(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 113868505 A
(43)申请公布日 2021.12.31

(21)申请号 202111032589.X

(22)申请日 2021.09.03

(71)申请人 北京达佳互联信息技术有限公司
地址 100085 北京市海淀区上地西路6号1幢1层101D1-7

(72)发明人 刘纯彰

(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 关志琨

(51)Int.Cl.
G06F 16/953(2019.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)

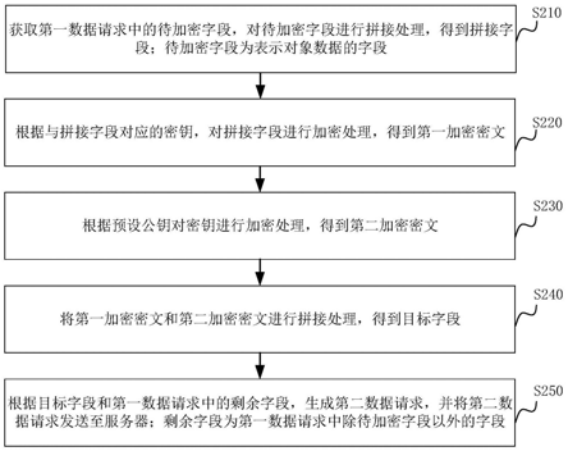
权利要求书2页 说明书15页 附图4页

(54)发明名称

数据处理方法、装置、电子设备、服务器及存储介质

(57)摘要

本公开关于一种数据处理方法、装置、电子设备、服务器及存储介质，该方法包括：获取第一数据请求中的待加密字段，对所述待加密字段进行拼接处理，得到拼接字段；所述待加密字段为表示对象数据的字段；根据与所述拼接字段对应的密钥，对所述拼接字段进行加密处理，得到第一加密密文；根据预设公钥对所述密钥进行加密处理，得到第二加密密文；将所述第一加密密文和所述第二加密密文进行拼接处理，得到目标字段；根据所述目标字段和所述第一数据请求中的剩余字段，生成第二数据请求，并将所述第二数据请求发送至服务器；所述剩余字段为所述第一数据请求中除所述待加密字段以外的字段。采用本方法，有利于避免数据泄露，从而提高了数据的安全性。



CN 113868505 A

1.一种数据处理方法,其特征在于,应用于终端,包括:

获取第一数据请求中的待加密字段,对所述待加密字段进行拼接处理,得到拼接字段;所述待加密字段为表示对象数据的字段;

根据与所述拼接字段对应的密钥,对所述拼接字段进行加密处理,得到第一加密密文;

根据预设公钥对所述密钥进行加密处理,得到第二加密密文;

将所述第一加密密文和所述第二加密密文进行拼接处理,得到目标字段;

根据所述目标字段和所述第一数据请求中的剩余字段,生成第二数据请求,并将所述第二数据请求发送至服务器;所述剩余字段为所述第一数据请求中除所述待加密字段以外的字段。

2.根据权利要求1所述的数据处理方法,其特征在于,所述获取第一数据请求中的待加密字段,包括:

获取第一数据请求中的字段的字段标识;

若所述字段的字段标识与预设字段标识匹配,则将所述字段识别为所述第一数据请求中的待加密字段;所述预设字段标识为表示对象数据的字段的字段标识。

3.根据权利要求1所述的数据处理方法,其特征在于,在对所述待加密字段进行拼接处理,得到拼接字段之前,还包括:

获取验证文件;所述验证文件用于验证所述待加密字段是否为表示对象数据的字段;

根据所述验证文件对所述待加密字段进行验证;

所述对所述待加密字段进行拼接处理,得到拼接字段,包括:

若所述待加密字段验证通过,则按照预设拼接顺序对所述待加密字段进行拼接处理,得到拼接字段。

4.一种数据处理方法,其特征在于,应用于服务器,包括:

接收终端发送的第二数据请求;

获取所述第二数据请求中的目标字段;所述目标字段由第一加密密文和第二加密密文组成,所述第二加密密文由预设公钥加密得到,所述第一加密密文由密钥加密得到;

根据与所述预设公钥匹配的预设私钥,对所述第二加密密文进行解密处理,得到所述密钥;

根据所述密钥对所述第一加密密文进行解密处理,得到拼接字段;

对所述拼接字段进行拆分处理,得到所述第一加密密文对应的原始字段。

5.一种数据处理装置,其特征在于,包括:

字段拼接单元,被配置为执行获取第一数据请求中的待加密字段,对所述待加密字段进行拼接处理,得到拼接字段;所述待加密字段为表示对象数据的字段;

第一加密单元,被配置为执行根据与所述拼接字段对应的密钥,对所述拼接字段进行加密处理,得到第一加密密文;

第二加密单元,被配置为执行根据预设公钥对所述密钥进行加密处理,得到第二加密密文;

密文拼接单元,被配置为执行将所述第一加密密文和所述第二加密密文进行拼接处理,得到目标字段;

请求发送单元,被配置为执行根据所述目标字段和所述第一数据请求中的剩余字段,

生成第二数据请求，并将所述第二数据请求发送至服务器；所述剩余字段为所述第一数据请求中除所述待加密字段以外的字段。

6.一种数据处理装置，其特征在于，包括：

请求接收单元，被配置为执行接收终端发送的第二数据请求；

字段获取单元，被配置为执行获取所述第二数据请求中的目标字段；所述目标字段由第一加密密文和第二加密密文组成，所述第二加密密文由预设公钥加密得到，所述第一加密密文由密钥加密得到；

第一解密单元，被配置为执行根据与所述预设公钥匹配的预设私钥，对所述第二加密密文进行解密处理，得到所述密钥；

第二解密单元，被配置为执行根据所述密钥对所述第一加密密文进行解密处理，得到拼接字段；

字段拆分单元，被配置为执行对所述拼接字段进行拆分处理，得到所述第一加密密文对应的原始字段。

7.一种电子设备，其特征在于，包括：

处理器；

用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为执行所述指令，以实现如权利要求1至3中任一项所述的数据处理方法。

8.一种服务器，其特征在于，包括：

处理器；

用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为执行所述指令，以实现如权利要求4所述的数据处理方法。

9.一种计算机可读存储介质，其特征在于，当所述计算机可读存储介质中的指令由电子设备的处理器执行时，使得所述电子设备能够执行如权利要求1至3中任一项所述的数据处理方法。

10.一种计算机程序产品，所述计算机程序产品中包括指令，其特征在于，所述指令被电子设备的处理器执行时，使得所述电子设备能够执行如权利要求1至3任一项所述的数据处理方法。

数据处理方法、装置、电子设备、服务器及存储介质

技术领域

[0001] 本公开涉及计算机技术领域，尤其涉及一种数据处理方法、装置、电子设备、服务器及存储介质。

背景技术

[0002] 在计算机技术领域中，一般是通过数据请求，比如数据上报请求或者数据查询请求，来上报数据或者请求数据；但是，在进行数据请求的过程中，请求中的字段的名称或者内容是明文信息，有些字段名称可能会暴露业务内部信息，有些字段内容可能会暴露用户个人信息，从而影响数据安全，进而导致数据的安全性较低。

发明内容

[0003] 本公开提供一种数据处理方法、装置、电子设备、服务器及存储介质，以至少解决相关技术中数据的安全性较低的问题。本公开的技术方案如下：

[0004] 根据本公开实施例的第一方面，提供一种数据处理方法，包括：

[0005] 获取第一数据请求中的待加密字段，对所述待加密字段进行拼接处理，得到拼接字段；所述待加密字段为表示对象数据的字段；

[0006] 根据与所述拼接字段对应的密钥，对所述拼接字段进行加密处理，得到第一加密密文；

[0007] 根据预设公钥对所述密钥进行加密处理，得到第二加密密文；

[0008] 将所述第一加密密文和所述第二加密密文进行拼接处理，得到目标字段；

[0009] 根据所述目标字段和所述第一数据请求中的剩余字段，生成第二数据请求，并将所述第二数据请求发送至服务器；所述剩余字段为所述第一数据请求中除所述待加密字段以外的字段。

