
发起访问请求
S915
数据库主机
接收访问请求
S931
验证应用身份
S932
发送应用名称
S933
验证目标数据库
是否在有权访问
的数据库列表中
S934
验证数据库口令
S935
访问控制平台
注册验证
S921
返回有权访问的数据库实例信息
以及标识应用身份的证书和私钥
S922
返回访问请求的发起方
有权访问的数据库列表
S923

图9

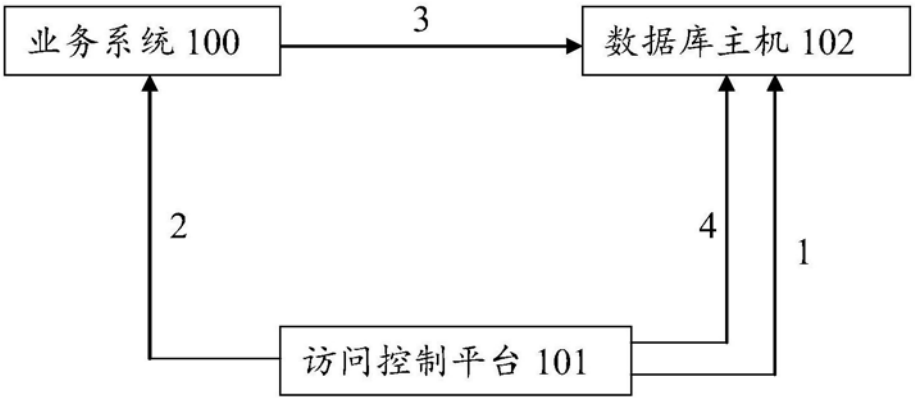

业务系统 100
3
数据库主机 102
2
4
1
访问控制平台 101

