(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 110061983 A
(43)申请公布日 2019.07.26

(21)申请号 201910281710.9

(22)申请日 2019.04.09

(71)申请人 苏宁易购集团股份有限公司
地址 210000 江苏省南京市玄武区苏宁大道1号

(72)发明人 郁国勇 孙迁

(74)专利代理机构 北京市万慧达律师事务所 11111
代理人 张慧娟

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

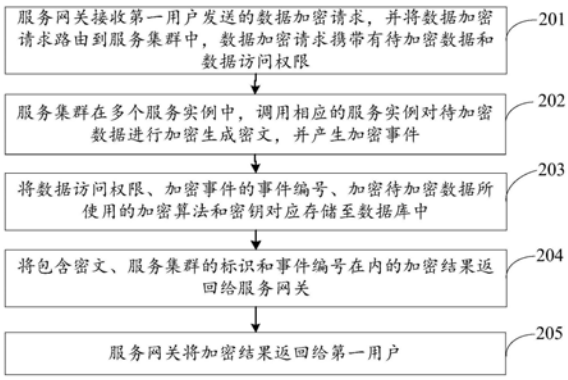
权利要求书2页 说明书9页 附图2页

(54)发明名称

一种数据处理方法及系统

(57)摘要

本发明公开了一种数据处理方法及系统，属于数据安全技术领域，方法包括：服务网关接收第一用户发送的数据加密请求，并将数据加密请求路由到服务集群中，数据加密请求携带有待加密数据和数据访问权限；服务集群在多个服务实例中，调用相应的服务实例对待加密数据进行加密生成密文，并产生加密事件；将数据访问权限、加密事件的事件编号、加密待加密数据所使用的加密算法和密钥对应存储至数据库中；将包含密文、服务集群的标识和事件编号在内的加密结果返回给服务网关；服务网关将加密结果返回给第一用户。本发明实施例能够降低数据生产方和使用方泄露密钥的风险，使得数据的安全性更高；且为数据访问权限最小化原则的落地提供了保障。



CN 110061983 A

1.一种数据处理方法,其特征在于,应用于数据处理系统中,所述数据处理系统包括服务网关和服务集群,所述服务集群包括多个服务实例,且所述服务集群中部署有数据库,所述方法包括:

所述服务网关接收第一用户发送的数据加密请求,并将所述数据加密请求路由到所述服务集群中,所述数据加密请求携带有待加密数据和数据访问权限;

所述服务集群在多个服务实例中,调用相应的服务实例对所述待加密数据进行加密生成密文,并产生加密事件;

将所述数据访问权限、所述加密事件的事件编号、加密所述待加密数据所使用的加密算法和密钥对应存储至所述数据库中;以及

将包含所述密文、所述服务集群的标识和所述事件编号在内的加密结果返回给所述服务网关;

所述服务网关将所述加密结果返回给所述第一用户。

2.根据权利要求1所述的方法,其特征在于,若所述服务集群的数量为多个时,所述将所述数据加密请求路由到所述服务集群中,包括:

根据预设的映射关系表,在多个所述服务集群中确定与所述第一用户具有映射关系的服务集群;

将所述数据加密请求路由至与所述第一用户具有映射关系的一个服务集群中。

3.根据权利要求2所述的方法,其特征在于,多个所述服务集群包括对称加密服务集群、Hash算法服务集群、不对称加密服务集群和业务定制加密服务集群中的至少两个。

4.根据权利要求1至3任意一项所述的方法,其特征在于,所述密钥是从密钥池中随机抽取到的,所述方法还包括:

根据预设的密钥更换条件,更换所述密钥池中的密钥。

5.根据权利要求4所述的方法,其特征在于,所述密钥更换条件为如下条件之一:

所述密钥池中的密钥的使用次数达到使用次数阈值;或者

所述密钥池中的密钥的存在时间达到时间阈值。

6.根据权利要求1所述的方法,其特征在于,所述方法还包括:

所述服务网关接收第二用户发送的数据解密请求,所述数据解密请求中携带有待加密密文、服务集群标识和加密事件编号;

所述服务网关将所述数据解密请求路由到所述服务集群标识对应的服务集群中;

所述服务集群从所述数据库中查询所述加密事件编号对应的数据访问权限,并在所述第二用户具有所述数据访问权限时,在所述多个服务实例中,调用相应的服务实例根据所述加密事件编号对应的加密算法和密钥对所述待加密密文进行解密得到明文;

所述服务集群将包含所述明文在内的解密结果返回给所述服务网关,以使所述服务网关将所述解密结果返回给所述第二用户。

7.根据权利要求1或6所述的方法,其特征在于,所述相应的服务实例是按照负载均衡方式或随机方式从所述多个服务实例中选择出的。

8.一种数据处理系统,其特征在于,包括服务网关和服务集群,所述服务集群包括多个服务实例,且所述服务集群中部署有数据库,其中:

