一种数据共享系统、方法、装置、设备及介质

相关申请的交叉引用

本申请要求在2022年09月19日提交中国专利局、申请号为202211147485.8、申请名称为“一种数据共享系统、方法、装置、设备及介质”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。

技术领域

本申请涉及数据共享技术领域，尤其涉及一种数据共享系统、方法、装置、设备及介质。

背景技术

传统数据保护主要侧重于在数据传输和写入存储介质时对其进行加密保护。当前针对应用的数据在计算状态（也即使用状态）下的安全保障能力不足，导致数据安全链条缺失最重要一环，因此，保障应用的数据在计算状态下的安全十分必要。

然而，即便可以保障每个应用在计算状态下的数据的安全，由于在实际应用场景中，通常存在多个应用之间需要共享数据的情况，在保障每个应用在计算状态下的数据的安全的前提下，如何实现多个应用之间可以共享数据，也是目前亟需解决的一个技术问题。

发明内容

本申请提供了一种数据共享系统、方法、装置、设备及介质，用于在保障每个应用的数据的安全的前提下，实现多个应用之间可以共享数据。

第一方面，本申请提供了一种数据共享系统，所述系统包括：

第一应用所属的设备，用于根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向所述目标访问

地址发送共享所述第二应用的数据的共享请求，所述共享请求中携带所述目标应用标识；

所述目标访问地址所属的设备，用于接收所述共享请求，根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥；基于所述目标加密密钥，对获取的数据进行解密；将解密后的数据发送给所述第一应用所属的设备；

所述目标数据库，用于存储数据。

第二方面，本申请提供了一种数据共享方法，所述方法应用于第一应用所属的设备，所述方法包括：

根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向所述目标访问地址发送共享所述第二应用的数据的共享请求，所述共享请求中携带所述目标应用标识；

接收所述目标访问地址所属的设备发送的解密后的所述第二应用的数据。

第三方面，本申请提供了一种数据共享方法，所述方法应用于目标访问地址所属的设备，所述方法包括：

接收第一应用所属的设备发送的共享请求，所述共享请求中携带所述目标应用标识；

根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据；

根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥；基于所述目标加密密钥，对获取的数据进行解密；将解密后的数据发送给所述第一应用所属的设备。

第四方面，本申请提供了一种数据共享方法，所述方法应用于第二应用所属的设备，所述方法包括：

若接收到管理平台发送的申请，展示所述申请中携带的第一应用的应用标识；

若接收到同意所述第一应用共享数据的确认指令，将所述确认指令发送给所述管理平台。

第五方面，本申请提供了一种数据共享方法，所述方法应用于管理平台，所述方法包括：

接收第一应用所属的设备发送的共享所述第二应用的数据的申请，所述申请中携带所述第一应用的应用标识；

将所述申请发送给所述第二应用所属的设备；

若接收到所述第二应用所属的设备发送的同意所述第一应用共享数据的确认指令，将保存的所述第二应用的目标应用标识及所述目标应用标识信息对应的目标访问地址发送给所述第一应用所属的设备。

第六方面，本申请提供了一种数据共享装置，所述装置包括：

第一确定模块，用于根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向所述目标访问地址发送共享所述第二应用的数据的共享请求，所述共享请求中携带所述目标应用标识；

第一接收模块，用于接收所述目标访问地址所属的设备发送的解密后的所述第二应用的数据。

第七方面，本申请提供了一种数据共享装置，所述装置包括：

第二接收模块，用于接收第一应用所属的设备发送的共享请求，所述共享请求中携带所述目标应用标识；

第二确定模块，用于根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据；

加解密模块，用于根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥；基于所述目标加密密钥，对获取的数据进行解密；将解密后的数据发送给所述第一应用所属的设备。

第八方面，本申请提供了一种数据共享装置，所述装置包括：

展示模块，用于若接收到管理平台发送的申请，展示所述申请中携带的

第一应用的应用标识;

第一发送模块，用于若接收到同意所述第一应用共享数据的确认指令，将所述确认指令发送给所述管理平台。

第九方面，本申请提供了一种数据共享装置，所述装置包括:

第三接收模块，用于接收第一应用所属的设备发送的共享所述第二应用的数据的申请，所述申请中携带所述第一应用的应用标识;

第二发送模块，用于将所述申请发送给所述第二应用所属的设备；若接收到所述第二应用所属的设备发送的同意所述第一应用共享数据的确认指令，将保存的所述第二应用的目标应用标识及所述目标应用标识信息对应的目标访问地址发送给所述第一应用所属的设备。

第十方面，本申请提供了一种电子设备，其包括处理器和存储器，其中，所述存储器存储有程序代码，当所述程序代码被所述处理器执行时，使得所述处理器执行上述第二方面-第五方面任一项所述方法的步骤。

第十一方面，本申请提供了一种计算机可读存储介质，其包括程序代码，当所述存储介质在电子设备上运行时，所述程序代码用于使所述电子设备执行上述第二方面-第五方面任一项所述方法的步骤。

由于本申请实施例中，第一应用所属的设备可以根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向目标访问地址发送共享第二应用的数据的共享请求，该共享请求中携带所述目标应用标识；目标访问地址所属的设备可以接收该共享请求，根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库；获取目标数据库中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥；基于目标加密密钥对获取的数据进行解密；将解密后的数据发送给第一应用所属的设备；基于此，可以在保障每个应用的数据的安全的前提下，实现多个应用之间可以共享数据的目的。

附图说明

为了更清楚地说明本申请实施例或相关技术中的实施方式，下面将对实施例或相关技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

图 1 示出了一些实施例提供的一种数据共享系统示意图；

图 2 示出了一些实施例提供的第一种数据共享过程示意图；

图 3 示出了一些实施例提供的第二种数据共享过程示意图；

图 4 示出了一些实施例提供的第三种数据共享过程示意图；

图 5 示出了一些实施例提供的第四种数据共享过程示意图；

图 6 示出了一些实施例提供的第五种数据共享过程示意图；

图 7 示出了一些实施例提供的一种写入数据过程示意图；

图 8 示出了一些实施例提供的一种读取数据过程示意图；

图 9 示出了一些实施例提供的一种数据安全存储过程示意图；

图 10 为本申请一些实施例提供的一种数据共享场景示意图；

图 11 示出了一些实施例提供的第六种数据共享过程示意图；

图 12 示出了一些实施例提供的第七种数据共享过程示意图；

图 13 示出了一些实施例提供的第八种数据共享过程示意图；

图 14 示出了一些实施例提供的第九种数据共享过程示意图；

图 15 示出了一些实施例提供的第一种数据共享装置示意图；

图 16 示出了一些实施例提供的第二种数据共享装置示意图；

图 17 示出了一些实施例提供的第三种数据共享装置示意图；

图 18 示出了一些实施例提供的第四种数据共享装置示意图；

图 19 示出了一些实施例提供的一种电子设备结构示意图。

具体实施方式

为了在保障每个应用的数据的安全的前提下，实现多个应用之间可以共

享数据，本申请提供了一种数据共享系统、方法、装置、设备及介质。

为使本申请的目的和实施方式更加清楚，下面将结合本申请示例性实施例中的附图，对本申请示例性实施方式进行清楚、完整地描述，显然，描述的示例性实施例仅是本申请一部分实施例，而不是全部的实施例。

需要说明的是，本申请中对于术语的简要说明，仅是为了方便理解接下来描述的实施方式，而不是意图限定本申请的实施方式。除非另有说明，这些术语应当按照其普通和通常的含义理解。

本申请中说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”等是用于区别类似或同类的对象或实体，而不必然意味着限定特定的顺序或先后次序，除非另外注明。应该理解这样使用的用语在适当情况下可以互换。

术语“包括”和“具有”以及他们的任何变形，意图在于覆盖但不排他的包含，例如，包含了一系列组件的产品或设备不必限于清楚地列出的所有组件，而是可包括没有清楚地列出的或对于这些产品或设备固有的其它组件。

术语“模块”是指任何已知或后来开发的硬件、软件、固件、人工智能、模糊逻辑或硬件或/和软件代码的组合，能够执行与该元件相关的功能。

最后应说明的是：以上各实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述各实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的范围。

图 1 示出了一些实施例提供的一种数据共享系统示意图，如图 1 所示，该系统包括：

第一应用所属的设备 11，用于根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向所述目标访问地址发送共享所述第二应用的数据的共享请求，所述共享请求中携带所述目标应用标识；

所述目标访问地址所属的设备 12，用于接收所述共享请求，根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库 13；获取所述目标数据库 13 中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥；基于所述目标加密密钥，对获取的数据进行解密；将解密后的数据发送给所述第一应用所属的设备 11；

所述目标数据库 13，用于存储数据。

在一种可能的实施方式中，数据共享系统中包括第一应用所属的设备 11、目标访问地址所属的设备 12、目标数据库 13。第一应用（如应用 B）所属的设备在需要获取（共享）第二应用（如应用 A）的数据时，可以根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，并向目标访问地址发送共享第二应用的数据的共享请求。可选的，共享请求中可以携带第二应用的目标应用标识。

目标访问地址所属的设备 12（也可称为前置加密模块）可以接收该共享请求，并可以根据预先保存的应用标识与数据库的对应关系，确定第二应用的目标应用标识对应的目标数据库 13，进而获得目标数据库 13 中保存的数据。在一种可能的实施方式中，为了保障每个应用的数据的安全，针对每个应用，该应用对应的数据库中保存的数据可以为基于该应用对应的加密密钥进行加密后的数据，也就是说，从目标数据库 13 中获取到数据可以为基于第二应用（如应用 A）的加密密钥加密后的数据。为了实现不同应用之间的数据共享，可以将解密后的数据发送给第一应用（如应用 B），具体的，目标访问地址所属的设备 12 可以预先保存每个应用标识与加密密钥的对应关系，在从目标数据库 13 中获取到数据之后，目标访问地址所属的设备 12 可以根据保存的应用标识与加密密钥的对应关系，确定第二应用（如应用 A）的目标应用标识对应的目标加密密钥，并基于该目标加密密钥对获取的数据进行解密，将解密后的数据发送给第一应用所属的设备 11，从而在保障每个应用的数据的安全的前提下，可以实现多个应用之间可以共享数据。