[0010] 在一示例性实施例中，所述获取第一数据请求中的待加密字段，包括：

[0011] 获取第一数据请求中的字段的字段标识；

[0012] 若所述字段的字段标识与预设字段标识匹配，则将所述字段识别为所述第一数据请求中的待加密字段；所述预设字段标识为表示对象数据的字段的字段标识。

[0013] 在一示例性实施例中，在对所述待加密字段进行拼接处理，得到拼接字段之前，还包括：

[0014] 获取验证文件；所述验证文件用于验证所述待加密字段是否为表示对象数据的字段；

[0015] 根据所述验证文件对所述待加密字段进行验证；

[0016] 所述对所述待加密字段进行拼接处理，得到拼接字段，包括：

[0017] 若所述待加密字段验证通过，则按照预设拼接顺序对所述待加密字段进行拼接处理，得到拼接字段。

[0018] 在一示例性实施例中，在将所述第一加密密文和所述第二加密密文进行拼接处

理，得到目标字段之前，还包括：

[0019] 分别对所述第一加密密文和所述第二加密密文进行再次加密处理，得到所述第一加密密文对应的第三加密密文和所述第二加密密文对应的第四加密密文；

[0020] 所述将所述第一加密密文和所述第二加密密文进行拼接处理，得到目标字段，包括：

[0021] 将所述第一加密密文对应的第三加密密文和所述第二加密密文对应的第四加密密文进行拼接处理，得到所述目标字段。

[0022] 在一示例性实施例中，在根据与所述拼接字段对应的密钥，对所述拼接字段进行加密处理，得到第一加密密文之前，还包括：

[0023] 生成随机密钥，并将所述随机密钥识别为与所述拼接字段对应的密钥。

[0024] 根据本公开实施例的第二方面，提供一种数据处理方法，包括：

[0025] 接收终端发送的第二数据请求；

[0026] 获取所述第二数据请求中的目标字段；所述目标字段由第一加密密文和第二加密密文组成，所述第二加密密文由预设公钥加密得到，所述第一加密密文由密钥加密得到；

[0027] 根据与所述预设公钥匹配的预设私钥，对所述第二加密密文进行解密处理，得到所述密钥；

[0028] 根据所述密钥对所述第一加密密文进行解密处理，得到拼接字段；

[0029] 对所述拼接字段进行拆分处理，得到所述第一加密密文对应的原始字段。

[0030] 在一示例性实施例中，所述获取所述第二数据请求中的目标字段，包括：

[0031] 获取所述第二数据请求中的字段的字段标识；

[0032] 从所述第二数据请求中的字段中，筛选出所述字段标识与目标字段标识相同的字段，并将所述字段识别为所述目标字段。

[0033] 在一示例性实施例中，所述接收终端发送的第二数据请求，包括：

[0034] 通过预设的网络通道，接收终端发送的第二数据请求；所述第二数据请求由所述终端根据所述目标字段和第一数据请求中的剩余字段生成，所述目标字段由所述原始字段经过加密处理后得到，所述剩余字段为所述第一数据请求中除所述原始字段以外的字段，所述原始字段为所述第一数据请求中表示对象数据的字段。

[0035] 在一示例性实施例中，在根据与所述预设公钥匹配的预设私钥，对所述第二加密密文进行解密处理，得到所述密钥之前，还包括：

[0036] 按照所述目标字段中的密文组合顺序，从所述目标字段中识别出所述第一加密密文和所述第二加密密文。

[0037] 在一示例性实施例中，在根据所述密钥对所述第一加密密文进行解密处理，得到拼接字段之前，还包括：

[0038] 获取所述密钥的格式；

[0039] 所述根据所述密钥对所述第一加密密文进行解密处理，得到拼接字段，包括：

[0040] 当所述密钥的格式与预设格式匹配时，根据所述密钥对所述第一加密密文进行解密处理，得到拼接字段。

[0041] 根据本公开实施例的第三方面，提供一种数据处理装置，包括：

[0042] 字段拼接单元，被配置为执行获取第一数据请求中的待加密字段，对所述待加密

字段进行拼接处理，得到拼接字段；所述待加密字段为表示对象数据的字段；

[0043] 第一加密单元，被配置为执行根据与所述拼接字段对应的密钥，对所述拼接字段进行加密处理，得到第一加密密文；

[0044] 第二加密单元，被配置为执行根据预设公钥对所述密钥进行加密处理，得到第二加密密文；

[0045] 密文拼接单元，被配置为执行将所述第一加密密文和所述第二加密密文进行拼接处理，得到目标字段；

[0046] 请求发送单元，被配置为执行根据所述目标字段和所述第一数据请求中的剩余字段，生成第二数据请求，并将所述第二数据请求发送至服务器；所述剩余字段为所述第一数据请求中除所述待加密字段以外的字段。

[0047] 在一示例性实施例中，所述字段拼接单元，还被配置为执行获取第一数据请求中的字段的字段标识；若所述字段的字段标识与预设字段标识匹配，则将所述字段识别为所述第一数据请求中的待加密字段；所述预设字段标识为表示对象数据的字段的字段标识。

[0048] 在一示例性实施例中，所述装置还包括字段验证单元，被配置为执行获取验证文件；所述验证文件用于验证所述待加密字段是否为表示对象数据的字段；根据所述验证文件对所述待加密字段进行验证；

[0049] 所述字段拼接单元，还被配置为执行若所述待加密字段验证通过，则按照预设拼接顺序对所述待加密字段进行拼接处理，得到拼接字段。

[0050] 在一示例性实施例中，所述装置还包括密文加密单元，被配置为执行分别对所述第一加密密文和所述第二加密密文进行再次加密处理，得到所述第一加密密文对应的第三加密密文和所述第二加密密文对应的第四加密密文；

[0051] 所述密文拼接单元，还被配置为执行将所述第一加密密文对应的第三加密密文和所述第二加密密文对应的第四加密密文进行拼接处理，得到所述目标字段。

[0052] 在一示例性实施例中，所述装置还包括密钥获取单元，被配置为执行生成随机密钥，并将所述随机密钥识别为与所述拼接字段对应的密钥。

[0053] 根据本公开实施例的第四方面，提供一种数据处理装置，包括：

[0054] 请求接收单元，被配置为执行接收终端发送的第二数据请求；

[0055] 字段获取单元，被配置为执行获取所述第二数据请求中的目标字段；所述目标字段由第一加密密文和第二加密密文组成，所述第二加密密文由预设公钥加密得到，所述第一加密密文由密钥加密得到；

[0056] 第一解密单元，被配置为执行根据与所述预设公钥匹配的预设私钥，对所述第二加密密文进行解密处理，得到所述密钥；

[0057] 第二解密单元，被配置为执行根据所述密钥对所述第一加密密文进行解密处理，得到拼接字段；

[0058] 字段拆分单元，被配置为执行对所述拼接字段进行拆分处理，得到所述第一加密密文对应的原始字段。

[0059] 在一示例性实施例中，所述字段获取单元，还被配置为执行获取所述第二数据请求中的字段的字段标识；从所述第二数据请求中的字段中，筛选出所述字段标识与目标字段标识相同的字段，并将所述字段识别为所述目标字段。

[0060] 在一示例性实施例中，所述请求接收单元，还被配置为执行通过预设的网络通道，接收终端发送的第二数据请求；所述第二数据请求由所述终端根据所述目标字段和第一数据请求中的剩余字段生成，所述目标字段由所述原始字段经过加密处理后得到，所述剩余字段为所述第一数据请求中除所述原始字段以外的字段，所述原始字段为所述第一数据请求中表示对象数据的字段。

[0061] 在一示例性实施例中，所述装置还包括密文识别单元，被配置为执行按照所述目标字段中的密文组合顺序，从所述目标字段中识别出所述第一加密密文和所述第二加密密文。

[0062] 在一示例性实施例中，所述装置还包括格式获取单元，被配置为执行获取所述密钥的格式；

[0063] 所述第二解密单元，还被配置为执行当所述密钥的格式与预设格式匹配时，根据所述密钥对所述第一加密密文进行解密处理，得到拼接字段。

[0064] 根据本公开实施例的第五方面，提供一种电子设备，包括：处理器；用于存储所述处理器可执行指令的存储器；其中，所述处理器被配置为执行所述指令，以实现如第一方面的任一项实施例中所述的数据处理方法。