所述服务网关,用于接收第一用户发送的数据加密请求,并将所述数据加密请求路由

到所述服务集群中，所述数据加密请求携带有待加密数据和数据访问权限；

所述服务集群，用于在多个服务实例中，调用相应的服务实例对所述待加密数据进行加密生成密文，并产生加密事件；

所述服务集群，还用于将所述数据访问权限、所述加密事件的事件编号、加密所述待加密数据所使用的加密算法和密钥对应存储至所述数据库中；以及

将包含所述密文、所述服务集群的标识和所述事件编号在内的加密结果返回给所述服务网关；

所述服务网关，还用于将所述加密结果返回给所述第一用户。

9.根据权利要求8所述的系统，其特征在于，若所述服务集群的数量为多个时，所述服务网关具体用于：

根据预设的映射关系表，在多个所述服务集群中确定与所述第一用户具有映射关系的服务集群；

将所述数据加密请求路由至与所述第一用户具有映射关系的一个服务集群中。

10.根据权利要求9所述的系统，其特征在于，多个所述服务集群包括对称加密服务集群、Hash算法服务集群、不对称加密服务集群和业务定制加密服务集群中的至少两个。

11.根据权利要求8至10任意一项所述的系统，其特征在于，所述密钥是从密钥池中随机抽取到的，所述服务集群具体还用于：

根据预设的密钥更换条件，更换所述密钥池中的密钥。

12.根据权利要求11所述的系统，其特征在于，所述密钥更换条件为如下条件之一：

所述密钥池中的密钥的使用次数达到使用次数阈值；或者

所述密钥池中的密钥的存在时间达到时间阈值。

13.根据权利要求8所述的系统，其特征在于，

所述服务网关，还用于接收第二用户发送的数据解密请求，所述数据解密请求中携带有待加密密文、服务集群标识和加密事件编号；

所述服务网关，还用于将所述数据解密请求路由到所述服务集群标识对应的服务集群中；

所述服务集群，还用于从所述数据库中查询所述加密事件编号对应的数据访问权限，并在所述第二用户具有所述数据访问权限时，在所述多个服务实例中，调用相应的服务实例根据所述加密事件编号对应的加密算法和密钥对所述待加密密文进行解密得到明文；

所述服务集群，还用于将包含所述明文在内的解密结果返回给所述服务网关；

所述服务网关，还用于将所述解密结果返回给所述第二用户。

14.根据权利要求8或13所述的系统，其特征在于，所述服务集群具体还用于：

按照负载均衡方式或随机方式从所述多个服务实例中选择出所述相应的服务实例。

一种数据处理方法及系统

技术领域

[0001] 本发明涉及数据安全技术领域,特别涉及一种数据处理方法及系统。

背景技术

[0002] 当前大数据领域中的数据安全管控的方法有以下几种:

[0003] 方法一、在入库前的数据生产或传输过程中使用同一个密钥对敏感数据进行加密,数据使用方使用对应密钥(对等或不对等)进行解密;

[0004] 方法二、对敏感数据进行高级别的权限管控,从物理和技术上保证只有必要的人员可以接触到敏感数据;

[0005] 方法三、在数据库的存取引擎上植入加解密机制,敏感数据加解密对用户透明。

[0006] 以上方法均存在缺陷和不足:

[0007] 针对第一种方法:数据生产方或使用方可以接触到加解密密钥,存在密钥泄露风险,密钥泄露则加密数据不再安全;

[0008] 针对第二种方法:虽然有高级别权限管控,但数据仓库管理人员还是可以直接接触敏感数据,不满足权限最小化原则;

[0009] 针对第三种方法:数据库存取引擎上植入加解密机制,不能避免数据在入库前数据流转过程中存在泄露的可能。

发明内容

[0010] 本发明旨在至少解决现有技术或相关技术中存在的技术问题之一,为此本发明提供一种数据处理方法及系统。

[0011] 本发明实施例提供的具体技术方案如下:

[0012] 第一方面,提供了一种数据处理方法,应用于数据处理系统中,所述数据处理系统包括服务网关和服务集群,所述服务集群包括多个服务实例,且所述服务集群中部署有数据库,所述方法包括:

[0013] 所述服务网关接收第一用户发送的数据加密请求,并将所述数据加密请求路由到所述服务集群中,所述数据加密请求携带有待加密数据和数据访问权限;

[0014] 所述服务集群在多个服务实例中,调用相应的服务实例对所述待加密数据进行加密生成密文,并产生加密事件;

[0015] 将所述数据访问权限、所述加密事件的事件编号、加密所述待加密数据所使用的加密算法和密钥对应存储至所述数据库中;以及

[0016] 将包含所述密文、所述服务集群的标识和所述事件编号在内的加密结果返回给所述服务网关;

[0017] 所述服务网关将所述加密结果返回给所述第一用户。

[0018] 进一步地,若所述服务集群的数量为多个时,所述将所述数据加密请求路由到所述服务集群中,包括:

[0019] 根据预设的映射关系表，在多个所述服务集群中确定与所述第一用户具有映射关系的服务集群；

[0020] 将所述数据加密请求路由至与所述第一用户具有映射关系的一个服务集群中。

[0021] 进一步地，多个所述服务集群包括对称加密服务集群、Hash算法服务集群、不对称加密服务集群和业务定制加密服务集群中的至少两个。

[0022] 进一步地，所述密钥是从密钥池中随机抽取到的，所述方法还包括：

[0023] 根据预设的密钥更换条件，更换所述密钥池中的密钥。

[0024] 进一步地，所述密钥更换条件为如下条件之一：

[0025] 所述密钥池中的密钥的使用次数达到使用次数阈值；或者

[0026] 所述密钥池中的密钥的存在时间达到时间阈值。

[0027] 进一步地，所述方法还包括：

[0028] 所述服务网关接收第二用户发送的数据解密请求，所述数据解密请求中携带有待加密密文、服务集群标识和加密事件编号；

[0029] 所述服务网关将所述数据解密请求路由到所述服务集群标识对应的服务集群中；

[0030] 所述服务集群从所述数据库中查询所述加密事件编号对应的数据访问权限，并在所述第二用户具有所述数据访问权限时，在所述多个服务实例中，调用相应的服务实例根据所述加密事件编号对应的加密算法和密钥对所述待加密密文进行解密得到明文；

[0031] 所述服务集群将包含所述明文在内的解密结果返回给所述服务网关，以使所述服务网关将所述解密结果返回给所述第二用户。

[0032] 进一步地，所述相应的服务实例是按照负载均衡方式或随机方式从所述多个服务实例中选择出的。

[0033] 第二方面，提供了一种数据处理系统，包括服务网关和服务集群，所述服务集群包括多个服务实例，且所述服务集群中部署有数据库，其中：

[0034] 所述服务网关，用于接收第一用户发送的数据加密请求，并将所述数据加密请求路由到所述服务集群中，所述数据加密请求携带有待加密数据和数据访问权限；

[0035] 所述服务集群，用于在多个服务实例中，调用相应的服务实例对所述待加密数据进行加密生成密文，并产生加密事件；

[0036] 所述服务集群，还用于将所述数据访问权限、所述加密事件的事件编号、加密所述待加密数据所使用的加密算法和密钥对应存储至所述数据库中；以及

[0037] 将包含所述密文、所述服务集群的标识和所述事件编号在内的加密结果返回给所述服务网关；

[0038] 所述服务网关，还用于将所述加密结果返回给所述第一用户。

[0039] 进一步地，若所述服务集群的数量为多个时，所述服务网关具体用于：

[0040] 根据预设的映射关系表，在多个所述服务集群中确定与所述第一用户具有映射关系的服务集群；

[0041] 将所述数据加密请求路由至与所述第一用户具有映射关系的一个服务集群中。

[0042] 进一步地，多个所述服务集群包括对称加密服务集群、Hash算法服务集群、不对称加密服务集群和业务定制加密服务集群中的至少两个。

[0043] 进一步地，所述密钥是从密钥池中随机抽取到的，所述服务集群具体还用于：

[0044] 根据预设的密钥更换条件，更换所述密钥池中的密钥。

[0045] 进一步地，所述密钥更换条件为如下条件之一：

[0046] 所述密钥池中的密钥的使用次数达到使用次数阈值；或者

[0047] 所述密钥池中的密钥的存在时间达到时间阈值。

[0048] 进一步地，所述服务网关，还用于接收第二用户发送的数据解密请求，所述数据解密请求中携带有待加密密文、服务集群标识和加密事件编号；

[0049] 所述服务网关，还用于将所述数据解密请求路由到所述服务集群标识对应的服务集群中；

[0050] 所述服务集群，还用于从所述数据库中查询所述加密事件编号对应的数据访问权限，并在所述第二用户具有所述数据访问权限时，在所述多个服务实例中，调用相应的服务实例根据所述加密事件编号对应的加密算法和密钥对所述待加密密文进行解密得到明文；

[0051] 所述服务集群，还用于将包含所述明文在内的解密结果返回给所述服务网关；

[0052] 所述服务网关，还用于将所述解密结果返回给所述第二用户。

[0053] 进一步地，所述服务集群具体还用于：

[0054] 按照负载均衡方式或随机方式从所述多个服务实例中选择出所述相应的服务实例。

[0055] 本发明实施例提供的技术方案带来的有益效果是：

[0056] 1、在数据加密和数据解密过程中，数据生产方和使用方均接触不到加解密密钥，从而降低了数据生产方和使用方泄露密钥的风险，使得数据的安全性更高；

[0057] 2、为数据访问权限最小化原则的落地提供了保障，保证了数据始终以特定的密文格式进行传输和存储，且传输过程和存储阶段涉及的系统和人员均无法获得明文，安全性高。

附图说明

[0058] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例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。

[0059] 图1是本发明实施例提供的一种应用环境的示意图；

[0060] 图2是本发明实施例一提供的一种数据处理方法的流程图；

[0061] 图3是本发明实施例二提供的一种数据处理方法的流程图；

[0062] 图4是本发明实施例三提供的一种数据处理系统的框图。

具体实施方式

[0063] 为使本发明的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明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前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0064] 在本申请的描述中，需要理解的是，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，在本申请的描述中，除非另有说明，“多个”的含义是两个或两个以上。