在一种可能的实施方式中，第一应用（如应用 B）如果想要共享第二应用（如应用 A）的数据，第一应用（如应用 B）所属的设备 11 可以先向数据共享系统中的管理平台发送共享第二应用的数据的申请，可选的，该申请中可以携带第一应用自身的应用标识。管理平台接收到第一应用（如应用 B）所属的设备发送的该申请后，可以将该申请发送给第二应用（如应用 A）所属的设备。第二应用（如应用 A）所属的设备可以接收管理平台发送的该申请，为了使第二应用的管理人员等可以对是否允许第一应用共享数据进行审批，第二应用（如应用 A）所属的设备可以展示该申请中携带的第一应用的应用标识。可选的，如果第二应用的管理人员等对该申请审批通过，同意第一应用共享第二应用的数据，可以点击审批通过按钮等，第二应用所属的设备可以接收到同意第一应用共享数据的确认指令，并可以在接收到该确认指令时，将该确认指令发送给管理平台。

管理平台可以接收第二应用所属的设备发送的确认指令，并可以在接收到确认指令时，将保存的第二应用的目标应用标识及目标应用标识对应的目标访问地址发送给第一应用所属的设备 11。可选的，若第二应用的目标应用标识包括主标识信息和副标识信息，管理平台可以将其中的副标识信息发送给第一应用（如应用 B）所属的设备，第一应用所属的设备 11 保存第二应用的副标识信息与目标访问地址的对应关系，关于第二应用的主标识信息和副标识信息在后续实施例中进行介绍，在此先不赘述。

在一种可能的实施方式中，第一应用所属的设备 11 可以接收管理平台发送的第二应用的目标应用标识及目标应用标识对应的目标访问地址，并可以保存该目标应用标识与目标访问地址的对应关系。示例性的，可以将该对应关系保存在第一应用所属的设备 11 的配置文件（数据库配置文件）中等。

为方便理解，下面通过一个具体实施例对本申请提供的数据共享过程进行说明。图 2 示出了一些实施例提供的第一种数据共享过程示意图，该过程包括以下步骤：

S201：第一应用所属的设备 11 向管理平台发送共享第二应用的数据的申

请，该申请中携带第一应用自身的应用标识。

S202：管理平台接收申请，并将该申请发送给第二应用所属的设备。

S203：第二应用所属的设备接收该申请并展示该申请中携带的第一应用的应用标识，若接收到同意第一应用共享数据的确认指令，将确认指令发送给管理平台。

S204：管理平台接收确认指令，将保存的第二应用的目标应用标识（如副标识信息）及目标应用标识对应的目标访问地址发送给第一应用所属的设备 11。

S205：第一应用所属的设备 11 保存目标应用标识与目标访问地址的对应关系。

S206：第一应用所属的设备 11 根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向目标访问地址发送共享第二应用的数据的共享请求，共享请求中携带该目标应用标识。

S207：目标访问地址所属的设备 12 接收共享请求，根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库 13；获取目标数据库 13 中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥；基于该目标加密密钥对获取的数据进行解密；将解密后的数据发送给第一应用所属的设备 11。

在一种可能的实施方式中，考虑到第一应用在共享第二应用的数据时，通常需要为第一应用配置设定的使用权限，例如第一应用只能读取第二应用的数据，而并不能在第二应用的数据库中写入数据，或者第二应用涉及的敏感数据需要先进行数据脱敏处理再发送给第一应用等，从而在使得不同应用之间可以共享数据的同时，还可以增加各应用的数据的安全性，目标访问地址所属的设备 12 在接收第一应用所属的设备 11 发送的上述共享请求之后，在根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库 13 之前，还可以判断共享请求的类型为读取数据请求还是写入数据请求，并基于该共享请求的类型以及预先保存的第一应用对第二应用的数据的

使用权限，判断该共享请求是否符合相应的使用权限。例如，如果第一应用对第二应用的使用权限为只能读取数据而不能写入数据，则只有在共享数据的类型为读取数据请求时，判断该共享请求符合相应的使用权限，再进行后续根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库 13；获取目标数据库 13 中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥；基于目标加密密钥对获取的数据进行解密；将解密后的数据发送给第一应用所属的设备 11 的步骤。

在一种可能的实施方式中，考虑到如果从目标数据库 13 中获取到的数据包含设定的如身份证号等敏感数据时，为了增加数据的安全性，在基于目标加密密钥对获取的数据进行解密之后，将解密后的数据发送给第一应用所属的设备 11 之前，目标访问地址所属的设备 12 还可以对解密后的数据进行数据脱敏处理，并将经过数据脱敏处理后的数据发送给第一应用所属的设备 11。其中，可以采用现有技术对数据进行数据脱敏处理，在此不再赘述。

为方便理解，下面通过一个具体实施例对本申请提供的数据共享过程进行说明。图 3 示出了一些实施例提供的第二种数据共享过程示意图，该过程包括以下步骤：

S301：第一应用所属的设备 11 根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向目标访问地址发送共享第二应用的数据的共享请求，共享请求中携带该目标应用标识。

S302：目标访问地址所属的设备 12 接收共享请求，若判断该共享请求的类型为读取数据请求且该共享请求符合使用权限，则根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库 13；获取目标数据库 13 中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥；基于该目标加密密钥对获取的数据进行解密。

S303：若获取的数据包含设定的敏感数据，目标访问地址所属的设备 12 对解密后的数据进行数据脱敏处理，并将经过数据脱敏处理后的数据发送给

第一应用所属的设备 11。

在一种可能的实施方式中，若第二应用的目标应用标识包括主标识信息和副标识信息，目标访问地址所属的设备 12 还可以判断共享请求中携带的目标应用标识是否为第二应用的副标识信息，若共享请求中携带的目标应用标识为第二应用的副标识信息，可以认为此时需要将某应用的数据共享给其他应用，为了保证数据的安全性，可以继而进行上述实施例中判断共享请求的类型为读取数据请求还是写入数据请求，基于该共享请求的类型以及预先保存的第一应用对第二应用的数据的使用权限，判断该共享请求是否符合使用权限，若符合使用权限，则再进行根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库 13 等后续步骤。

为方便理解，下面通过一个具体实施例对本申请提供的数据共享过程进行说明。图 4 示出了一些实施例提供的第三种数据共享过程示意图，该过程包括以下步骤：

S401：第一应用所属的设备 11 根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向目标访问地址发送共享第二应用的数据的共享请求，共享请求中携带该目标应用标识。

S402：目标访问地址所属的设备 12 接收共享请求，若第二应用的目标应用标识包括主标识信息和副标识信息，判断该共享请求中携带的目标应用标识是否为第二应用的副标识信息，若是，则进行 S403。

S403：若判断共享请求的类型为读取数据请求且该共享请求符合使用权限，则根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库 13；获取目标数据库 13 中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥；基于该目标加密密钥对获取的数据进行解密。

S404：若获取的数据包含设定的敏感数据，目标访问地址所属的设备 12 对解密后的数据进行数据脱敏处理，并将经过数据脱敏处理后的数据发送给第一应用所属的设备 11。

实施例 2:

考虑到传统数据保护主要侧重于在数据传输和写入存储介质时对其进行加密保护。当前针对应用的数据在计算状态（也即使用状态）下的安全保障能力不足，导致数据安全链条缺失最重要一环，因此，保障应用的数据在计算状态下的安全十分必要，然而目前尚没有很好的如何保障应用的数据在计算状态下的安全的技术方案。本申请实施例提供了一种可以保障应用的数据在计算状态下的安全性的技术方案，为方便理解，下面以保障上述实施例中的第二应用（如应用 A）的数据的安全性为例进行举例说明。

在一种可能的实施方式中，上述数据共享系统中还可以包括：管理平台和第二应用（如应用 A）所属的设备。为了保障数据的安全性，第二应用所属的设备可以先向管理平台发送一个数据存储安全保护请求，该数据存储安全保护请求中可以携带第二应用的名称及第二应用的目标访问地址。管理平台可以接收第二应用所属的设备发送的数据存储安全保护请求，并生成第二应用的名称对应的目标应用标识以及目标加密密钥，保存该目标应用标识与目标加密密钥的对应关系。可选的，管理平台生成的第二应用的名称对应的目标应用标识可以包括上述实施例中提及的主标识信息以及副标识信息，可以理解的，该主标识信息以及副标识信息可以对应同一个目标加密密钥。

在一种可能的实施方式中，目标访问地址所属的设备 12 可以向管理平台发送获取第二应用对应的目标加密密钥的获取密钥请求。管理平台接收到该获取密钥请求后，可以根据保存的应用标识与加密密钥的对应关系，确定第二应用的目标应用标识对应的目标加密密钥，将目标加密密钥发送给目标访问地址所属的设备12。目标访问地址所属的设备12可以接收该目标加密密钥，并保存该目标加密密钥与目标应用标识的对应关系。

为方便理解，下面通过一个具体实施例对本申请提供的数据共享过程进行说明。图 5 示出了一些实施例提供的第四种数据共享过程示意图，该过程包括以下步骤:

S501: 第二应用（如应用 A）所属的设备向管理平台发送一个数据存储

安全保护请求，该数据存储安全保护请求中携带第二应用的名称及第二应用的目标访问地址。

S502：管理平台接收第二应用所属的设备发送的数据存储安全保护请求，生成第二应用的名称对应的目标应用标识以及目标加密密钥，保存该目标应用标识与目标加密密钥的对应关系。

S503：目标访问地址所属的设备 12 向管理平台发送获取第二应用对应的目标加密密钥的获取密钥请求。管理平台接收到该获取密钥请求后，根据保存的应用标识与加密密钥的对应关系，确定第二应用的目标应用标识对应的目标加密密钥，将目标加密密钥发送给目标访问地址所属的设备 12。目标访问地址所属的设备 12 接收该目标加密密钥，并保存该目标加密密钥与目标应用标识的对应关系。