[0065] 根据本公开实施例的第六方面，提供一种服务器，包括：处理器；用于存储所述处理器可执行指令的存储器；其中，所述处理器被配置为执行所述指令，以实现如第二方面的任一项实施例中所述的数据处理方法。

[0066] 根据本公开实施例的第七方面，提供一种计算机可读存储介质，当所述计算机可读存储介质中的指令由电子设备的处理器执行时，使得所述电子设备能够执行第一方面的任一项实施例中所述的数据处理方法。

[0067] 根据本公开实施例的第八方面，提供一种计算机可读存储介质，当所述计算机可读存储介质中的指令由服务器的处理器执行时，使得所述服务器能够执行第二方面的任一项实施例中所述的数据处理方法。

[0068] 根据本公开实施例的第九方面，提供一种计算机程序产品，所述计算机程序产品包括指令，所述指令被电子设备的处理器执行时，使得所述电子设备能够执行第一方面的任一项实施例中所述的数据处理方法。

[0069] 根据本公开实施例的第十方面，提供一种计算机程序产品，所述计算机程序产品包括指令，所述指令被服务器的处理器执行时，使得所述服务器能够执行第二方面的任一项实施例中所述的数据处理方法。

[0070] 本公开的实施例提供的技术方案至少带来以下有益效果：

[0071] 通过获取第一数据请求中的待加密字段，对待加密字段进行拼接处理，得到拼接字段；待加密字段为表示对象数据的字段；然后根据与拼接字段对应的密钥，对拼接字段进行加密处理，得到第一加密密文，以及根据预设公钥对密钥进行加密处理，得到第二加密密文；最后将第一加密密文和第二加密密文进行拼接处理，得到目标字段，并根据目标字段和第一数据请求中的剩余字段，生成第二数据请求，并将第二数据请求发送至服务器；剩余字段为第一数据请求中除待加密字段以外的字段；这样，实现了在进行数据请求的过程中，对数据请求中的字段进行加密的目的，避免了数据请求中的字段泄露，导致数据的安全性较低的缺陷，从而提高了数据的安全性。

[0072] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

[0073] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理，并不构成对本公开的不当限定。

[0074] 图1是根据一示例性实施例示出的一种数据处理方法的应用环境图。

[0075] 图2是根据一示例性实施例示出的一种数据处理方法的流程图。

[0076] 图3是根据一示例性实施例示出的另一种数据处理方法的流程图。

[0077] 图4是根据一示例性实施例示出的又一种数据处理方法的流程图。

[0078] 图5是根据一示例性实施例示出的一种数据处理装置的框图。

[0079] 图6是根据一示例性实施例示出的另一种数据处理装置的框图。

[0080] 图7是根据一示例性实施例示出的一种电子设备的框图。

[0081] 图8是根据一示例性实施例示出的一种服务器的框图。

具体实施方式

[0082] 为了使本领域普通人员更好地理解本公开的技术方案，下面将结合附图，对本公开实施例中的技术方案进行清楚、完整地描述。

[0083] 需要说明的是，本公开的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本公开的实施例能够以除了在这里图示或描述的那些以外的顺序实施。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

[0084] 还需要说明的是，本公开所涉及的用户信息(包括但不限于用户设备信息、用户个人信息等)和数据(包括但不限于用于展示的数据、分析的数据等)，均为经用户授权或者经过各方充分授权的信息和数据。

[0085] 本公开所提供的数据处理方法，可以应用于如图1所示的应用环境中。其中，终端110通过网络与服务器120进行交互。具体地，参考图1，终端110获取获取第一数据请求中的待加密字段，对待加密字段进行拼接处理，得到拼接字段；待加密字段为表示对象数据的字段；根据与拼接字段对应的密钥，对拼接字段进行加密处理，得到第一加密密文；根据预设公钥对密钥进行加密处理，得到第二加密密文；将第一加密密文和第二加密密文进行拼接处理，得到目标字段；根据目标字段和第一数据请求中的剩余字段，生成第二数据请求，并将第二数据请求发送至服务器；剩余字段为第一数据请求中除待加密字段以外的字段。其中，终端110可以但不限于是各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备，服务器120可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

[0086] 图2是根据一示例性实施例示出的一种数据处理方法的流程图，如图2所示，该数据处理方法用于如图1所示的终端中，包括以下步骤：

[0087] 在步骤S210中，获取第一数据请求中的待加密字段，对待加密字段进行拼接处理，

得到拼接字段;待加密字段为表示对象数据的字段。

[0088] 其中,第一数据请求是指携带有请求字段的请求,比如数据上报请求、接口请求、数据查询请求、业务数据请求等;在实际场景中,第一数据请求可以通过用户触发得到。第一数据请求中包括多个字段,比如待加密字段。

[0089] 其中,待加密字段是指第一数据请求中需要进行加密处理的字段,具体是指第一数据请求中表示对象数据的字段,比如用户ID、用户名称、业务信息等。需要说明的是,对象数据具体是指隐私数据,隐私数据是指与用户信息或者业务内部信息相关的数据。

[0090] 具体地,终端根据用于识别出表示对象数据的字段的指令,识别出第一数据请求中表示对象数据的字段,并将第一数据请求中表示对象数据的字段作为第一数据请求中的待加密字段;接着根据字段拼接指令,对第一数据请求中的待加密字段进行拼接处理,得到拼接字段。

[0091] 举例说明,终端获取数据上报请求中用于表示用户信息的字段A和用于表示业务内部信息的字段B,并将字段A和字段B进行拼接处理,得到拼接字段AB。

[0092] 在步骤S220中,根据与拼接字段对应的密钥,对拼接字段进行加密处理,得到第一加密密文。

[0093] 其中,与拼接字段对应的密钥,是指预设位数(比如11位)的随机密钥;针对每一个第一数据上报请求,与拼接字段对应的密钥都是不相同的。第一加密密文,是指通过密钥对拼接字段进行加密处理后得到的密文。

[0094] 具体地,终端获取与拼接字段对应的密钥,并根据该密钥对拼接字段进行对称加密处理,得到加密密文,将该加密密文作为第一加密密文。

[0095] 举例说明,终端根据密钥C对拼接字段AB进行加密处理,得到第一加密密文DEF。

[0096] 在步骤S230中,根据预设公钥对密钥进行加密处理,得到第二加密密文。

[0097] 其中,预设公钥是指约定的非对称密钥对中的终端公钥;第二加密密文,是指通过预设公钥对密钥进行加密处理后得到的密文。

[0098] 具体地,终端获取预设公钥,并根据预设公钥对密钥进行非对称加密处理,得到密钥密文,将该密钥密文作为第二加密密文。

[0099] 举例说明,终端根据终端公钥N对密钥C进行加密处理,得到第二加密密文HGI。

[0100] 在步骤S240中,将第一加密密文和第二加密密文进行拼接处理,得到目标字段。

[0101] 其中,目标字段由第一加密密文和第二加密密文拼接而成,具有固定的目标字段标识,比如M。

[0102] 具体地,终端将第一加密密文和第二加密密文组合在一起,得到组合密文,并将该组合密文作为目标字段。

[0103] 在步骤S250中,根据目标字段和第一数据请求中的剩余字段,生成第二数据请求,并将第二数据请求发送至服务器;剩余字段为第一数据请求中除待加密字段以外的字段。

[0104] 其中,第一数据请求中的剩余字段,是指第一数据请求中除待加密字段以外的字段;比如,第一数据请求中包括字段A、字段B、字段C和字段D,字段A和字段B均为待加密字段,则字段C和字段D为第一数据请求中的剩余字段。

[0105] 其中,第二数据请求,是指由目标字段和第一数据请求中的剩余字段所组成的数据请求。

[0106] 具体地，终端获取第一数据请求中除待加密字段以外的字段，并将其作为第一数据请求中的剩余字段；将目标字段和第一数据请求中的剩余字段，导入数据请求模板中，得到新的第一数据请求，并将其作为第二数据请求；将第二数据请求发送至对应的服务器，服务器根据接收到的第二数据请求，执行相应的数据处理。