图10

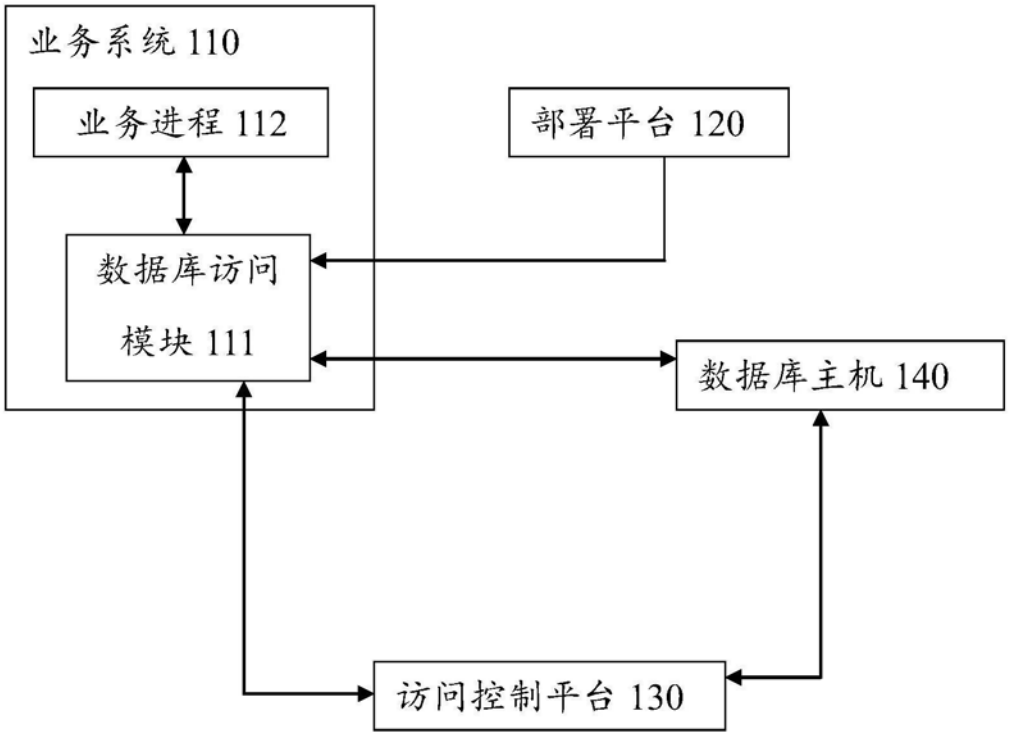

业务系统 110
业务进程 112
部署平台 120
数据库访问
模块 111
数据库主机 140
访问控制平台 130

图11

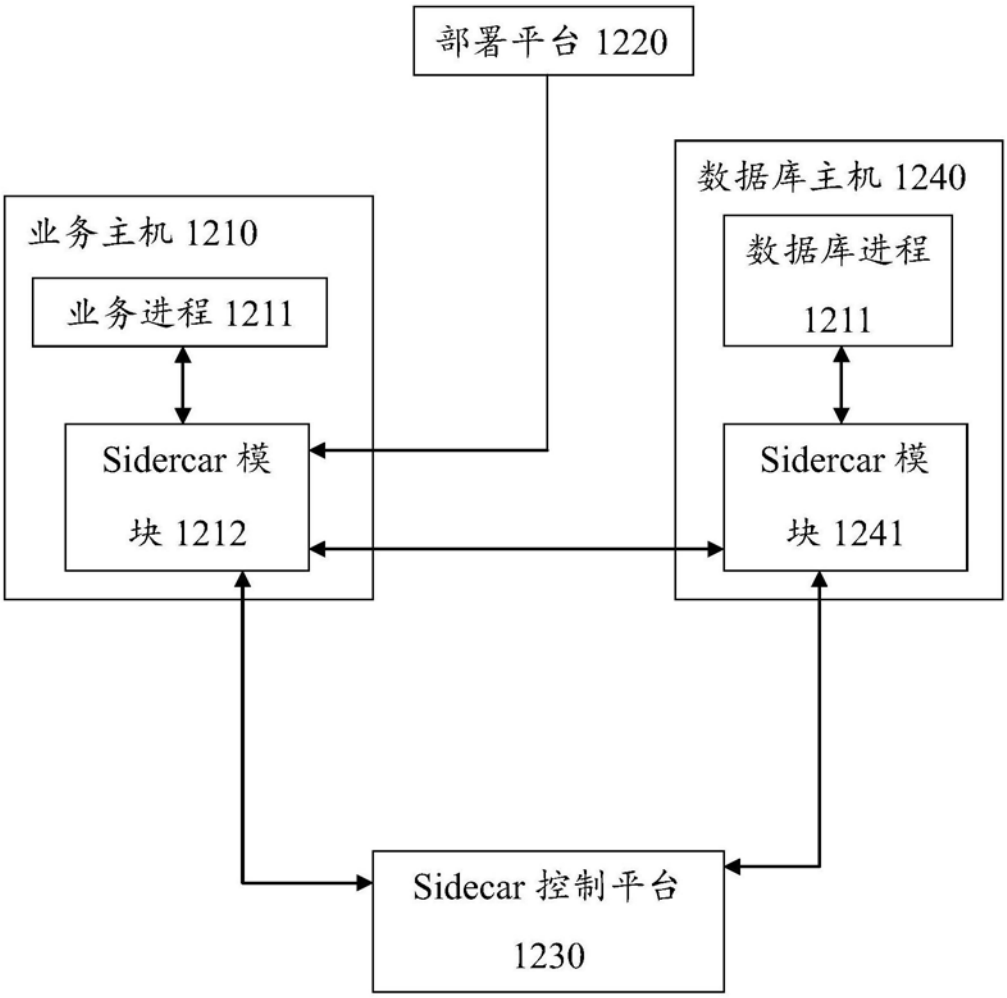

部署平台 1220
数据库主机 1240
数据库进程 1211
业务主机 1210
业务进程 1211
Sidercar 模块 1212
Sidercar 模块 1241
Sidecar 控制平台 1230

图12