S504：第一应用（如应用 B）所属的设备向管理平台发送共享第二应用的数据的申请，该申请中携带第一应用自身的应用标识。

S505：管理平台接收申请，并将该申请发送给第二应用所属的设备。第二应用所属的设备接收该申请并展示该申请中携带的第一应用的应用标识，若接收到同意第一应用共享数据的确认指令，将确认指令发送给管理平台。管理平台接收确认指令，将保存的第二应用的目标应用标识（如副标识信息）及目标应用标识对应的目标访问地址发送给第一应用所属的设备 11。

S506：第一应用所属的设备 11 保存目标应用标识与目标访问地址的对应关系。第一应用所属的设备 11 根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向目标访问地址发送共享第二应用的数据的共享请求，共享请求中携带该目标应用标识。

S507：目标访问地址所属的设备 12 接收共享请求，根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库 13；获取目标数据库 13 中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥；基于该目标加密密钥对获取的数据进行解密；将解密后的数据发送给第一应用所属的设备 11。

在一种可能的实施方式中，为了提高加密密钥的安全性，管理平台中保存的加密密钥可以是保存在管理平台的可信执行环境（Trusted Execution Environment，TEE）中的。以第二应用的目标加密密钥为例，管理平台中保存的目标加密密钥可以是保存在管理平台的可信执行环境（Trusted Execution Environment，TEE）中的。另外，目标访问地址所属的设备 12 中保存的加密密钥也可以是保存在目标访问地址所属的设备 12 的 TEE 中的。以第二应用的目标加密密钥为例，目标加密密钥也可以是保存在目标访问地址所属的设备 12 的 TEE 中的。

在一种可能的实施方式中，为了进一步提高对保存的加密密钥的安全性，管理平台还可以基于设定的 TEE 物理存储根密钥(为方便描述，称为第一 TEE 物理存储根密钥)将各应用的加密密钥进行加密后，在保存在自身的 TEE 中，也就是说，管理平台中保存的加密密钥可以为基于设定的第一 TEE 物理存储根密钥加密后的密钥。可选的，管理平台在将目标加密密钥发送给目标访问地址所属的设备 12 时，如果管理平台中保存的目标加密密钥为基于设定的第一 TEE 物理存储根密钥加密后的密钥，管理平台可以基于设定的第一 TEE 物理存储根密钥对目标加密密钥进行解密，将解密后的目标加密密钥，发送给目标访问地址所属的设备 12。

在一种可能的实施方式中，为了增加目标加密密钥的安全性，管理平台在将目标加密密钥发送给目标访问地址所属的设备 12 时，可以基于临时建立的安全通道，将目标加密密钥发送给目标访问地址所属的设备 12。在一种可能的实施方式中，在基于临时建立的安全通道，将目标加密密钥发送给目标访问地址所属的设备 12 时，为了进一步增加目标加密密钥的安全性，管理平台与目标访问地址所属的设备 12 可以协商一个临时安全通道密钥，管理平台可以基于该临时安全通道密钥，对目标加密密钥进行加密，并基于临时建立的安全通道，将加密后的目标加密密钥发送给目标访问地址所属的设备 12。目标访问地址所属的设备 12 接收到基于临时安全通道密钥加密后的目标加密密钥时，可以基于相应的临时安全通道密钥，对目标加密密钥进行解密，得

到解密后的目标加密密钥。在一种可能的实施方式中，目标访问地址所属的设备12还可以基于设定的第二TEE物理存储根密钥对目标加密密钥进行加密，然后保存加密后的目标加密密钥。

为方便理解，下面通过一个具体实施例对本申请提供的数据共享过程进行说明。图 6 示出了一些实施例提供的第五种数据共享过程示意图，该过程包括以下步骤:

S601: 第二应用所属的设备向管理平台发送数据存储安全保护请求，该数据存储安全保护请求中携带第二应用的名称及第二应用的目标访问地址。

S602: 管理平台接收第二应用所属的设备发送的数据存储安全保护请求，生成第二应用的名称对应的目标应用标识以及目标加密密钥，基于设定的第一 TEE 物理存储根密钥对该目标加密密钥进行加密，将加密后的目标加密密钥保存在管理平台的可信执行环境（TEE）中，并保存目标应用标识与目标加密密钥的对应关系。

由于是在 TEE 中生成保存目标加密密钥，且基于第一 TEE 物理存储根密钥对目标加密密钥进行加密后在保存，可以保证加密密钥的明文不出 TEE，可以保证 TEE 的安全性。

S603: 目标访问地址所属的设备 12 向管理平台发送获取第二应用对应的目标加密密钥的获取密钥请求。管理平台接收目标访问地址所属的设备 12 发送的获取密钥请求，根据保存的应用标识与加密密钥的对应关系，确定第二应用的目标应用标识对应的目标加密密钥。管理平台基于第一 TEE 物理存储根密钥对目标加密密钥进行解密，并基于与目标访问地址所属的设备 12 协商的临时安全通道密钥，对目标加密密钥进行加密，基于临时建立的安全通道，将加密后的目标加密密钥发送给目标访问地址所属的设备 12。

相较于相关技术中将加密密钥的明文出现在加密机外的应用内存中，而且加密密钥传输过程中的安全性无法保证而言，本申请不仅可以在 TEE 中生成保存目标加密密钥，基于第一 TEE 物理存储根密钥对目标加密密钥进行加密后在保存，保证加密密钥的明文不出 TEE，保证 TEE 的安全性。另外，本

申请还可以基于安全通道将目标加密密钥发送给目标访问地址所属的设备 12，可以保障目标加密密钥在传输过程中的安全性。另外，本申请基于安全通道发送该目标加密密钥时，还可以基于临时安全通道密钥对目标加密密钥加密后再发送，可以进一步保障目标加密密钥的明文在传输过程中不被泄露，进一步保障目标加密密钥在传输过程中的安全性。

S604：目标访问地址所属的设备 12 接收基于临时安全通道密钥加密后的目标加密密钥，基于临时安全通道密钥，对目标加密密钥进行解密，并基于设定的第二 TEE 物理存储根密钥对目标加密密钥进行加密，将加密后的目标加密密钥保存在目标访问地址所属的设备 12 的 TEE 中，并保存目标加密密钥与目标应用标识的对应关系。

由于目标访问地址所属的设备 12 可以将目标加密密钥保存在 TEE 中，且基于第二 TEE 物理存储根密钥对目标加密密钥进行加密后在保存，可以保证加密密钥的明文不出 TEE，可以保证 TEE 的安全性。

本申请实施例中加密密钥从生成、传输、存储等全生命周期均在 TEE 及加密状态下进行，加密密钥的明文不出 TEE，可以保证加密密钥的安全性。

在一种可能的实施方式中，管理平台在接收到第二应用所属的设备发送的数据存储安全保护请求，生成第二应用的名称对应的目标应用标识之后，可以将该目标应用标识发送给第二应用所属的设备，示例性的，可以将目标应用标识中的主标识信息发送给第二应用所属的设备。

在一种可能的实施方式中，在第二应用需要将数据写入对应的数据库（目标数据库 13）中时，第二应用所属的设备可以向目标访问地址发送写入数据请求，该写入数据请求中携带待写入数据库中的数据以及第二应用的目标应用标识（如主标识信息）。目标访问地址所属的设备 12 可以接收该写入数据请求，并根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥，基于目标加密密钥，对待写入数据库中的数据进行加密，将加密后的数据保存到对应的目标数据库 13 中。

在一种可能的实施方式中，为了实现对待写入数据库中的数据的精细加

密，增加加密的灵活性，第二应用的管理人员等还可以设置相应的加密策略，例如需要加密的字段、采用的加密算法、加密规则等，其中加密策略可以根据需求灵活设置，本申请对此不作具体限定，第二应用所属的设备向管理平台发送的数据存储安全保护请求中可以携带该加密策略。可选的，目标访问地址所属的设备 12 可以向管理平台发送获取第二应用的加密策略请求，该加密策略请求中可以携带第二应用对应的目标应用标识。若数据存储安全保护请求中携带对数据的加密策略，管理平台可以将该加密策略发送给目标访问地址所属的设备 12。目标访问地址所属的设备 12 接收管理平台发送的加密策略，保存目标应用标识与加密策略的对应关系。若接收到第二应用所属的设备发送的写入数据请求，目标访问地址所属的设备 12 可以根据保存的应用标识与加密策略的对应关系，确定目标应用标识对应的目标加密策略，并基于目标加密密钥以及目标加密策略，对待写入数据库中的数据进行加密。

示例性的，图 7 示出了一些实施例提供的一种写入数据过程示意图，如图 7 所示，第二应用所属的设备（为方面描述，图中称为应用程序）向目标访问地址（图中称为前置加密模块）发送写入数据请求，该写入数据请求中携带待写入数据库中的数据以及第二应用的目标应用标识。

可选的，目标访问地址所属的设备 12（前置加密模块）中包括加解密模块和加密代理模块，其中，加解密模块可以部署在目标访问地址所属的设备 12 的 TEE 中，加解密模块中保存有加密密钥（目标加密密钥），后续可以在 TEE 中基于目标加密密钥对相应的数据进行加密或解密，保证数据及加密密钥的安全性。

在一种可能的实施方式中，加密代理模块可以拦截解析写入数据请求，即结构化查询语言（Structured Query Language，SQL），其中，SQL 语言是一种数据库查询和程序设计语言，可以用于存取数据等。加密代理模块可以根据保存的应用标识与加密策略的对应关系，确定第二应用的目标应用标识对应的目标加密策略。加密代理模块可以基于该目标加密策略，确定待写入数据库的数据中需要进行加密的子数据，可以将需要进行加密的子数据从待写