[0065] 图1是本发明实施例提供的一种应用环境的示意图，如图1所示，该应用环境可以包括客户端01、服务网关02和服务集群03。其中，客户端01可以是运行于数据生产方或数据提供方的用户设备中，也可以是运行于数据使用方的用户设备中，可以理解的是，客户端01的数量不限于一个，且上述的用户设备包括但不限于台式电脑、平板电脑、笔记本电脑、智能手机等类型的实体设备。服务网关02可以统一对客户端01提供REST API(Application Programming Interface，应用程序编程接口)以接收外部请求，将接收到的外部请求转发到后端的服务集群中，此外，服务网关还具备有权限控制等功能；服务集群03中包括服务实例1、服务实例2…..服务实例n等多个服务实例，多个服务实例中包括多种不同类型的服务实例，各类型中的服务实例的数量至少为一个，每个服务实例均可以通过部署相应的加密解密算法来提供加密解密服务。

[0066] 实施例一

[0067] 本发明实施例提供了一种数据处理方法，该数据处理方法应用于数据处理系统中，数据处理系统包括服务网关和服务集群，服务集群包括多个服务实例，且服务集群中部署有数据库，如图2所示，该数据处理方法可以包括步骤：

[0068] 201、服务网关接收第一用户发送的数据加密请求，并将数据加密请求路由到服务集群中，数据加密请求携带有待加密数据和数据访问权限。

[0069] 本实施例中，第一用户可以是数据生产方或数据提供方，第一用户通过第一客户端向服务网关提交数据加密请求。

[0070] 其中，数据加密请求中携带的待加密数据可以是包含有敏感信息的数据，例如，用户身份信息或资产信息等。

[0071] 数据加密请求中携带的数据访问权限用于指示对待加密数据的密文进行解密的权限，数据访问权限中可以包含有授权访问用户的用户标识，该用户标识可以是用户名、客户端地址(例如，MAC地址)等，这里不做限定。

[0072] 其中，上述的服务集群可以为对称加密服务集群、Hash算法服务集群、不对称加密服务集群和业务定制加密服务集群中的任意一个。服务集群中包括的多个服务实例中可以包括多种不同类型的服务实例，各类型中的服务实例的数量至少为一个，每个服务实例均可以通过部署相应的加密解密算法来提供加密解密服务。这里所说的类型是指部署的加解密算法相同。

[0073] 若服务集群为对称加密服务集群时，则该服务集群中可以包括若干个DES加密服务实例、若干个3DES加密服务实例、若干个SM4加密服务实例、若干个AES加密服务实例；若服务集群为Hash算法服务集群时，则该服务集群中可以包括若干个MD5服务实例、若干个SHA服务实例、若干个SM3服务实例；若干个AES加密服务实例；若服务集群为非对称加密服务集群时，则该服务集群中可以包括若干个RSA加密服务实例、若干个ECC加密服务实例、若干个SM2加密服务实例。

[0074] 进一步地，在步骤201中将数据加密请求路由到服务集群中步骤之前，本发明实施例提供的方法还可以包括：

[0075] 对第一用户进行身份认证和鉴权，若第一用户未通过身份认证或鉴权，则向第一

用户返回加密请求失败信息，若第一用户通过鉴权，则将数据加密请求路由到服务集群中。

[0076] 本实施例中，通过对服务调用方进行身份认证并进行鉴权，如此通过权限控制可以为不同的客户端提供不同的权限，为服务集群的访问及可用性等提供监控功能，且可以针对不同的客户端开放不同的服务集群，从而可以提高访问服务集群的安全性。

[0077] 进一步地，若服务集群的数量为多个时，步骤201中服务网关将数据加密请求路由到服务集群中，该过程可以包括：

[0078] 根据预设的映射关系表，在多个服务集群中确定与数据加密请求中的用户标识具有映射关系的服务集群，将数据加密请求路由至与用户标识具有映射关系的一个服务集群中。

[0079] 其中，多个服务集群包括对称加密服务集群、Hash算法服务集群、不对称加密服务集群和业务定制加密服务集群中的至少两个。

[0080] 在具体实施过程中，服务网关可以在数据生产方或数据提供方完成服务注册后，建立数据生产方或数据提供方的用户标识和多个服务集群之间的映射关系，从而在数据生产方或数据提供方通过第一客户端，该映射关系可以一对一的关系，也可以一对多的关系，若为一对多的关系，可以将数据加密请求随机路由至与用户标识具有映射关系的一个服务集群中。

[0081] 此外，当数据加密请求中携带有指定的加密服务标识时，可以将该加密服务请求路由至与用户标识具有映射关系的、且加密服务标识对应的服务集群中。

[0082] 本实施例中，在服务集群的数量为多个时，通过根据预设的映射关系表，将加密请求路由至与数据加密请求中的用户标识具有映射关系的服务集群中，如此可以满足不同用户的不同加密服务的调用需求，且实现了对加密服务集群的安全访问进行控制，从而提高了访问服务集群的安全性。