[0107] 上述数据处理方法中，通过获取第一数据请求中的待加密字段，对待加密字段进行拼接处理，得到拼接字段；待加密字段为表示对象数据的字段；然后根据与拼接字段对应的密钥，对拼接字段进行加密处理，得到第一加密密文，以及根据预设公钥对密钥进行加密处理，得到第二加密密文；最后将第一加密密文和第二加密密文进行拼接处理，得到目标字段，并根据目标字段和第一数据请求中的剩余字段，生成第二数据请求，并将第二数据请求发送至服务器；剩余字段为第一数据请求中除待加密字段以外的字段；这样，实现了在进行数据请求的过程中，对数据请求中的字段进行加密的目的，避免了数据请求中的字段泄露，导致数据的安全性较低的缺陷，从而提高了数据的安全性。

[0108] 在一示例性实施例中，在步骤S210中，获取第一数据请求中的待加密字段，包括：获取第一数据请求中的字段的字段标识；若字段的字段标识与预设字段标识匹配，则将字段识别为第一数据请求中的待加密字段；预设字段标识为表示对象数据的字段的字段标识。

[0109] 其中，字段标识是指字段的唯一标识信息，比如字段名称。预设字段标识具体是指表示隐私数据的字段的字段标识，比如Name、ID、帐号、业务名称等。

[0110] 具体地，终端根据字段标识获取指令，获取第一数据请求中的字段的字段标识；然后将第一数据请求中的字段的字段标识与预设字段标识进行匹配，得到匹配结果；根据匹配结果，从第一数据请求中的字段中，筛选出字段标识与预设字段标识匹配的字段，作为第一数据请求中的待加密字段。

[0111] 举例说明，假设第一数据请求中的某个字段的字段标识为ID或者帐号，则将该字段识别为待加密字段。

[0112] 本公开实施例提供的技术方案，通过获取第一数据请求中的待加密字段，有利于后续对待加密字段进行加密，避免待加密字段泄露，从而提高了数据的安全性；同时，只获取第一数据请求中的待加密字段，有利于后续仅对待加密字段进行加密，避免了对第一数据请求中的所有字段进行加密，导致加密时间较长的缺陷。

[0113] 在一示例性实施例中，在步骤S210中，在对待加密字段进行拼接处理，得到拼接字段之前，还包括：获取验证文件；验证文件用于验证待加密字段是否为表示对象数据的字段；根据验证文件对待加密字段进行验证；那么，上述步骤S210中，对待加密字段进行拼接处理，得到拼接字段，包括：若待加密字段验证通过，则按照预设拼接顺序对待加密字段进行拼接处理，得到拼接字段。

[0114] 其中，验证文件是一种用于验证待加密字段是否为表示对象数据的字段的算法文件，具体是指一种用于验证待加密字段是否为表示隐私数据的字段的算法文件。待加密字段验证通过，说明待验证字段为表示对象数据的字段，进而说明待验证字段为表示隐私数据的字段；待加密字段验证不通过，说明待验证字段不是表示对象数据的字段，进而说明待验证字段不是表示隐私数据的字段。预设拼接顺序，是指预先设定的对待加密字段进行拼接处理的顺序，比如从左到右拼接、从右到左拼接等。

[0115] 具体地，终端从本地数据库中获取用于验证待加密字段是否为表示对象数据的字段的验证文件，并根据验证文件对第一数据请求中的待加密字段进行验证，以判断待加密字段是否为表示对象数据的字段；若待加密字段为表示对象数据的字段，则说明待加密字段验证通过，并按照预设拼接顺序，将待加密字段进行拼接处理，得到拼接字段。

[0116] 进一步地，若待加密字段不是表示对象数据的字段，则说明该待加密字段验证不通过，并通过终端对该待加密字段进行删除，得到第一数据请求中的目标待加密字段；按照预设拼接顺序，将目标待加密字段进行拼接处理，得到拼接字段。

[0117] 本公开实施例提供的技术方案，在根据验证文件对待加密字段验证通过的情况下，才按照预设拼接顺序对待加密字段进行拼接处理，得到拼接字段，有利于避免在获取第一数据请求中的待加密字段的过程中存在错误，导致获取的待加密字段不准确的缺陷，从而提高了最终得到的待加密字段的准确性。

[0118] 在一示例性实施例中，在步骤S240中，在将第一加密密文和第二加密密文进行拼接处理，得到目标字段之前，还包括：分别对第一加密密文和第二加密密文进行再次加密处理，得到第一加密密文对应的第三加密密文和第二加密密文对应的第四加密密文；那么，上述步骤S240中，将第一加密密文和第二加密密文进行拼接处理，得到目标字段，包括：将第一加密密文对应的第三加密密文和第二加密密文对应的第四加密密文进行拼接处理，得到目标字段。

[0119] 其中，第三加密密文是通过对第一加密密文进行再次加密处理后得到的密文，第四加密密文是通过对第二加密密文进行再次加密处理后得到的密文。

[0120] 需要说明的是，对第一加密密文和第二加密密文进行再次加密处理的方法可以是各种加密算法，比如对称加密算法、非对称加密算法等，具体本公开不做限定。

[0121] 具体地，终端从本地数据库中获取第一公钥，根据第一公钥对第一加密密文进行再次加密处理，得到再次加密处理后的密文，作为第一加密密文对应的第三加密密文；根据第一公钥对第二加密密文进行再次加密处理，得到再次加密处理后的密文，作为第二加密密文对应的第四加密密文；将第一加密密文对应的第三加密密文和第二加密密文对应的第四加密密文组合在一起，得到组合密文，并将该组合密文作为目标字段。

[0122] 本公开实施例提供的技术方案，对第一加密密文和第二加密密文进行再次加密处理后，再进行拼接，有利于提高得到的目标字段的安全性，进一步提高了数据的安全性。

[0123] 在一示例性实施例中，在步骤S220中，在根据与拼接字段对应的密钥，对拼接字段进行加密处理，得到第一加密密文之前，还包括：生成随机密钥，并将随机密钥识别为与拼接字段对应的密钥。

[0124] 其中，随机密钥可以是固定位数的随机密钥，也可以是指不固定位数的随机密钥，具体本公开不做限定。

[0125] 具体地，在对待加密字段进行拼接处理，得到拼接字段之后，终端根据随机密钥生成算法，生成一个随机密钥，并将该随机密钥识别为与该拼接字段对应的密钥。

[0126] 举例说明，在得到拼接字段之后，终端生成一个随机密钥ABDGEHJ，并将该随机密钥ABDGEHJ作为与该拼接字段对应的密钥。

[0127] 本公开实施例提供的技术方案，通过生成随机密钥，并将随机密钥识别为与拼接字段对应的密钥，有利于后续根据随机密钥对拼接字段进行加密处理，得到第一加密密文，

使得每次对拼接字段进行加密处理的密钥都不一样，进而使得加密得到的第一加密密文不容易被破解，从而提高了得到的第一加密密文的安全性，进一步提高了数据的安全性。

[0128] 图3是根据一示例性实施例示出的另一种数据处理方法的流程图，如图3所示，该数据处理方法用于如图1所示的服务器中，包括以下步骤：

[0129] 在步骤S310中，接收终端发送的第二数据请求。

[0130] 在步骤S320中，获取第二数据请求中的目标字段；目标字段由第一加密密文和第二加密密文组成，第二加密密文由预设公钥加密得到，第一加密密文由密钥加密得到。