入数据库的数据中提取出来，将待写入数据库的数据中需要加密的子数据的明文数据和第二应用的目标应用标识发送给加解密模块。加解密模块接收到需要加密的子数据以及目标应用标识后，可以根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥，在 TEE 中，基于目标加密密钥，对需要加密的子数据进行加密，并将加密后的子数据的密文数据返回给加密代理模块。加密代理模块将加密后的子数据重新拼接到待写入数据库的数据中，也就是说写入数据库中的数据中可以有其中一部分子数据是加密后的密文数据，当然也可以是将写入数据库中的数据中全部的子数据均进行加密，可以根据需求灵活设置，本申请对此不做具体限定，加密代理模块可以将基于目标加密密钥以及目标加密策略，加密后的数据保存到对应的目标数据库 13 中。

本申请应用（如第二应用）在使用数据库安全存储服务时，只需要将数据库配置文件中的数据库访问地址（目标访问地址）修改为指向前置加密模块（目标访问地址所属的设备 12），然后就可以通过该目标访问地址直接调用现有数据库接口即可，应用（第二应用）对数据库（目标数据库 13）的访问先经过前置加密模块，前置加密模块通过拦截、解析 SQL 语句以及匹配加密策略，并在 TEE 中对数据（待写入数据库中的数据）进行加密，然后将加密后的数据（密文）发送至目标数据库 13 进行相应处理和存储。相较于相关技术中将明文发送至数据库进行相应处理而只将处理结果进行加密保存在数据库中而言，由于本申请是将加密后的数据发送至数据库进行相应处理，因此即使是数据库特权账户或运维人员等也无法在数据库层面接触到应用的明文数据，从而可以更有效保障用户隐私数据的计算和存储的安全性。

另外，本申请提供的数据共享方法对现有数据库兼容，无需改变现有数据库客户端调用接口和服务端数据库系统，即可将数据库处理数据由明文变为密文，实现密态数据库，即使是数据库特权账户或运维人员等也无法在数据库层面接触到应用的明文数据，可以方便有效地保障用户隐私数据的计算和存储的安全性。

在一种可能的实施方式中，当第二应用需要读取数据时，第二应用所属的设备可以向目标访问地址发送读取数据请求，该读取数据请求中可以携带第二应用的目标应用标识。目标访问地址所属的设备12接收该读取数据请求，并可以根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库13。目标访问地址所属的设备12可以继而获取目标数据库13中保存的数据，并根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥，基于目标加密密钥，对获取的数据进行解密，将解密后的数据发送给第二应用所属的设备。

在一种可能的实施方式中，与上述实施例相同，目标访问地址所属的设备12可以向管理平台发送获取第二应用的加密策略请求，该加密策略请求中可以携带第二应用对应的目标应用标识。若第二应用所属的设备发送的数据存储安全保护请求中携带对数据的加密策略，管理平台可以将该加密策略发送给目标访问地址所属的设备12。目标访问地址所属的设备12接收加密策略，保存目标应用标识与加密策略的对应关系。后续如果接收到第二应用所属的设备发送的上述读取数据请求，目标访问地址所属的设备12可以根据保存的应用标识与加密策略的对应关系，确定目标应用标识对应的目标加密策略，基于目标加密密钥以及目标加密策略，对从目标数据库13中获取的数据进行解密，将解密后的数据发送给第二应用所属的设备。

示例性的，图8示出了一些实施例提供的一种读取数据过程示意图，如图8所示，第二应用所属的设备（图中称为应用程序）向目标访问地址（图中称为前置加密模块）发送读取数据请求，该读取数据请求中携带第二应用的目标应用标识。可选的，目标访问地址所属的设备12（前置加密模块）中包括加解密模块和加密代理模块，其中，加密代理模块可以拦截解析读取数据请求，即SQL。

加密代理模块根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库13；获取目标数据库13中保存的数据。加密代理模块根据保存的应用标识与加密策略的对应关系，确定第二应用的目标应用标识

对应的目标加密策略。加密代理模块可以基于该目标加密策略，确定从目标数据库 13 中获取的数据中加密的子数据，可以将加密的子数据从数据中提取出来，将加密的子数据和第二应用的目标应用标识发送给加解密模块。加解密模块接收到加密的子数据以及目标应用标识后，可以根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥，基于目标加密密钥，对加密的子数据进行解密，并将解密后的子数据的明文数据返回给加密代理模块。加密代理模块将解密后的子数据重新拼接到从目标数据库 13 获取的数据中，加密代理模块可以将解密后的数据发送给第二应用所属的设备。

同样的，与上述实施例相同，目标访问地址所属的设备 12 向管理平台发送获取第二应用的加密策略请求，该加密策略请求中携带第二应用对应的目标应用标识，若第二应用所属的设备发送的数据存储安全保护请求中携带对数据的加密策略，管理平台将加密策略发送给目标访问地址所属的设备 12；目标访问地址所属的设备 12 接收该加密策略，保存目标应用标识与加密策略的对应关系之后，若目标访问地址所属的设备 12 接收到第一应用所属的设备发送的共享请求，目标访问地址所属的设备 12 可以根据保存的应用标识与加密策略的对应关系，确定目标应用标识对应的目标加密策略；基于目标加密密钥以及目标加密策略，对从目标数据库 13 获取的数据进行解密，将解密后的数据发送给第一应用所属的设备。其中，基于目标加密密钥以及目标加密策略，对从目标数据库 13 获取的数据进行解密的过程与上述实施例相同，在此不再赘述。

在一种可能的实施方式中，可以将目标访问地址所属的设备 12（前置加密模块）集成到第二应用所属的设备中，也可以将目标访问地址所属的设备 12（前置加密模块）部署到加密网关集群中。示例性的，当只针对一个应用进行安全存储服务时，可以将目标访问地址所属的设备 12（前置加密模块）集成到该应用所属的设备中。参阅图 9，图 9 示出了一些实施例提供的一种数据安全存储过程示意图，当有多个应用均需要进行数据存储安全保护服务（又

可称为安全存储服务）时，可以将目标访问地址所属的设备 12（前置加密模块）部署到加密网关集群中，也就是说第二应用的数量为多个时，针对每个第二应用所属的设备，均可以向部署在加密网关集群中的目标访问地址所属的设备 12（前置加密模块）发送写入数据请求，该写入数据请求中携带的待写入数据库中的数据为明文数据，针对每个第二应用，目标访问地址所属的设备 12（前置加密模块）可以根据保存的应用标识与加密密钥的对应关系，确定该第二应用的目标应用标识对应的目标加密密钥，基于该目标加密密钥，对该第二应用的待写入数据库中的数据进行加密，将加密后的数据（密文）保存到该第二应用对应的目标数据库 13 中。在一种可能的实施方式中，不同的应用可以对应不同的数据库，即每个应用可以分别对应一个专属的数据库。

由于针对不同的第二应用，本申请可以基于不同的加密密钥对不同的第二应用的数据进行加密，从而可以根据应用的不同做到应用间数据的自动安全隔离，增加数据的安全性。

另外，每个第二应用所属的设备均可以向部署在加密网关集群中的目标访问地址所属的设备 12（前置加密模块）发送读取数据请求，针对每个第二应用，目标访问地址所属的设备 12（前置加密模块）可以根据保存的应用标识与数据库的对应关系，确定该第二应用的目标应用标识对应的目标数据库 13；获取该目标数据库 13 中保存的该第二应用相应的数据，可以理解的，从数据库中获取到的数据为加密后的数据，即密文数据；目标访问地址所属的设备 12（前置加密模块）根据保存的应用标识与加密密钥的对应关系，确定该第二应用的目标应用标识对应的目标加密密钥，基于该目标加密密钥，对获取的数据进行解密，将解密后的数据（明文）发送给该第二应用所属的设备。

在一种可能的实施方式中，管理平台可以部署在一个单独的设备中，也可以部署在第一应用所属的设备 11 或者第二应用所属的设备中，本申请对此不作具体限定，可以根据需求灵活设置。

为方便理解，下面通过一个具体实施例对本申请提供的数据共享过程进

行举例说明。图 10 为本申请一些实施例提供的一种数据共享场景示意图，如图 10 所示，该过程可以包括:（1）第二应用（应用 A）注册授权过程、（2）目标加密密钥传输过程、（3）第二应用写入或读取数据过程、（4）第一应用（应用 B）申请共享第二应用的数据、（5）第一应用共享第二应用的数据等步骤。

其中:（1）第二应用（应用 A）注册授权过程可以包括:

第二应用所属的设备向管理平台发送数据存储安全保护请求，该数据存储安全保护请求中携带第二应用的名称及第二应用的目标访问地址。管理平台接收数据存储安全保护请求，生成第二应用的名称对应的目标应用标识以及目标加密密钥，并保存目标应用标识与目标加密密钥的对应关系。可选的，可以将生成的目标加密密钥保存在管理平台的 TEE 中。可选的，管理平台生成的目标应用标识包括主标识信息和副标识信息，其中将主标识信息发送给第二应用所属的设备，第二应用所属的设备在其数据库配置文件中保存该主标识信息与目标访问地址的对应关系，其中，目标访问地址可以为前置加密模块的地址。

（2）目标加密密钥传输过程可以包括:

目标访问地址所属的设备 12（前置加密模块）向管理平台发送获取第二应用对应的目标加密密钥的获取密钥请求。管理平台接收获取密钥请求，根据保存的应用标识与加密密钥的对应关系，确定第二应用的目标应用标识对应的目标加密密钥，将目标加密密钥通过建立的安全加密通道发送给目标访问地址所属的设备 12。目标访问地址所属的设备 12 接收目标加密密钥，将目标加密密钥保存在 TEE 中，并保存目标加密密钥与第二应用的目标应用标识的对应关系。

（3）第二应用写入或读取数据的过程如下:

其中第二应用写入数据的过程为：第二应用所属的设备向目标访问地址发送写入数据请求，写入数据请求中携带待写入数据库中的数据以及第二应用的目标应用标识（如主标识信息）。目标访问地址所属的设备 12（前置加密