[0083] 202、服务集群在多个服务实例中，调用相应的服务实例对待加密数据进行加密生成密文，并产生加密事件。

[0084] 具体的，该过程可以包括：

[0085] 按照负载均衡方式或随机方式从多个服务实例中选择出相应的服务实例；

[0086] 调用该服务实例根据预置该服务实例上的加密算法和预先生成的密钥对待加密数据进行加密，生成密文，同时产生加密事件。

[0087] 其中，按照负载均衡方式从多个服务实例中选择出相应的服务实例，包括：

[0088] 对多个服务实例的负载状态进行实时监控，并根据监控结果，按照负载均衡方式从多个服务实例中选择当前负载最小一个服务实例。

[0089] 其中，服务实例的负载状态可以包括CPU使用率、内存使用率、磁盘读写、网络连接状态中的一种或多种。

[0090] 其中，用于加密待加密数据的密钥是从密钥池中随机抽取到的。于本实施例中，可以预先对不同类型的加密算法分别设定加解密密钥池，并在加解密密钥池中预先生成预设数量的密钥，服务集群在调用服务实例进行加密服务时，可以从对应的加解密密钥池中随机抽取一个/对密钥作为本次加密待加密数据的密钥。

[0091] 进一步地，本发明实施例提供的方法还包括：

[0092] 根据预设的密钥更换条件，更换密钥池中的密钥。

[0093] 其中,密钥更换条件为如下条件之一:

[0094] 密钥池中的密钥的使用次数达到使用次数阈值;或者

[0095] 密钥池中的密钥的存在时间达到时间阈值。

[0096] 具体的,可以当密钥池中的密钥的使用次数达到使用次数阈值时,将该密钥从密钥池中删除,并同时生成一个/对新的密钥放入密钥池中;或者,可以将当密钥池中的密钥的存在时间达到时间阈值时,将该密钥从密钥池中删除,并同时生成一个/对新的密钥放入密钥池中。

[0097] 本发明实施例中,通过根据预设的密钥更换条件更换密钥池中的密钥,能够进一步提供数据加密过程中的安全性。

[0098] 示例性地,假如在多个服务实例中,调用的一个服务实例为AES加密服务实例,若待加密数据为身份证号,调用AES加密服务实例根据AES算法和从密钥池中随机抽取的密钥对身份证号进行加密,生成身份证号的密文为“eeL3FXVjnhb7J3xOjYJbkiQZnnQjYOQHScUG7VsWvCE=”,对应的密文长度为44byte,加密服务同时生成一个事件编号,该事件编号用于唯一标识本次的加密事件,其中,该事件编号可以为一个64位长度的流水号,并通过使用十进制来表示。

[0099] 203、将数据访问权限、加密事件的事件编号、加密待加密数据所使用的加密算法和密钥对应存储至数据库中。

[0100] 其中,数据库可以采用键值(Key-Value)数据库,键值数据库可以将数据按照键值对的形式进行组织、索引和存储。

[0101] 具体的,以加密事件的事件编号作为Key,以数据访问权限、加密待加密数据所使用的加密算法和密钥作为Value,对应存储至键值数据库中。

[0102] 本实施例中,通过使用键值数据库进行存储加密事件的事件编号、数据访问权限、加密待加密数据所使用的加密算法和密钥,可以便于后续可以基于加密事件编号的快速检索,检索性能高,使得数据库资源消耗小,且可以实现对密文的数据访问权限进行管控,避免了数据库中的加密算法和密钥被不适当的用户调用服务集群中的解密服务而解密得到明文,从而进一步确保了数据的安全性。

[0103] 204、将包含密文、服务集群的标识和事件编号在内的加密结果返回给服务网关。

[0104] 具体的,对加密事件编号、服务集群的标识和加密事件编号按照一定数据格式进行组装,得到加密结果。

[0105] 在具体实施过程中,加密结果可以是由事件编号的字节数组、服务集群的标识和密文的字节数组依次拼接得到的字节数组。

[0106] 205、服务网关将加密结果返回给第一用户。

[0107] 其中,服务网关向第一用户返回加密结果后,第一用户可以对加密结果存储至数据仓库中或进行传输至其他用户。

[0108] 本发明实施例提供了一种数据处理方法,由于通过服务网关将用户发送的数据加密请求路由转发至相应的服务集群中进行加密处理,并接收服务集群返回的加密结果,在该加密过程中,由于生成密文所使用的加密算法和密钥被服务集群保存至数据库中,用户无法接触到加密密钥,因此不会存在通过数据生产方和使用方泄露密钥的风险,从而保证了更高的数据安全性,同时,由于数据加密请求中还携带有数据访问权限,由此可以为数据

访问权限最小化原则的落地提供了保障，保证了数据始终以特定的密文格式进行传输和存储，并且传输过程和存储阶段涉及的系统和人员均无法获得明文，进一步保证了数据的安全性。

[0109] 实施例二

[0110] 本发明实施例提供了一种数据处理方法，在本实施例中，该数据处理方法除了包括图2中描述的步骤之外，在步骤205之后，还包括步骤301至步骤304，为了描述简洁起见，省略了图2中描述的步骤。如图3所示，该数据处理方法还包括：

[0111] 301、服务网关接收第二用户发送的数据解密请求，数据解密请求中携带有待加密密文、服务集群标识和加密事件编号。

[0112] 本实施例中，第二用户可以是数据使用方，第二用户通过第二客户端向服务网关提交数据加密请求。

[0113] 302、服务网关将数据解密请求路由到服务集群标识对应的服务集群中。

[0114] 本实施例中，服务网关可以根据服务集群标识确定对应的服务集群中，将数据解密请求路由至该对应的服务集群中。

[0115] 进一步地，在步骤302之前，本发明实施例提供的方法还可以包括：

[0116] 服务网关对第二用户进行身份认证和鉴权，若第二用户未通过身份认证或鉴权，则向第二用户返回解密请求失败信息，若第二用户通过鉴权，则将数据解密请求路由到对应的服务集群中。