[0131] 在步骤S330中，根据与预设公钥匹配的预设私钥，对第二加密密文进行解密处理，得到密钥。

[0132] 其中，预设私钥是指约定的非对称密钥对中的服务器私钥。

[0133] 在步骤S340中，根据密钥对第一加密密文进行解密处理，得到拼接字段。

[0134] 在步骤S350中，对拼接字段进行拆分处理，得到第一加密密文对应的原始字段。

[0135] 其中，第一加密密文对应的原始字段，是指第一数据请求中的各个待加密字段。

[0136] 具体地，服务器接收终端发送的第二数据请求，并根据目标字段获取指令，获取第二数据请求中的目标字段；对目标字段进行拆分处理，得到第一加密密文和第二加密密文；获取与预设公钥匹配的预设私钥，根据预设私钥对第二加密密文进行解密处理，得到对拼接字段进行加密的密钥；根据该密钥对第一加密密文进行解密处理，得到拼接字段；对拼接字段进行拆分处理，得到第一加密密文对应的各个原始字段，即第一查询请求中的各个待加密字段。

[0137] 需要说明的是，图3所示的数据处理方法的解密原理跟图2所示的数据处理方法的加密原理是一样的，故针对图3所示的数据处理方法中的各个步骤的具体限定，可以参考图2所示的数据处理方法中的各个步骤的具体限定，在此不再赘述。

[0138] 举例说明，客户端向服务端发送第一查询请求，第一查询请求中客户端对若干需要加密的字段进行拼接，得到拼接串Q，并通过一定位数的随机秘钥K对拼接串Q进行加密，得到加密密文X，接着使用约定的非对称秘钥对中的公钥P加密秘钥K得秘钥密文KS，对秘钥密文KS和加密密文X进行拼接，生成固定字段M；服务端接受第一查询请求，从字段M中拆分出秘钥密文KS和加密密文X，用约定的非对称秘钥对中的私钥A对秘钥密文KS进行解密，得秘钥K，使用秘钥K解密加密密文X，获得拼接串Q，分拆拼接串Q后得若干原始字段。

[0139] 上述数据处理方法中，通过接收终端发送的第二数据请求；获取第二数据请求中的目标字段；目标字段由第一加密密文和第二加密密文组成，第二加密密文由预设公钥加密得到，第一加密密文由密钥加密得到；根据与预设公钥匹配的预设私钥，对第二加密密文进行解密处理，得到密钥；根据密钥对第一加密密文进行解密处理，得到拼接字段；对拼接字段进行拆分处理，得到第一加密密文对应的原始字段；这样，实现了对第二数据请求中的目标字段进行解密处理的目的，可以避免数据被窃取，从而提高了数据的安全性。

[0140] 在一示例性实施例中，在步骤S320中，获取第二数据请求中的目标字段，具体包括：获取第二数据请求中的字段的字段标识；从第二数据请求中的字段中，筛选出字段标识与目标字段标识相同的字段，并将字段识别为目标字段。

[0141] 其中，目标字段标识是指目标字段的标识信息，针对所有的目标字段，目标字段标识都是一样的。

[0142] 具体地，服务器根据字段标识获取指令，获取第二数据请求中的字段的字段标识；然后将第二数据请求中的字段的字段标识与目标字段标识进行匹配，得到匹配结果；根据匹配结果，从第二数据请求中的字段中，筛选出字段标识与目标字段标识匹配的字段，作为第二数据请求中的目标字段。

[0143] 举例说明，第二数据请求中包括4个字段，分别是字段A、字段B、字段C和字段M，对应的字段标识分别是A1、B1、C1和M1，而目标字段标识为M1，与字段M的字段标识相同，则将字段M识别为第二数据请求中的目标字段。

[0144] 本公开实施例提供的技术方案，通过获取第二数据请求中的目标字段，有利于后续对目标字段中的第一加密密文和第二加密密文进行解密处理，得到第一加密密文对应的原始字段；同时，通过将第二数据请求中的字段的字段标识与目标字段标识进行匹配，有利于提高第二数据请求中的目标字段的确定准确率。

[0145] 在一示例性实施例中，在步骤S310中，接收终端发送的第二数据请求，具体包括：通过预设的网络通道，接收终端发送的第二数据请求；第二数据请求由终端根据目标字段和第一数据请求中的剩余字段生成，目标字段由原始字段经过加密处理后得到，剩余字段为第一数据请求中除原始字段以外的字段，原始字段为第一数据请求中表示对象数据的字段。

[0146] 其中，预设的网络通道是指专门的网络通道，比如私有网络通道。

[0147] 具体地，终端对第一数据请求中表示对象数据的原始字段进行加密处理，得到第一加密密文和第二加密密文，将第一加密密文和第二加密密文进行拼接处理，得到目标字段；获取第一数据请求中除原始字段以外的字段，并将其作为第一数据请求中的剩余字段；根据目标字段和第一数据请求中的剩余字段，生成第一数据请求，并通过预设的网络通道，将第一数据请求发送至服务器；服务器通过预设的网络通道，接收终端发送的第一数据请求。

[0148] 本公开实施例提供的技术方案，通过终端根据第一数据请求中表示对象数据的原始字段经过加密后得到的目标字段和第一数据请求中除原始字段以外的剩余字段，生成第二数据请求，并将第二数据请求通过预设的网络通道发送至对应的服务器，有利于避免数据泄露，进一步提高了数据的安全性。

[0149] 在一示例性实施例中，上述步骤S330，在根据与预设公钥匹配的预设私钥，对第二加密密文进行解密处理，得到密钥之前，还包括：按照目标字段中的密文组合顺序，从目标字段中识别出第一加密密文和第二加密密文。

[0150] 其中，目标字段由第一加密密文和第二加密密文，按照密文组合顺序所组合而成，比如第一加密密文在前，第二加密密文在后，或者第二加密密文在前，第一加密密文在后。密文组合顺序是指第一加密密文和第二加密密文的组合顺序。

[0151] 举例说明，假设目标字段中的密文组合顺序为第一加密密文在前，第二加密密文在后，则服务器按照该密文组合顺序，分别将目标字段中的第一段密文和第二段密文识别为第一加密密文和第二加密密文；假设目标字段中的密文组合顺序为第二加密密文在前，第一加密密文在后，则服务器按照该密文组合顺序，分别将目标字段中的第一段密文和第二段密文识别为第二加密密文和第一加密密文。

[0152] 本公开实施例提供的技术方案，按照目标字段中的密文组合顺序对目标字段中的

密文进行识别，有利于从目标字段中准确识别出第一加密密文和第二加密密文，同时有利于后续根据与预设公钥匹配的预设私钥，对第二加密密文进行解密处理，得到密钥，进而根据密钥对第一加密密文进行解密处理，得到拼接字段。

[0153] 在一示例性实施例中，上述步骤S340，在根据密钥对第一加密密文进行解密处理，得到拼接字段之前，还包括：获取密钥的格式；那么，上述步骤S340，根据密钥对第一加密密文进行解密处理，得到拼接字段，具体包括：当密钥的格式与预设格式匹配时，根据密钥对第一加密密文进行解密处理，得到拼接字段。

[0154] 其中，预设格式是指预先设置的密钥格式，比如总共有11位，前5位为数字，后6位为字母。密钥的格式与预设格式匹配，是指密钥的格式与预设格式相同。

[0155] 具体地，服务器通过密钥格式获取指令，获取密钥的格式，并判断密钥的格式与预设格式是否匹配；当密钥的格式与预设格式匹配时，则根据密钥对第一加密密文进行解密处理，得到拼接字段；当密钥的格式与预设格式不匹配时，说明得到的密钥存在错误，需要重新获取密钥，以保证得到的密钥的格式与预设格式匹配。

[0156] 举例说明，比如得到的密钥A的格式为：总共有11位，前5位为数字，后6位为字母，而预设格式为：总共有11位，前5位为数字，后6位为字母，则说明密钥A的格式与预设格式匹配，并根据密钥A对第一加密密文进行解密处理，得到拼接字段。

[0157] 本公开实施例提供的技术方案，当密钥的格式与预设格式匹配时，根据密钥对第一加密密文进行解密处理，得到拼接字段，有利于提高得到的拼接字段的准确性和安全性，进一步提高了数据的安全性。

[0158] 为了更清晰阐明本公开实施例提供的数据处理方法，以下以一个具体的实施例对该数据处理方法进行具体说明。在一个实施例中，如图4所示，本公开还提供了另一种数据处理方法，具体包括以下内容：