模块）中的加密代理模块接收写入数据请求，识别到写入数据请求中携带的目标应用标识为第二应用的主标识信息，则可以认为该写入数据请求为第二应用想在第二应用自身对应的数据库中写入数据的合规请求，可以基于应用主逻辑（主 Schema）来进行相应的写入数据的过程，即可以将待写入数据库中的数据（明文）发送给目标访问地址所属的设备 12（前置加密模块）中的加解密模块，该加解密模块配置在 TEE 中，加密密钥保存在该加解密模块中。加解密模块根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥，基于目标加密密钥，对待写入数据库中的数据进行加密，将加密后的数据（密文）发送给加密代理模块，加密代理模块将加密后的数据保存在第二应用对应的目标数据库 13 中。

第二应用读取数据的过程为：第二应用所属的设备向目标访问地址发送读取数据请求，读取数据请求中携带第二应用的目标应用标识（如主标识信息）。目标访问地址所属的设备 12（前置加密模块）中的加密代理模块接收读取数据请求，识别到读取数据请求中携带的目标应用标识为第二应用的主标识信息，则可以认为该读取数据请求为第二应用想读取第二应用自身对应的数据库中数据的合规请求，可以基于应用主逻辑（主 Schema）来进行相应的读取数据的过程，即可以根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库 13；获取目标数据库 13 中保存的数据。加密代理模块将获取的数据（密文）发送给加解密模块，加解密模块根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥，基于目标加密密钥，对获取的数据进行解密，将解密后的数据发送给加密代理模块，加密代理模块将解密后的数据发送给第二应用所属的设备。

（4）第一应用（应用 B）申请共享第二应用的数据的过程可以包括：

第一应用（应用 B）所属的设备向管理平台发送共享第二应用（应用 A）的数据的申请，该申请中携带第一应用的应用标识。管理平台接收该申请，并将申请发送给第二应用所属的设备。第二应用所属的设备接收申请并展示申请中携带的第一应用的应用标识，若接收到同意第一应用共享数据的确认

指令，将确认指令发送给管理平台。管理平台接收确认指令，将保存的第二应用的目标应用标识中的副标识信息及目标应用标识信息对应的目标访问地址发送给第一应用所属的设备 11。第一应用所属的设备 11 保存第二应用的副标识信息与目标访问地址的对应关系。

（5）第一应用共享第二应用的数据的过程包括:

第一应用（应用 B）所属的设备根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识（如副标识信息）对应的目标访问地址，向目标访问地址发送共享第二应用的数据的共享请求，该共享请求中携带目标应用标识（如副标识信息）。

目标访问地址所属的设备 12 终端中的加密代理模块判断共享请求中携带的目标应用标识是否为第二应用的副标识信息，若是，则基于应用副逻辑（副 Schema）来进行相应的共享数据的过程，即可以判断共享请求的类型为读取数据请求还是写入数据请求，如果该共享请求为读取数据请求，且预先保存的第一应用对第二应用的数据的使用权限中包括第一应用可以读取第二应用的数据，则认为该共享请求符合使用权限，可以根据保存的应用标识与数据库的对应关系，确定目标应用标识对应的目标数据库 13；获取目标数据库 13 中保存的数据。加密代理模块将从目标数据库 13 中获取的数据发送给加解密模块，加解密模块根据保存的应用标识与加密密钥的对应关系，确定目标应用标识对应的目标加密密钥，基于目标加密密钥对获取的数据进行解密，将解密后的数据发送给加密代理模块。加密代理模块将解密后的数据发送给第一应用所属的设备 11。

实施例 3:

基于相同的技术构思，本申请提供了一种数据共享方法，该数据共享方法应用于第一应用所属的设备，图 11 示出了一些实施例提供的第六种数据共享过程示意图，该数据共享过程包括以下步骤:

S1101: 根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向所述目标访问地址发送共享所述第

二应用的数据的共享请求，所述共享请求中携带所述目标应用标识。

S1102：接收所述目标访问地址所属的设备发送的解密后的所述第二应用的数据。

第一应用所属的设备可以为 PC、移动终端等设备，也可以是服务器等设备。

在一种可能的实施方式中，所述根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址之前，所述方法还包括：

向管理平台发送共享所述第二应用的数据的申请，所述申请中携带所述第一应用的应用标识；

若接收到所述管理平台发送的所述第二应用的目标应用标识及所述目标应用标识信息对应的目标访问地址，保存所述目标应用标识与所述目标访问地址的对应关系。

基于相同的技术构思，本申请提供了一种数据共享方法，该数据共享方法应用于目标访问地址所属的设备，图 12 示出了一些实施例提供的第七种数据共享过程示意图，该数据共享过程包括以下步骤：

S1201：接收第一应用所属的设备发送的共享请求，所述共享请求中携带所述目标应用标识。

S1202：根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据。

S1203：根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥；基于所述目标加密密钥，对获取的数据进行解密；将解密后的数据发送给所述第一应用所属的设备。

目标访问地址所属的设备可以为 PC、移动终端等设备，也可以是服务器等设备。

在一种可能的实施方式中，所述接收第一应用所属的设备发送的共享请求之后，所述根据保存的应用标识与数据库的对应关系，确定所述目标应用

标识对应的目标数据库之前，所述方法还包括：

判断所述共享请求的类型为读取数据请求还是写入数据请求，基于所述共享请求的类型以及预先保存的所述第一应用对所述第二应用的数据的使用权限，判断所述共享请求是否符合所述使用权限，若是，则进行后续根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库的步骤。

在一种可能的实施方式中，所述基于所述目标加密密钥对获取的数据进行解密之后，所述将解密后的数据发送给所述第一应用所属的设备之前，所述方法还包括：

若获取的数据包含设定的敏感数据，则对所述解密后的数据进行数据脱敏处理；

所述将解密后的数据发送给所述第一应用所属的设备，包括：

将经过数据脱敏处理后的数据发送给所述第一应用所属的设备。

在一种可能的实施方式中，所述接收第一应用所属的设备发送的共享请求之后，所述判断所述共享请求的类型为读取数据请求还是写入数据请求之前，所述方法还包括：

若所述第二应用的目标应用标识包括主标识信息和副标识信息，判断所述共享请求中携带的目标应用标识是否为所述第二应用的副标识信息，若是，则进行后续步骤。

在一种可能的实施方式中，所述接收第一应用所属的设备发送的共享请求之前，所述方法还包括：

向管理平台发送获取所述第二应用对应的目标加密密钥的获取密钥请求；

若接收到所述管理平台发送的所述第二应用对应的目标加密密钥，保存所述目标加密密钥与所述目标应用标识的对应关系。

在一种可能的实施方式中，接收到所述管理平台发送的所述第二应用对应的目标加密密钥之后，所述保存所述目标加密密钥与所述目标应用标识的对应关系之前，所述方法还包括：

若接收到的目标加密密钥为基于与所述管理平台协商的临时安全通道密钥加密后的目标加密密钥，基于所述临时安全通道密钥，对所述目标加密密钥进行解密。

在一种可能的实施方式中，保存所述目标加密密钥包括：

基于设定的第二 TEE 物理存储根密钥对所述目标加密密钥进行加密，保存加密后的目标加密密钥。

在一种可能的实施方式中，所述方法还包括：

接收第二应用所属的设备发送的写入数据请求，所述写入数据请求中携带待写入数据库中的数据以及所述第二应用的目标应用标识；

根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥，基于所述目标加密密钥，对所述待写入数据库中的数据进行加密，将加密后的数据保存到对应的目标数据库中。

在一种可能的实施方式中，所述基于所述目标加密密钥，对所述待写入数据库中的数据进行加密，包括：

根据预先保存的应用标识与加密策略的对应关系，确定所述目标应用标识对应的目标加密策略；基于所述目标加密密钥以及所述目标加密策略，对所述待写入数据库中的数据进行加密。

在一种可能的实施方式中，所述方法还包括：

接收第二应用所属的设备发送的读取数据请求，所述读取数据请求中携带所述第二应用的目标应用标识；

根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据；

根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥，基于所述目标加密密钥，对获取的数据进行解密，将解密后的数据发送给所述第二应用所属的设备。

在一种可能的实施方式中，所述基于所述目标加密密钥，对获取的数据进行解密，包括：

根据预先保存的应用标识与加密策略的对应关系，确定所述目标应用标识对应的目标加密策略；

基于所述目标加密密钥以及所述目标加密策略，对获取的所述数据进行解密。

基于相同的技术构思，本申请提供了一种数据共享方法，该数据共享方法应用于第二应用所属的设备，图 13 示出了一些实施例提供的第八种数据共享过程示意图，该数据共享过程包括以下步骤：

S1301：若接收到管理平台发送的申请，展示所述申请中携带的第一应用的应用标识。

S1302：若接收到同意所述第一应用共享数据的确认指令，将所述确认指令发送给所述管理平台。

第二应用所属的设备可以为 PC、移动终端等设备，也可以是服务器等设备。

在一种可能的实施方式中，所述方法还包括：

向所述管理平台发送数据存储安全保护请求，所述数据存储安全保护请求中携带所述第二应用的名称及所述第二应用的目标访问地址。

在一种可能的实施方式中，所述方法还包括：

向所述目标访问地址发送写入数据请求，所述写入数据请求中携带待写入数据库中的数据以及所述第二应用的目标应用标识。

在一种可能的实施方式中，所述方法还包括：

向所述目标访问地址发送读取数据请求，所述读取数据请求中携带所述第二应用的目标应用标识；

接收所述目标访问地址所属的设备发送的解密后的数据。

基于相同的技术构思，本申请提供了一种数据共享方法，该数据共享方法应用于管理平台，图 14 示出了一些实施例提供的第九种数据共享过程示意图，该数据共享过程包括以下步骤：

S1401：接收第一应用所属的设备发送的共享所述第二应用的数据的申请，

所述申请中携带所述第一应用的应用标识。

S1402：将所述申请发送给所述第二应用所属的设备。

S1403：若接收到所述第二应用所属的设备发送的同意所述第一应用共享数据的确认指令，将保存的所述第二应用的目标应用标识及所述目标应用标识信息对应的目标访问地址发送给所述第一应用所属的设备。