[0117] 本实施例中，通过服务网关对服务调用方进行身份认证并进行鉴权，如此可以通过权限控制可以为不同的客户端提供不同的权限，为服务集群的访问及可用性等提供监控功能，且可以针对不同的客户端可以开放不同的服务集群，从而保证了访问服务集群的安全性，并实现了对调用解密服务的权限管控。

[0118] 303、服务集群从数据库中查询加密事件编号对应的数据访问权限，并在第二用户具有数据访问权限时，在多个服务实例中，调用相应的服务实例根据加密事件编号对应的加密算法和密钥对待加密密文进行解密得到明文。

[0119] 本实施例中，服务集群可以从数据库中查询加密事件编号对应的数据访问权限，并将第二用户的用户标识与数据访问权限中的授权访问用户的用户标识进行比对，若比对一致，则确定第二用户具有数据访问权限，若比对不一致，则第二用户不具有数据访问权限，当第二用户不具有数据访问权限时，服务集群则通过服务网关向第二用户返回解密请求失败信息。

[0120] 在服务集群确定第二用户具有数据访问权限后，则在均预置有加密事件编号对应的加密算法的多个服务实例中，按照负载均衡方式或随机方式从该多个服务实例中选择一个服务实例，以使该服务实例根据加密算法和密钥对密文进行解密得到明文。

[0121] 在具体实施过程中，可以对均预置有加密事件编号对应的加密算法的多个服务实例的负载状态进行实时监控，并根据监控结果，按照负载均衡方式从该多个服务实例中选择当前负载最小的一个服务实例进行解密服务。

[0122] 其中，服务实例的负载状态可以包括CPU使用率、内存使用率、磁盘读写、网络连接状态中的一种或多种。

[0123] 304、服务集群将包含明文在内的解密结果返回给服务网关，以使服务网关将解密

结果返回给第二用户。

[0124] 本发明实施例提供了一种数据处理方法，由于通过服务网关将用户发送的数据解密请求路由转发至相应的服务集群中进行解密处理，在数据解密过程中，首先判断作为数据使用方的用户是否具有数据访问权限，当具有数据访问权限，才进行数据解密服务，由此可以避免数据使用方接触用于解密密文的密钥而产生数据使用方可能泄露密钥的风险，从而使得数据的安全性更高；另外，也实现了对密文的数据访问权限进行管控，避免了数据库中的加密算法和密钥被不适当的用户调用服务集群中的解密服务而解密得到明文，从而进一步确保了数据的安全性。

[0125] 实施例三

[0126] 本发明实施例提供了一种数据处理系统，如图4所示，该数据处理系统可以包括服务网关41和服务集群42，服务集群42包括多个服务实例，且服务集群42中部署有数据库，其中：

[0127] 服务网关41，用于接收第一用户发送的数据加密请求，并将数据加密请求路由到服务集群中，数据加密请求携带有待加密数据和数据访问权限；

[0128] 服务集群42，用于在多个服务实例中，调用相应的服务实例对待加密数据进行加密生成密文，并产生加密事件；

[0129] 服务集群42，还用于将数据访问权限、加密事件的事件编号、加密待加密数据所使用的加密算法和密钥对应存储至数据库中；以及

[0130] 将包含密文、服务集群的标识和事件编号在内的加密结果返回给服务网关；

[0131] 服务网关41，还用于将加密结果返回给第一用户。

[0132] 进一步地，若服务集群的数量为多个时，服务网关41具体用于：

[0133] 根据预设的映射关系表，在多个服务集群中确定与第一用户具有映射关系的服务集群；

[0134] 将数据加密请求路由至与第一用户具有映射关系的一个服务集群中。

[0135] 进一步地，多个服务集群42包括对称加密服务集群、Hash算法服务集群、不对称加密服务集群和业务定制加密服务集群中的至少两个。

[0136] 进一步地，密钥是从密钥池中随机抽取到的，服务集群42具体还用于：

[0137] 根据预设的密钥更换条件，更换密钥池中的密钥。

[0138] 进一步地，密钥更换条件为如下条件之一：

[0139] 密钥池中的密钥的使用次数达到使用次数阈值；或者

[0140] 密钥池中的密钥的存在时间达到时间阈值。

[0141] 进一步地，服务网关41，还用于接收第二用户发送的数据解密请求，数据解密请求中携带有待加密密文、服务集群标识和加密事件编号；

[0142] 服务网关41，还用于将数据解密请求路由到服务集群标识对应的服务集群中；

[0143] 服务集群42，还用于从数据库中查询加密事件编号对应的数据访问权限，并在第二用户具有数据访问权限时，在多个服务实例中，调用相应的服务实例根据加密事件编号对应的加密算法和密钥对待加密密文进行解密得到明文；