[0159] 客户端过滤请求中需要加密的字段；客户端对这些字段进行拼接，得到拼接串；客户端使用随机秘钥对拼接串进行对称加密，得到加密密文；客户端使用约定的客户端公钥对上一步使用的随机秘钥进行加密，得到秘钥密文；客户端对秘钥密文和加密密文进行拼接，生成固定请求字段M；客户端发送请求至服务端；服务端收到请求后，对M字段进行拆分，得到秘钥密文和加密密文；服务端使用约定的服务端私钥，对秘钥密文进行对称解密，得到秘钥；服务端使用上一步得到的秘钥对加密密文进行解密，得到拼接串；服务端对拼接串进行拆分，得到若干原始字段。

[0160] 上述数据处理方法，可以达到以下技术效果：(1)有利于保护业务安全，以及保护用户的隐私数据，从而提高了数据安全性；(2)本方法是通用方法，在客户端和服务端接入层进行统一接入，可以实现对业务的无侵入和无感知。

[0161] 应该理解的是，虽然图2-图3的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，图2-图3中的至少一部分步骤可以包括多个步骤或者多个阶段，这些步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

[0162] 可以理解的是，本说明书中上述方法的各个实施例之间相同/相似的部分可互相参见，每个实施例重点说明的是与其他实施例的不同之处，相关之处参见其他方法实施例的说明即可。

[0163] 图5是根据一示例性实施例示出的一种数据处理装置的框图。参照图5，该装置包括字段拼接单元510，第一加密单元520，第二加密单元530，密文拼接单元540和请求发送单元550。

[0164] 字段拼接单元510，被配置为执行获取第一数据请求中的待加密字段，对待加密字段进行拼接处理，得到拼接字段；待加密字段为表示对象数据的字段。

[0165] 第一加密单元520，被配置为执行根据与拼接字段对应的密钥，对拼接字段进行加密处理，得到第一加密密文。

[0166] 第二加密单元530，被配置为执行根据预设公钥对密钥进行加密处理，得到第二加密密文。

[0167] 密文拼接单元540，被配置为执行将第一加密密文和第二加密密文进行拼接处理，得到目标字段。

[0168] 请求发送单元550，被配置为执行根据目标字段和第一数据请求中的剩余字段，生成第二数据请求，并将第二数据请求发送至服务器；剩余字段为第一数据请求中除待加密字段以外的字段。

[0169] 在一示例性实施例中，字段拼接单元510，还被配置为执行获取第一数据请求中的字段的字段标识；若字段的字段标识与预设字段标识匹配，则将字段识别为第一数据请求中的待加密字段；预设字段标识为表示对象数据的字段的字段标识。

[0170] 在一示例性实施例中，数据处理装置还包括字段验证单元，被配置为执行获取验证文件；验证文件用于验证待加密字段是否为表示对象数据的字段；根据验证文件对待加密字段进行验证；

[0171] 字段拼接单元510，还被配置为执行若待加密字段验证通过，则按照预设拼接顺序对待加密字段进行拼接处理，得到拼接字段。

[0172] 在一示例性实施例中，数据处理装置还包括密文加密单元，被配置为执行分别对第一加密密文和第二加密密文进行再次加密处理，得到第一加密密文对应的第三加密密文和第二加密密文对应的第四加密密文；

[0173] 密文拼接单元540，还被配置为执行将第一加密密文对应的第三加密密文和第二加密密文对应的第四加密密文进行拼接处理，得到目标字段。

[0174] 在一示例性实施例中，数据处理装置还包括密钥获取单元，被配置为执行生成随机密钥，并将随机密钥识别为与拼接字段对应的密钥。

[0175] 图6是根据一示例性实施例示出的另一种数据处理装置的框图。参照图6，该装置包括请求接收单元610，字段获取单元620，第一解密单元630，第二解密单元640和字段拆分单元650。

[0176] 请求接收单元610，被配置为执行接收终端发送的第二数据请求。

[0177] 字段获取单元620，被配置为执行获取第二数据请求中的目标字段；目标字段由第一加密密文和第二加密密文组成，第二加密密文由预设公钥加密得到，第一加密密文由密钥加密得到。

[0178] 第一解密单元630，被配置为执行根据与预设公钥匹配的预设私钥，对第二加密密文进行解密处理，得到密钥。

[0179] 第二解密单元640，被配置为执行根据密钥对第一加密密文进行解密处理，得到拼接字段。

[0180] 字段拆分单元650，被配置为执行对拼接字段进行拆分处理，得到第一加密密文对应的原始字段。

[0181] 在一示例性实施例中，字段获取单元620，还被配置为执行获取第二数据请求中的字段的字段标识；从第二数据请求中的字段中，筛选出字段标识与目标字段标识相同的字段，并将字段识别为目标字段。

[0182] 在一示例性实施例中，请求接收单元，还被配置为执行通过预设的网络通道，接收终端发送的第二数据请求；第二数据请求由终端根据目标字段和第一数据请求中的剩余字段生成，目标字段由原始字段经过加密处理后得到，剩余字段为第一数据请求中除原始字段以外的字段，原始字段为第一数据请求中表示对象数据的字段。

[0183] 在一示例性实施例中，数据处理装置还包括密文识别单元，被配置为执行按照目标字段中的密文组合顺序，从目标字段中识别出第一加密密文和第二加密密文。

[0184] 在一示例性实施例中，数据处理装置还包括格式获取单元，被配置为执行获取密钥的格式；

[0185] 第二解密单元，还被配置为执行当密钥的格式与预设格式匹配时，根据密钥对第一加密密文进行解密处理，得到拼接字段。

[0186] 关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

[0187] 图7是根据一示例性实施例示出的一种用于执行数据处理方法的电子设备700的框图。例如，电子设备700可以是移动电话、计算机、数字广播终端、消息收发设备、游戏控制台、平板设备、医疗设备、健身设备、个人数字助理等。

[0188] 参照图7，电子设备700可以包括以下一个或多个组件：处理组件702、存储器704、电源组件706、多媒体组件708、音频组件710、输入/输出(I/O)的接口712、传感器组件714以及通信组件716。

[0189] 处理组件702通常控制电子设备700的整体操作，诸如与显示、电话呼叫、数据通信、相机操作和记录操作相关联的操作。处理组件702可以包括一个或多个处理器720来执行指令，以完成上述的方法的全部或部分步骤。此外，处理组件702可以包括一个或多个模块，便于处理组件702和其他组件之间的交互。例如，处理组件702可以包括多媒体模块，以方便多媒体组件708和处理组件702之间的交互。

[0190] 存储器704被配置为存储各种类型的数据以支持在电子设备700的操作。这些数据的示例包括用于在电子设备700上操作的任何应用程序或方法的指令、联系人数据、电话簿数据、消息、图片、视频等。存储器704可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器(SRAM)、电可擦除可编程只读存储器(EEPROM)、可擦除可编程只读存储器(EPROM)、可编程只读存储器(PROM)、只读存储器(ROM)、磁存储器、快闪存储器、磁盘、光盘或石墨烯存储器。

[0191] 电源组件706为电子设备700的各种组件提供电力。电源组件706可以包括电源管

理系统，一个或多个电源，及其他与为电子设备700生成、管理和分配电力相关联的组件。

[0192] 多媒体组件708包括在所述电子设备700和用户之间的提供输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器(LCD)和触摸面板(TP)。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件708包括前置摄像头和/或后置摄像头。当电子设备700处于操作模式，如拍摄模式或视频模式时，前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是固定的光学透镜系统或具有焦距和光学变焦能力。

[0193] 音频组件710被配置为输出和/或输入音频信号。例如，音频组件710包括麦克风(MIC)，当电子设备700处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器704或经由通信组件716发送。在一些实施例中，音频组件710还包括扬声器，用于输出音频信号。

[0194] I/O接口712为处理组件702和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

[0195] 传感器组件714包括一个或多个传感器，用于为电子设备700提供各个方面的状态评估。例如，传感器组件714可以检测到电子设备700的打开/关闭状态，组件的相对定位，例如所述组件为电子设备700的显示器和小键盘，传感器组件714还可以检测电子设备700或电子设备700组件的位置改变，用户与电子设备700接触的存在或不存在，电子设备700方位或加速/减速和电子设备700的温度变化。传感器组件714可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件714还可以包括光传感器，如CMOS或CCD图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件714还可以包括加速度传感器、陀螺仪传感器、磁传感器、压力传感器或温度传感器。