在一种可能的实施方式中，所述接收第一应用所属的设备发送的共享所述第二应用的数据的申请之前，所述方法还包括：

接收所述第二应用所属的设备发送的数据存储安全保护请求，所述数据存储安全保护请求中携带所述第二应用的名称及所述第二应用的目标访问地址；

接收所述数据存储安全保护请求，生成所述第二应用的名称对应的目标应用标识以及目标加密密钥，并保存所述目标应用标识与所述目标加密密钥的对应关系；

若接收到所述目标访问地址所属的设备发送的获取所述第二应用对应的目标加密密钥的获取密钥请求；

根据保存的应用标识与加密密钥的对应关系，确定所述第二应用的目标应用标识对应的目标加密密钥，将所述目标加密密钥发送给所述目标访问地址所属的设备。

在一种可能的实施方式中，所述确定所述第二应用的目标应用标识对应的目标加密密钥之后，所述将所述目标加密密钥发送给所述目标访问地址所属的设备之前，所述方法还包括：

若保存的所述目标加密密钥为基于设定的第一 TEE 物理存储根密钥加密后的密钥，基于所述第一 TEE 物理存储根密钥对所述目标加密密钥解密；

将所述目标加密密钥发送给所述目标访问地址所属的设备，包括：

将解密后的目标加密密钥，发送给所述目标访问地址所属的设备。

在一种可能的实施方式中，所述将所述目标加密密钥发送给所述目标访问地址所属的设备，包括：

基于建立的安全通道，将所述目标加密密钥发送给所述目标访问地址所属的设备。

在一种可能的实施方式中，所述基于建立的安全通道，将所述目标加密密钥发送给所述目标访问地址所属的设备，包括:

基于与所述目标访问地址所属的设备协商的临时安全通道密钥，对所述目标加密密钥进行加密，基于所述安全通道，将加密后的目标加密密钥发送给所述目标访问地址所属的设备。

在一种可能的实施方式中，所述方法还包括:

接收所述目标访问地址所属的设备发送的获取所述第二应用的加密策略请求，其中所述加密策略请求中携带所述第二应用对应的目标应用标识;

若所述目标应用标识对应的第二应用所属的设备发送的所述数据存储安全保护请求中携带对数据的加密策略，将所述加密策略发送给所述目标访问地址所属的设备，使所述目标访问地址所属的设备保存所述目标应用标识与所述加密策略的对应关系。

实施例 4:

基于相同的技术构思，本申请提供了一种数据共享装置，应用于第一应用所属的设备，图 15 示出了一些实施例提供的第一种数据共享装置示意图，该装置包括:

第一确定模块 151，用于根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向所述目标访问地址发送共享所述第二应用的数据的共享请求，所述共享请求中携带所述目标应用标识;

第一接收模块 152，用于接收所述目标访问地址所属的设备发送的解密后的所述第二应用的数据。

在一种可能的实施方式中，所述第一确定模块 151，还用于向管理平台发送共享所述第二应用的数据的申请，所述申请中携带所述第一应用的应用标识；若接收到所述管理平台发送的所述第二应用的目标应用标识及所述目标

应用标识信息对应的目标访问地址，保存所述目标应用标识与所述目标访问地址的对应关系。

基于相同的技术构思，本申请提供了一种数据共享装置，应用于目标访问地址所属的设备，图 16 示出了一些实施例提供的第二种数据共享装置示意图，该装置包括:

第二接收模块 161，用于接收第一应用所属的设备发送的共享请求，所述共享请求中携带所述目标应用标识;

第二确定模块 162，用于根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据;

加解密模块 163，用于根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥；基于所述目标加密密钥，对获取的数据进行解密；将解密后的数据发送给所述第一应用所属的设备。

在一种可能的实施方式中，所述第二确定模块 162，还用于判断所述共享请求的类型为读取数据请求还是写入数据请求，基于所述共享请求的类型以及预先保存的所述第一应用对所述第二应用的数据的使用权限，判断所述共享请求是否符合所述使用权限，若是，则进行后续根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库的步骤。

在一种可能的实施方式中，所述加解密模块 163，还用于若获取的数据包含设定的敏感数据，则对所述解密后的数据进行数据脱敏处理；将经过数据脱敏处理后的数据发送给所述第一应用所属的设备。

在一种可能的实施方式中，所述第二确定模块 162，还用于若所述第二应用的目标应用标识包括主标识信息和副标识信息，判断所述共享请求中携带的目标应用标识是否为所述第二应用的副标识信息，若是，则进行后续判断所述共享请求的类型为读取数据请求还是写入数据请求的步骤。

在一种可能的实施方式中，所述第二接收模块 161，还用于向管理平台发送获取所述第二应用对应的目标加密密钥的获取密钥请求；若接收到所述管理平台发送的所述第二应用对应的目标加密密钥，保存所述目标加密密钥与

所述目标应用标识的对应关系。

在一种可能的实施方式中，所述第二接收模块 161，还用于若接收到的目标加密密钥为基于与所述管理平台协商的临时安全通道密钥加密后的目标加密密钥，基于所述临时安全通道密钥，对所述目标加密密钥进行解密。

在一种可能的实施方式中，所述第二接收模块 161，具体用于基于设定的第二 TEE 物理存储根密钥对所述目标加密密钥进行加密，保存加密后的目标加密密钥。

在一种可能的实施方式中，所述加解密模块 163，还用于接收第二应用所属的设备发送的写入数据请求，所述写入数据请求中携带待写入数据库中的数据以及所述第二应用的目标应用标识；根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥，基于所述目标加密密钥，对所述待写入数据库中的数据进行加密，将加密后的数据保存到对应的目标数据库中。

在一种可能的实施方式中，所述加解密模块 163，具体用于根据预先保存的应用标识与加密策略的对应关系，确定所述目标应用标识对应的目标加密策略；基于所述目标加密密钥以及所述目标加密策略，对所述待写入数据库中的数据进行加密。

在一种可能的实施方式中，所述加解密模块 163，还用于接收第二应用所属的设备发送的读取数据请求，所述读取数据请求中携带所述第二应用的目标应用标识；根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥，基于所述目标加密密钥，对获取的数据进行解密，将解密后的数据发送给所述第二应用所属的设备。

在一种可能的实施方式中，所述加解密模块 163，具体用于根据预先保存的应用标识与加密策略的对应关系，确定所述目标应用标识对应的目标加密策略；基于所述目标加密密钥以及所述目标加密策略，对获取的所述数据进

行解密。

基于相同的技术构思，本申请提供了一种数据共享装置，应用于第二应用所属的设备，图 17 示出了一些实施例提供的第三种数据共享装置示意图，该装置包括:

展示模块 171，用于若接收到管理平台发送的申请，展示所述申请中携带的第一应用的应用标识;

第一发送模块 172，用于若接收到同意所述第一应用共享数据的确认指令，将所述确认指令发送给所述管理平台。

在一种可能的实施方式中，所述第一发送模块 172，还用于向所述管理平台发送数据存储安全保护请求，所述数据存储安全保护请求中携带所述第二应用的名称及所述第二应用的目标访问地址。

在一种可能的实施方式中，所述第一发送模块 172，还用于向所述目标访问地址发送写入数据请求，所述写入数据请求中携带待写入数据库中的数据以及所述第二应用的目标应用标识。

在一种可能的实施方式中，所述第一发送模块 172，还用于向所述目标访问地址发送读取数据请求，所述读取数据请求中携带所述第二应用的目标应用标识; 接收所述目标访问地址所属的设备发送的解密后的数据。

基于相同的技术构思，本申请提供了一种数据共享装置，应用于管理平台，图 18 示出了一些实施例提供的第四种数据共享装置示意图，该装置包括:

第三接收模块 181，用于接收第一应用所属的设备发送的共享所述第二应用的数据的申请，所述申请中携带所述第一应用的应用标识;

第二发送模块 182，用于将所述申请发送给所述第二应用所属的设备; 若接收到所述第二应用所属的设备发送的同意所述第一应用共享数据的确认指令，将保存的所述第二应用的目标应用标识及所述目标应用标识信息对应的目标访问地址发送给所述第一应用所属的设备。

在一种可能的实施方式中，所述第三接收模块 181，还用于接收所述第二应用所属的设备发送的数据存储安全保护请求，所述数据存储安全保护请求

中携带所述第二应用的名称及所述第二应用的目标访问地址；接收所述数据存储安全保护请求，生成所述第二应用的名称对应的目标应用标识以及目标加密密钥，并保存所述目标应用标识与所述目标加密密钥的对应关系；若接收到所述目标访问地址所属的设备发送的获取所述第二应用对应的目标加密密钥的获取密钥请求；根据保存的应用标识与加密密钥的对应关系，确定所述第二应用的目标应用标识对应的目标加密密钥，将所述目标加密密钥发送给所述目标访问地址所属的设备。

在一种可能的实施方式中，所述第三接收模块 181，还用于若保存的所述目标加密密钥为基于设定的第一 TEE 物理存储根密钥加密后的密钥，基于所述第一 TEE 物理存储根密钥对所述目标加密密钥解密；将解密后的目标加密密钥，发送给所述目标访问地址所属的设备。

在一种可能的实施方式中，所述第三接收模块 181，具体用于基于建立的安全通道，将所述目标加密密钥发送给所述目标访问地址所属的设备。

在一种可能的实施方式中，所述第三接收模块 181，具体用于基于与所述目标访问地址所属的设备协商的临时安全通道密钥，对所述目标加密密钥进行加密，基于所述安全通道，将加密后的目标加密密钥发送给所述目标访问地址所属的设备。

在一种可能的实施方式中，所述第二发送模块 182，还用于接收所述目标访问地址所属的设备发送的获取所述第二应用的加密策略请求，其中所述加密策略请求中携带所述第二应用对应的目标应用标识；若所述目标应用标识对应的第二应用所属的设备发送的所述数据存储安全保护请求中携带对数据的加密策略，将所述加密策略发送给所述目标访问地址所属的设备，使所述目标访问地址所属的设备保存所述目标应用标识与所述加密策略的对应关系。