[0144] 服务集群42，还用于将包含明文在内的解密结果返回给服务网关；

[0145] 服务网关41，还用于将解密结果返回给第二用户。

[0146] 进一步地，服务集群42具体还用于：

[0147] 按照负载均衡方式或随机方式从多个服务实例中选择出相应的服务实例。

[0148] 本实施例提供的数据处理系统，与本发明实施例所提供的数据处理方法属于同一发明构思，可执行本发明实施例所提供的数据处理方法，具备执行数据处理方法相应的功能模块和有益效果。未在本实施例中详尽描述的技术细节，可参见本发明实施例提供的数据处理方法，此处不再加以赘述。

[0149] 上述所有可选技术方案，可以采用任意结合形成本发明的可选实施例，在此不再一一赘述。

[0150] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0151] 以上仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

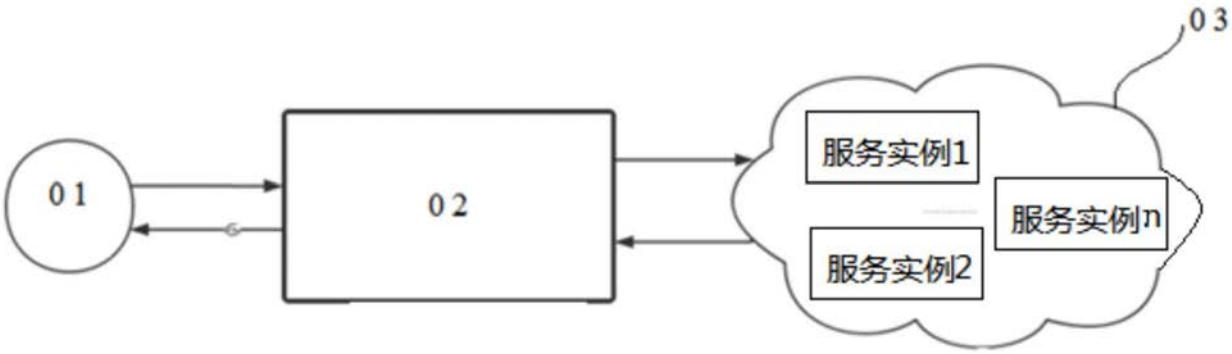

03
01
02
服务实例1
服务实例n
服务实例2

图1

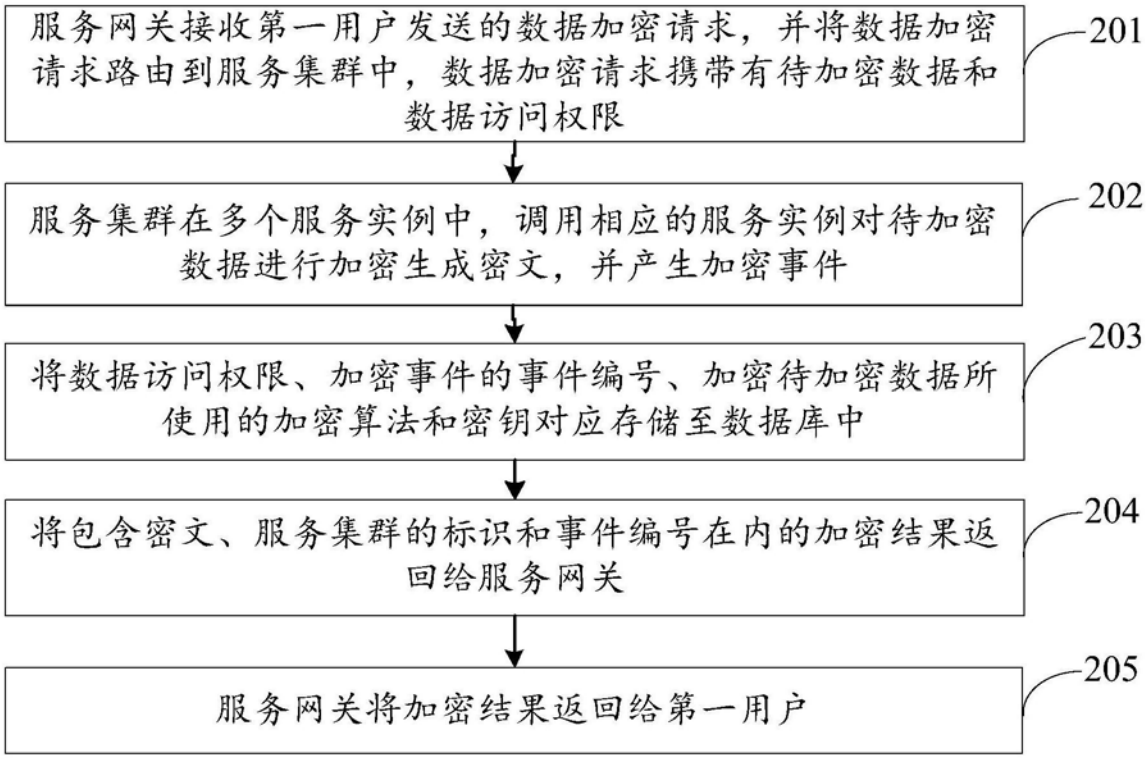

服务网关接收第一用户发送的数据加密请求，并将数据加密请求路由到服务集群中，数据加密请求携带有待加密数据和数据访问权限
201
服务集群在多个服务实例中，调用相应的服务实例对待加密数据进行加密生成密文，并产生加密事件
202
将数据访问权限、加密事件的事件编号、加密待加密数据所使用的加密算法和密钥对应存储至数据库中
203
将包含密文、服务集群的标识和事件编号在内的加密结果返回给服务网关
204
服务网关将加密结果返回给第一用户
205