[0196] 通信组件716被配置为便于电子设备700和其他设备之间有线或无线方式的通信。电子设备700可以接入基于通信标准的无线网络，如WiFi，运营商网络(如2G、3G、4G或5G)，或它们的组合。在一个示例性实施例中，通信组件716经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件716还包括近场通信(NFC)模块，以促进短程通信。例如，在NFC模块可基于射频识别(RFID)技术，红外数据协会(IrDA)技术，超宽带(UWB)技术，蓝牙(BT)技术和其他技术来实现。

[0197] 在示例性实施例中，电子设备700可以被一个或多个应用专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述方法。

[0198] 在示例性实施例中，还提供了一种包括指令的计算机可读存储介质，例如包括指令的存储器704，上述指令可由电子设备700的处理器720执行以完成上述方法。例如，计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0199] 在示例性实施例中，还提供一种计算机程序产品，所述计算机程序产品中包括指令，上述指令可由电子设备700的处理器720执行以完成上述方法。

[0200] 图8是根据一示例性实施例示出的一种用于执行数据处理方法的设备800的框图。例如，设备800可以为服务器。参照图8，设备800包括处理组件820，其进一步包括一个或多个处理器，以及由存储器822所代表的存储器资源，用于存储可由处理组件820的执行的指令，例如应用程序。存储器822中存储的应用程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理组件820被配置为执行指令，以执行上述方法。

[0201] 设备800还可以包括：电源组件824被配置为执行设备800的电源管理，有线或无线网络接口826被配置为将设备800连接到网络，和输入输出(I/O)接口828。设备800可以操作基于存储在存储器822的操作系统，例如Windows Server，Mac OS X，Unix，Linux，FreeBSD或类似。

[0202] 在示例性实施例中，还提供了一种包括指令的计算机可读存储介质，例如包括指令的存储器822，上述指令可由设备800的处理器执行以完成上述方法。存储介质可以是计算机可读存储介质，例如，所述计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0203] 在示例性实施例中，还提供一种计算机程序产品，所述计算机程序产品中包括指令，上述指令可由设备800的处理器执行以完成上述方法。

[0204] 需要说明的，上述的装置、电子设备、服务器、计算机可读存储介质、计算机程序产品等根据方法实施例的描述还可以包括其他的实施方式，具体的实现方式可以参照相关方法实施例的描述，在此不作一一赘述。

[0205] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本公开的其它实施方案。本公开旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由权利要求指出。

[0206] 应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

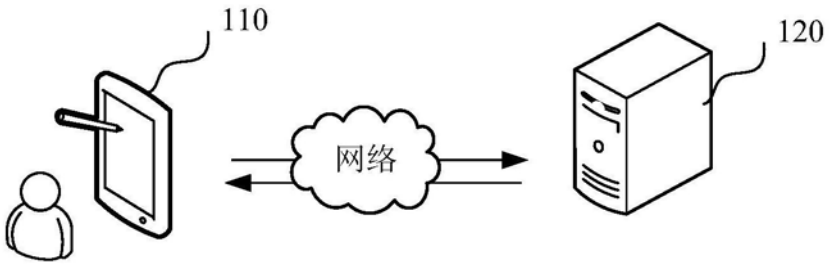

110
120
网络

图1

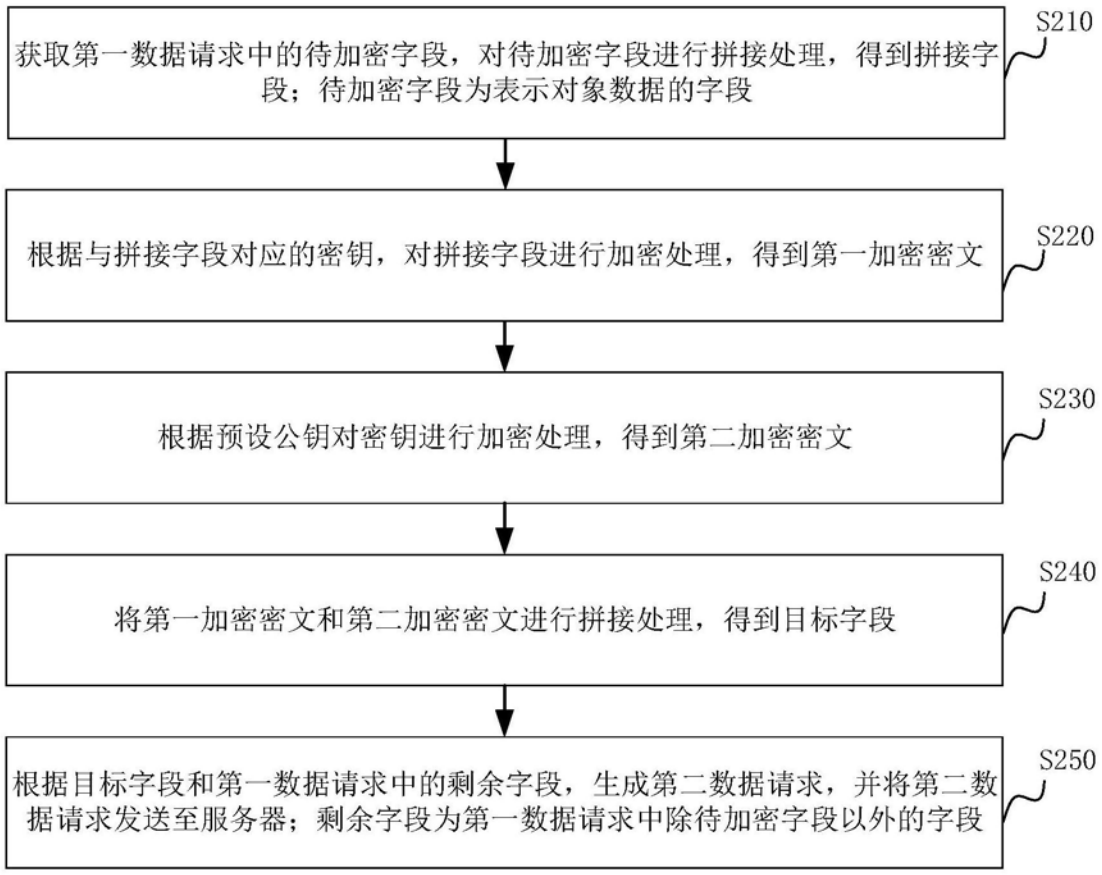

获取第一数据请求中的待加密字段，对待加密字段进行拼接处理，得到拼接字段；待加密字段为表示对象数据的字段
S210
根据与拼接字段对应的密钥，对拼接字段进行加密处理，得到第一加密密文
S220
根据预设公钥对密钥进行加密处理，得到第二加密密文
S230
将第一加密密文和第二加密密文进行拼接处理，得到目标字段
S240
根据目标字段和第一数据请求中的剩余字段，生成第二数据请求，并将第二数据请求发送至服务器；剩余字段为第一数据请求中除待加密字段以外的字段
S250