基于相同的技术构思，本申请还提供了一种电子设备，图 19 示出了一些实施例提供的一种电子设备结构示意图，如图 19 所示，包括：处理器 191、通信接口 192、存储器 193 和通信总线 194，其中，处理器 191，通信接口 192，存储器 193 通过通信总线 194 完成相互间的通信；

在一种可能的实施方式中，所述存储器 193 中存储有计算机程序，当所述程序被所述处理器 191 执行时，使得所述处理器 191 执行上述任意一种数据共享方法的步骤。

由于上述电子设备解决问题的原理与数据共享方法相似，因此上述电子设备的实施可以参见方法的实施，重复之处不再赘述。

上述电子设备提到的通信总线可以是外设部件互连标准（Peripheral Component Interconnect，PCI）总线或扩展工业标准结构（Extended Industry Standard Architecture，EISA）总线等。该通信总线可以分为地址总线、数据总线、控制总线等。为便于表示，图中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

通信接口 192 用于上述电子设备与其他设备之间的通信。

存储器可以包括随机存取存储器（Random Access Memory，RAM），也可以包括非易失性存储器（Non-Volatile Memory，NVM），例如至少一个磁盘存储器。可选地，存储器还可以是至少一个位于远离前述处理器的存储装置。

上述处理器可以是通用处理器，包括中央处理器、网络处理器（Network Processor，NP）等；还可以是数字指令处理器（Digital Signal Processing，DSP）、专用集成电路、现场可编程门陈列或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。

基于相同的技术构思，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质内存储有可由电子设备执行的计算机程序，当所述程序在所述电子设备上运行时，使得所述电子设备执行时实现上述任意一种数据共享方法的步骤。

上述计算机可读存储介质可以是电子设备中的处理器能够存取的任何可用介质或数据存储设备，包括但不限于磁性存储器如软盘、硬盘、磁带、磁光盘（MO）等、光学存储器如 CD、DVD、BD、HVD 等、以及半导体存储器如 ROM、EPROM、EEPROM、非易失性存储器（NAND FLASH）、固态硬盘（SSD）等。

基于相同的技术构思，在上述各实施例的基础上，本申请提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行如上述任一所述数据共享方法的步骤。

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。

本申请是参照根据本申请的方法、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。

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。

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。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1、一种数据共享系统，所述系统包括:

第一应用所属的设备，用于根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向所述目标访问地址发送共享所述第二应用的数据的共享请求，所述共享请求中携带所述目标应用标识;

所述目标访问地址所属的设备，用于接收所述共享请求，根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥；基于所述目标加密密钥，对获取的数据进行解密；将解密后的数据发送给所述第一应用所属的设备;

所述目标数据库，用于存储数据。

2、根据权利要求 1 所述的系统，所述系统还包括：管理平台和第二应用所属的设备;

所述第一应用所属的设备，还用于向所述管理平台发送共享所述第二应用的数据的申请，所述申请中携带所述第一应用的应用标识;

所述管理平台，用于接收所述申请，并将所述申请发送给所述第二应用所属的设备;

所述第二应用所属的设备，用于接收所述申请并展示所述申请中携带的所述第一应用的应用标识，若接收到同意所述第一应用共享数据的确认指令，将所述确认指令发送给所述管理平台;

所述管理平台，还用于接收所述确认指令，将保存的所述第二应用的目标应用标识及所述目标应用标识信息对应的目标访问地址发送给所述第一应用所属的设备;

所述第一应用所属的设备，还用于保存所述目标应用标识与所述目标访问地址的对应关系。

3、根据权利要求 1 所述的系统，所述目标访问地址所属的设备，还用于判断所述共享请求的类型为读取数据请求还是写入数据请求，基于所述共享请求的类型以及预先保存的所述第一应用对所述第二应用的数据的使用权限，判断所述共享请求是否符合所述使用权限，若是，则进行根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库的步骤。

4、根据权利要求 1-3 任一所述的系统，所述目标访问地址所属的设备，还用于若获取的数据包含设定的敏感数据，则对所述解密后的数据进行数据脱敏处理，并将经过数据脱敏处理后的数据发送给所述第一应用所属的设备。

5、根据权利要求 3 所述的系统，所述目标访问地址所属的设备，还用于若所述第二应用的目标应用标识包括主标识信息和副标识信息，判断所述共享请求中携带的目标应用标识是否为所述第二应用的副标识信息，若是，则进行判断所述共享请求的类型为读取数据请求还是写入数据请求，基于所述共享请求的类型以及预先保存的所述第一应用对所述第二应用的数据的使用权限，判断所述共享请求是否符合所述使用权限的步骤。

6、根据权利要求 1 所述的系统，所述系统还包括：管理平台和第二应用所属的设备；

所述第二应用所属的设备，用于向所述管理平台发送数据存储安全保护请求，所述数据存储安全保护请求中携带所述第二应用的名称及所述第二应用的目标访问地址；

所述管理平台，还用于接收所述数据存储安全保护请求，生成所述第二应用的名称对应的目标应用标识以及目标加密密钥，并保存所述目标应用标识与所述目标加密密钥的对应关系；

所述目标访问地址所属的设备，还用于向所述管理平台发送获取所述第二应用对应的目标加密密钥的获取密钥请求；

所述管理平台，用于接收所述获取密钥请求，根据保存的应用标识与加密密钥的对应关系，确定所述第二应用的目标应用标识对应的目标加密密钥，将所述目标加密密钥发送给所述目标访问地址所属的设备；

所述目标访问地址所属的设备，还用于接收所述目标加密密钥，并保存所述目标加密密钥与所述目标应用标识的对应关系。

7、根据权利要求 6 所述的系统，其中，所述管理平台中保存的所述目标加密密钥是保存在所述管理平台的可信执行环境 TEE 中的；和/或，

所述目标访问地址所属的设备中保存的所述目标加密密钥是保存在所述目标访问地址所属的设备的 TEE 中的。

8、根据权利要求 6-7 任一所述的系统，所述管理平台，还用于若保存的所述目标加密密钥为基于设定的第一 TEE 物理存储根密钥加密后的密钥，基于所述第一 TEE 物理存储根密钥对所述目标加密密钥解密，将解密后的目标加密密钥，发送给所述目标访问地址所属的设备。

9、根据权利要求 6-7 任一所述的系统，其中，所述管理平台，具体用于基于建立的安全通道，将所述目标加密密钥发送给所述目标访问地址所属的设备。

10、根据权利要求 9 所述的系统，其中，所述管理平台，具体用于基于与所述目标访问地址所属的设备协商的临时安全通道密钥，对所述目标加密密钥进行加密，基于所述安全通道，将加密后的目标加密密钥发送给所述目标访问地址所属的设备;

所述目标访问地址所属的设备，还用于接收基于与所述管理平台协商的所述临时安全通道密钥加密后的目标加密密钥，基于所述临时安全通道密钥，对所述目标加密密钥进行解密。

11、根据权利要求 6 或 7 或 10 所述的系统，所述目标访问地址所属的设备，还用于基于设定的第二 TEE 物理存储根密钥对所述目标加密密钥进行加密，保存加密后的目标加密密钥。

12、根据权利要求 6 所述的系统，所述第二应用所属的设备，还用于向所述目标访问地址发送写入数据请求，所述写入数据请求中携带待写入数据库中的数据以及所述第二应用的目标应用标识;

所述目标访问地址所属的设备，还用于接收所述写入数据请求，根据保

存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥，基于所述目标加密密钥，对所述待写入数据库中的数据进行加密，将加密后的数据保存到对应的目标数据库中。

13、根据权利要求 12 所述的系统，所述目标访问地址所属的设备，还用于向所述管理平台发送获取所述第二应用的加密策略请求，所述加密策略请求中携带所述第二应用对应的目标应用标识；

所述管理平台，还用于接收所述加密策略请求，若所述目标应用标识对应的第二应用所属的设备发送的所述数据存储安全保护请求中，携带对数据的加密策略，将所述加密策略发送给所述目标访问地址所属的设备；

所述目标访问地址所属的设备，还用于接收所述加密策略，保存所述目标应用标识与所述加密策略的对应关系；若接收到所述写入数据请求，则根据保存的应用标识与加密策略的对应关系，确定所述目标应用标识对应的目标加密策略；基于所述目标加密密钥以及所述目标加密策略，对所述待写入数据库中的数据进行加密。

14、根据权利要求 6 所述的系统，第二应用所属的设备，还用于向所述目标访问地址发送读取数据请求，所述读取数据请求中携带所述第二应用的目标应用标识；

所述目标访问地址所属的设备，还用于接收所述读取数据请求，根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据；根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥，基于所述目标加密密钥，对获取的数据进行解密，将解密后的数据发送给所述第二应用所属的设备。

15、根据权利要求 14 所述的系统，所述目标访问地址所属的设备，还用于向所述管理平台发送获取所述第二应用的加密策略请求，所述加密策略请求中携带所述第二应用对应的目标应用标识；

所述管理平台，还用于接收所述加密策略请求，若所述目标应用标识对

应的第二应用所属的设备发送的所述数据存储安全保护请求中，携带对数据的加密策略，将所述加密策略发送给所述目标访问地址所属的设备;

所述目标访问地址所属的设备，还用于接收所述加密策略，保存所述目标应用标识与所述加密策略的对应关系；若接收到所述读取数据请求，根据保存的应用标识与加密策略的对应关系，确定所述目标应用标识对应的目标加密策略；基于所述目标加密密钥以及所述目标加密策略，对获取的所述数据进行解密。

16、一种数据共享方法，所述方法应用于第一应用所属的设备，所述方法包括:

根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向所述目标访问地址发送共享所述第二应用的数据的共享请求，所述共享请求中携带所述目标应用标识;

接收所述目标访问地址所属的设备发送的解密后的所述第二应用的数据。

17、根据权利要求 16 所述的方法，所述根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址之前，所述方法还包括:

向管理平台发送共享所述第二应用的数据的申请，所述申请中携带所述第一应用的应用标识;