图2

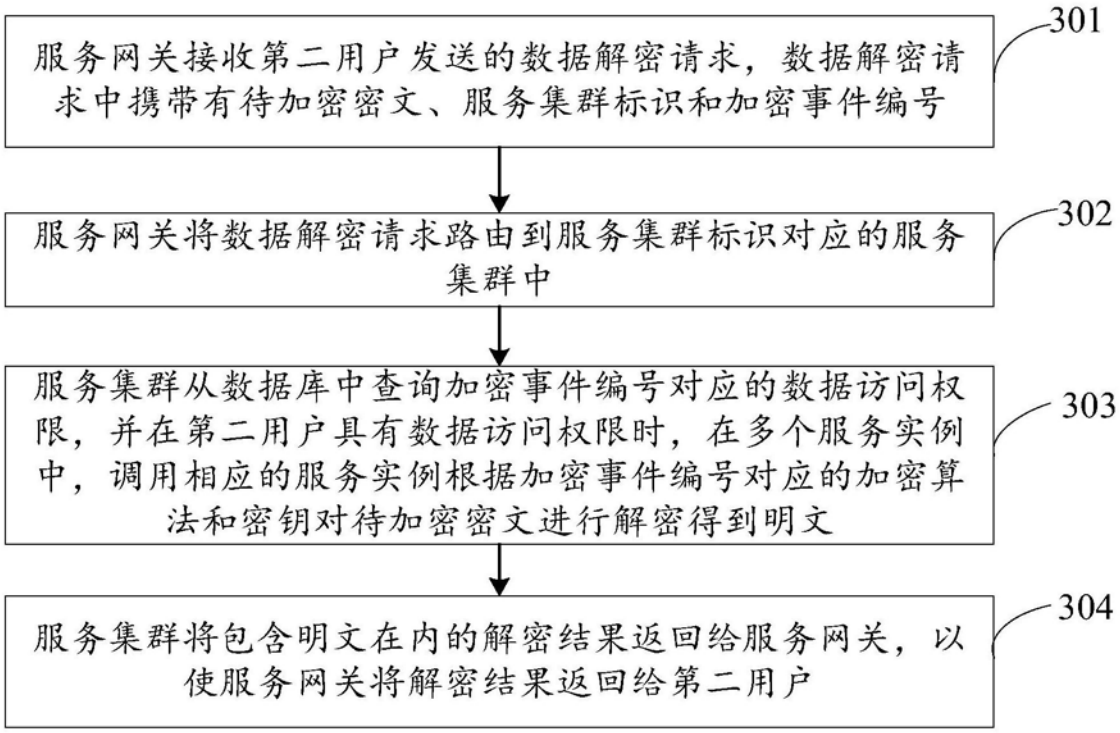

服务网关接收第二用户发送的数据解密请求，数据解密请求中携带有待加密密文、服务集群标识和加密事件编号
301
服务网关将数据解密请求路由到服务集群标识对应的服务集群中
302
服务集群从数据库中查询加密事件编号对应的数据访问权限，并在第二用户具有数据访问权限时，在多个服务实例中，调用相应的服务实例根据加密事件编号对应的加密算法和密钥对待加密密文进行解密得到明文
303
服务集群将包含明文在内的解密结果返回给服务网关，以使服务网关将解密结果返回给第二用户
304

图3

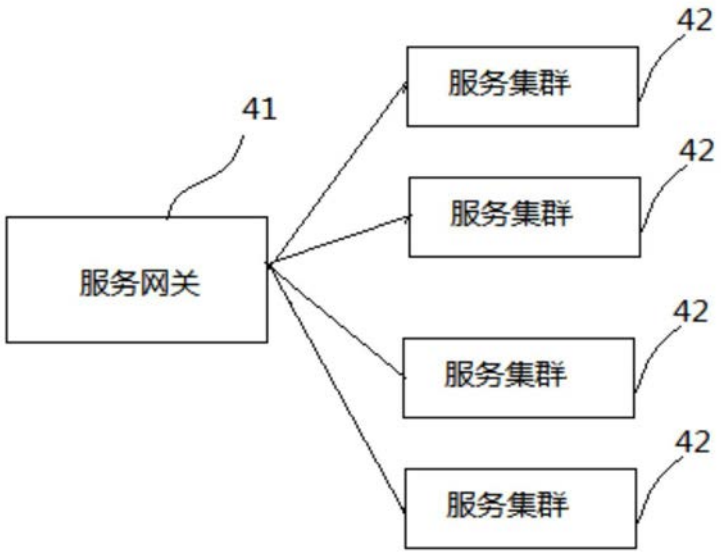

41
服务网关
42
服务集群
42
服务集群
42
服务集群
42
服务集群

图4