若接收到所述管理平台发送的所述第二应用的目标应用标识及所述目标应用标识信息对应的目标访问地址，保存所述目标应用标识与所述目标访问地址的对应关系。

18、一种数据共享方法，所述方法应用于目标访问地址所属的设备，所述方法包括:

接收第一应用所属的设备发送的共享请求，所述共享请求中携带所述目标应用标识;

根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据;

根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥；基于所述目标加密密钥，对获取的数据进行解密；将解密后的数据发送给所述第一应用所属的设备。

19、根据权利要求 18 所述的方法，所述接收第一应用所属的设备发送的共享请求之后，所述根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库之前，所述方法还包括:

判断所述共享请求的类型为读取数据请求还是写入数据请求，基于所述共享请求的类型以及预先保存的所述第一应用对所述第二应用的数据的使用权限，判断所述共享请求是否符合所述使用权限，若是，则进行后续根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库的步骤。

20、根据权利要求 18 或 19 所述的方法，所述基于所述目标加密密钥对获取的数据进行解密之后，所述将解密后的数据发送给所述第一应用所属的设备之前，所述方法还包括:

若获取的数据包含设定的敏感数据，则对所述解密后的数据进行数据脱敏处理;

所述将解密后的数据发送给所述第一应用所属的设备，包括:

将经过数据脱敏处理后的数据发送给所述第一应用所属的设备。

21、根据权利要求 19 所述的方法，所述接收第一应用所属的设备发送的共享请求之后，所述判断所述共享请求的类型为读取数据请求还是写入数据请求之前，所述方法还包括:

若所述第二应用的目标应用标识包括主标识信息和副标识信息，判断所述共享请求中携带的目标应用标识是否为所述第二应用的副标识信息，若是，则进行后续步骤。

22、根据权利要求 18 所述的方法，所述接收第一应用所属的设备发送的共享请求之前，所述方法还包括:

向管理平台发送获取所述第二应用对应的目标加密密钥的获取密钥请求;

若接收到所述管理平台发送的所述第二应用对应的目标加密密钥，保存所述目标加密密钥与所述目标应用标识的对应关系。

23、根据权利要求 22 所述的方法，接收到所述管理平台发送的所述第二应用对应的目标加密密钥之后，所述保存所述目标加密密钥与所述目标应用标识的对应关系之前，所述方法还包括：

若接收到的目标加密密钥为基于与所述管理平台协商的临时安全通道密钥加密后的目标加密密钥，基于所述临时安全通道密钥，对所述目标加密密钥进行解密。

24、根据权利要求 22 或 23 所述的方法，其中，保存所述目标加密密钥包括：

基于设定的第二 TEE 物理存储根密钥对所述目标加密密钥进行加密，保存加密后的目标加密密钥。

25、根据权利要求 22 所述的方法，所述方法还包括：

接收第二应用所属的设备发送的写入数据请求，所述写入数据请求中携带待写入数据库中的数据以及所述第二应用的目标应用标识；

根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥，基于所述目标加密密钥，对所述待写入数据库中的数据进行加密，将加密后的数据保存到对应的目标数据库中。

26、根据权利要求 25 所述的方法，其中，所述基于所述目标加密密钥，对所述待写入数据库中的数据进行加密，包括：

根据预先保存的应用标识与加密策略的对应关系，确定所述目标应用标识对应的目标加密策略；基于所述目标加密密钥以及所述目标加密策略，对所述待写入数据库中的数据进行加密。

27、根据权利要求 22 所述的方法，所述方法还包括：

接收第二应用所属的设备发送的读取数据请求，所述读取数据请求中携带所述第二应用的目标应用标识；

根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应

的目标数据库；获取所述目标数据库中保存的数据；

根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥，基于所述目标加密密钥，对获取的数据进行解密，将解密后的数据发送给所述第二应用所属的设备。

28、根据权利要求 27 所述的方法，其中，所述基于所述目标加密密钥，对获取的数据进行解密，包括：

根据预先保存的应用标识与加密策略的对应关系，确定所述目标应用标识对应的目标加密策略；

基于所述目标加密密钥以及所述目标加密策略，对获取的所述数据进行解密。

29、一种数据共享方法，所述方法应用于第二应用所属的设备，所述方法包括：

若接收到管理平台发送的申请，展示所述申请中携带的第一应用的应用标识；

若接收到同意所述第一应用共享数据的确认指令，将所述确认指令发送给所述管理平台。

30、根据权利要求 29 所述的方法，所述方法还包括：

向所述管理平台发送数据存储安全保护请求，所述数据存储安全保护请求中携带所述第二应用的名称及所述第二应用的目标访问地址。

31、根据权利要求 30 所述的方法，所述方法还包括：

向所述目标访问地址发送写入数据请求，所述写入数据请求中携带待写入数据库中的数据以及所述第二应用的目标应用标识。

32、根据权利要求 30 所述的方法，所述方法还包括：

向所述目标访问地址发送读取数据请求，所述读取数据请求中携带所述第二应用的目标应用标识；

接收所述目标访问地址所属的设备发送的解密后的数据。

33、一种数据共享方法，所述方法应用于管理平台，所述方法包括：

接收第一应用所属的设备发送的共享所述第二应用的数据的申请，所述申请中携带所述第一应用的应用标识;

将所述申请发送给所述第二应用所属的设备;

若接收到所述第二应用所属的设备发送的同意所述第一应用共享数据的确认指令，将保存的所述第二应用的目标应用标识及所述目标应用标识信息对应的目标访问地址发送给所述第一应用所属的设备。

34、根据权利要求 33 所述的方法，所述接收第一应用所属的设备发送的共享所述第二应用的数据的申请之前，所述方法还包括:

接收所述第二应用所属的设备发送的数据存储安全保护请求，所述数据存储安全保护请求中携带所述第二应用的名称及所述第二应用的目标访问地址;

接收所述数据存储安全保护请求，生成所述第二应用的名称对应的目标应用标识以及目标加密密钥，并保存所述目标应用标识与所述目标加密密钥的对应关系;

若接收到所述目标访问地址所属的设备发送的获取所述第二应用对应的目标加密密钥的获取密钥请求;

根据保存的应用标识与加密密钥的对应关系，确定所述第二应用的目标应用标识对应的目标加密密钥，将所述目标加密密钥发送给所述目标访问地址所属的设备。

35、根据权利要求 34 所述的方法，所述确定所述第二应用的目标应用标识对应的目标加密密钥之后，所述将所述目标加密密钥发送给所述目标访问地址所属的设备之前，所述方法还包括:

若保存的所述目标加密密钥为基于设定的第一 TEE 物理存储根密钥加密后的密钥，基于所述第一 TEE 物理存储根密钥对所述目标加密密钥解密;

将所述目标加密密钥发送给所述目标访问地址所属的设备，包括:

将解密后的目标加密密钥，发送给所述目标访问地址所属的设备。

36、根据权利要求 34 或 35 所述的方法，其中，所述将所述目标加密密

钥发送给所述目标访问地址所属的设备，包括:

基于建立的安全通道，将所述目标加密密钥发送给所述目标访问地址所属的设备。

37、根据权利要求 36 所述的方法，其中，所述基于建立的安全通道，将所述目标加密密钥发送给所述目标访问地址所属的设备，包括:

基于与所述目标访问地址所属的设备协商的临时安全通道密钥，对所述目标加密密钥进行加密，基于所述安全通道，将加密后的目标加密密钥发送给所述目标访问地址所属的设备。

38、根据权利要求 34 所述的方法，所述方法还包括:

接收所述目标访问地址所属的设备发送的获取所述第二应用的加密策略请求，其中所述加密策略请求中携带所述第二应用对应的目标应用标识;

若所述目标应用标识对应的第二应用所属的设备发送的所述数据存储安全保护请求中携带对数据的加密策略，将所述加密策略发送给所述目标访问地址所属的设备，使所述目标访问地址所属的设备保存所述目标应用标识与所述加密策略的对应关系。

39、一种数据共享装置，所述装置包括:

第一确定模块，用于根据预先保存的应用标识与访问地址的对应关系，确定第二应用的目标应用标识对应的目标访问地址，向所述目标访问地址发送共享所述第二应用的数据的共享请求，所述共享请求中携带所述目标应用标识;

第一接收模块，用于接收所述目标访问地址所属的设备发送的解密后的所述第二应用的数据。

40、一种数据共享装置，所述装置包括:

第二接收模块，用于接收第一应用所属的设备发送的共享请求，所述共享请求中携带所述目标应用标识;

第二确定模块，用于根据保存的应用标识与数据库的对应关系，确定所述目标应用标识对应的目标数据库；获取所述目标数据库中保存的数据;

加解密模块，用于根据保存的应用标识与加密密钥的对应关系，确定所述目标应用标识对应的目标加密密钥；基于所述目标加密密钥，对获取的数据进行解密；将解密后的数据发送给所述第一应用所属的设备。

41、一种数据共享装置，所述装置包括:

展示模块，用于若接收到管理平台发送的申请，展示所述申请中携带的第一应用的应用标识;

第一发送模块，用于若接收到同意所述第一应用共享数据的确认指令，将所述确认指令发送给所述管理平台。

42、一种数据共享装置，所述装置包括:

第三接收模块，用于接收第一应用所属的设备发送的共享所述第二应用的数据的申请，所述申请中携带所述第一应用的应用标识;

第二发送模块，用于将所述申请发送给所述第二应用所属的设备；若接收到所述第二应用所属的设备发送的同意所述第一应用共享数据的确认指令，将保存的所述第二应用的目标应用标识及所述目标应用标识信息对应的目标访问地址发送给所述第一应用所属的设备。

43、一种电子设备，其包括处理器和存储器，其中，所述存储器存储有程序代码，当所述程序代码被所述处理器执行时，使得所述处理器执行权利要求 16 至 38 任一项所述方法的步骤。

44、一种计算机可读存储介质，其包括程序代码，当所述存储介质在电子设备上运行时，所述程序代码用于使所述电子设备执行权利要求 16 至 38 任一项所述方法的步骤。