图2

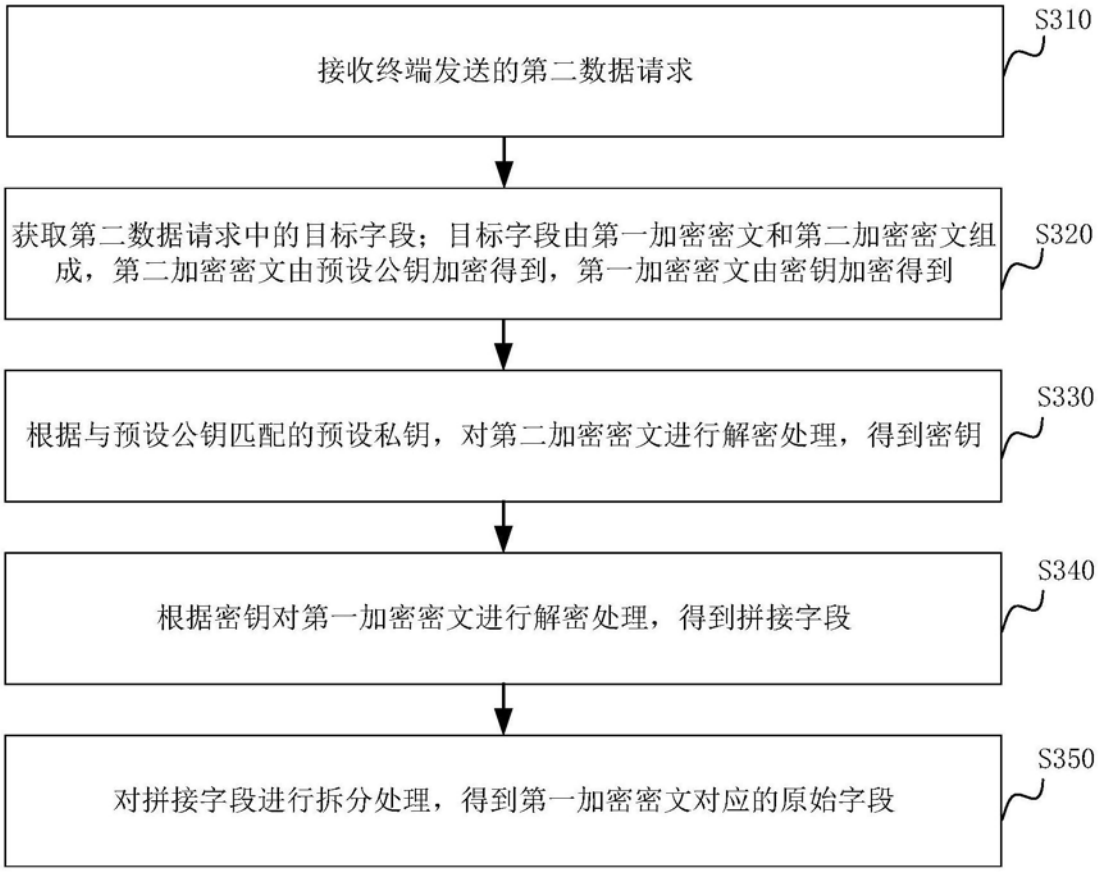

接收终端发送的第二数据请求
S310
获取第二数据请求中的目标字段；目标字段由第一加密密文和第二加密密文组成，第二加密密文由预设公钥加密得到，第一加密密文由密钥加密得到
S320
根据与预设公钥匹配的预设私钥，对第二加密密文进行解密处理，得到密钥
S330
根据密钥对第一加密密文进行解密处理，得到拼接字段
S340
对拼接字段进行拆分处理，得到第一加密密文对应的原始字段
S350

图3

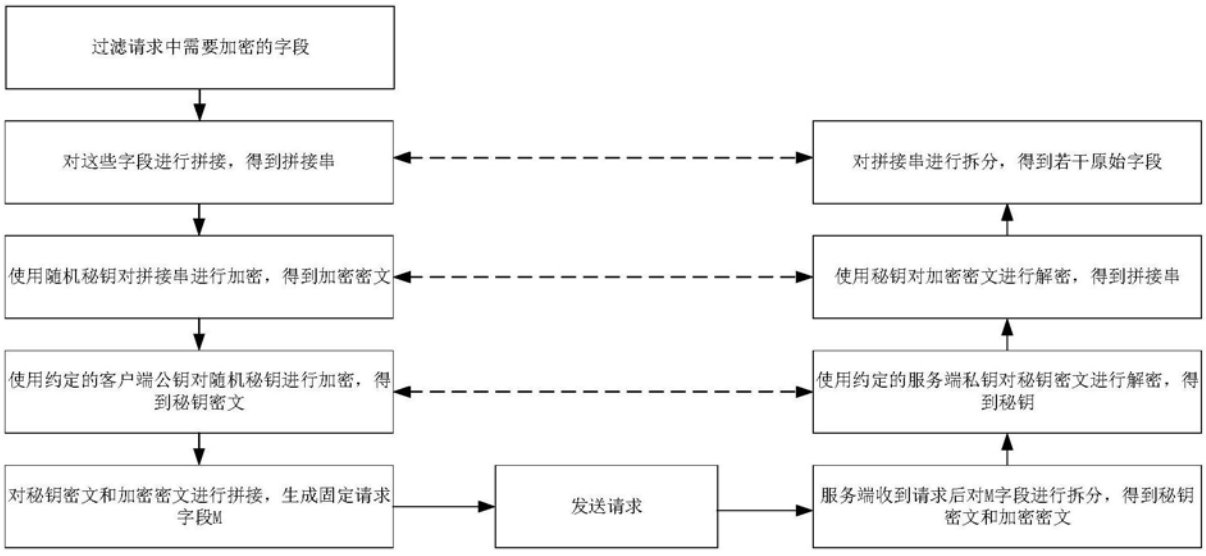

过滤请求中需要加密的字段
对这些字段进行拼接，得到拼接串
使用随机秘钥对拼接串进行加密，得到加密密文
使用约定的客户端公钥对随机秘钥进行加密，得到秘钥密文
对秘钥密文和加密密文进行拼接，生成固定请求字段M
发送请求
服务端收到请求后对M字段进行拆分，得到秘钥密文和加密密文
使用约定的服务端私钥对秘钥密文进行解密，得到秘钥
使用秘钥对加密密文进行解密，得到拼接串
对拼接串进行拆分，得到若干原始字段

图4

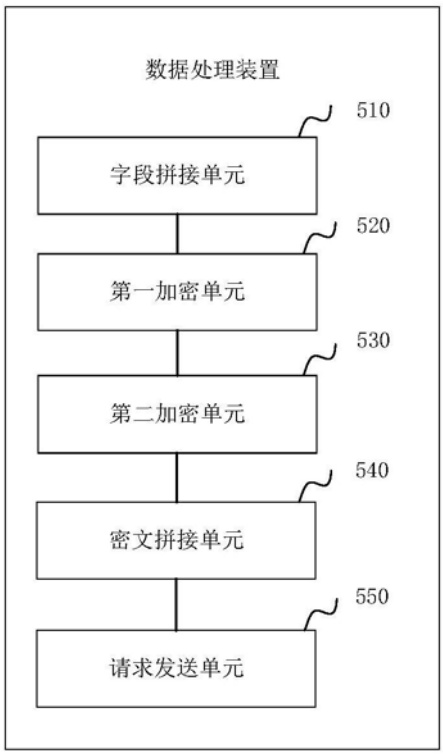

数据处理装置
510
字段拼接单元
520
第一加密单元
530
第二加密单元
540
密文拼接单元
550
请求发送单元

图5

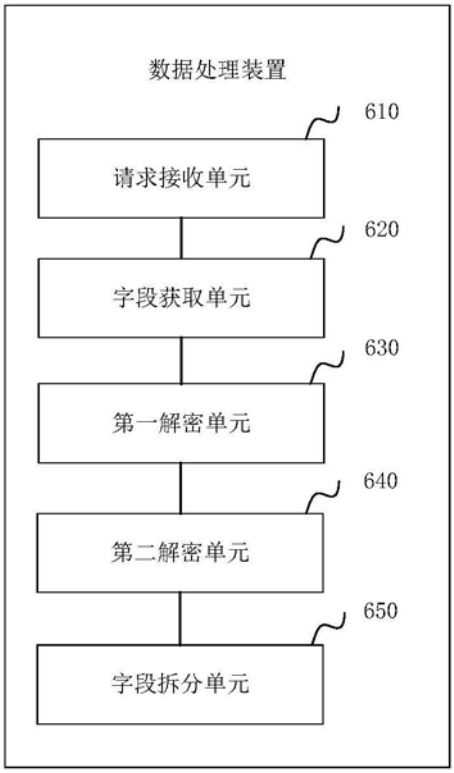

数据处理装置
610
请求接收单元
620
字段获取单元
630
第一解密单元
640
第二解密单元
650
字段拆分单元

图6

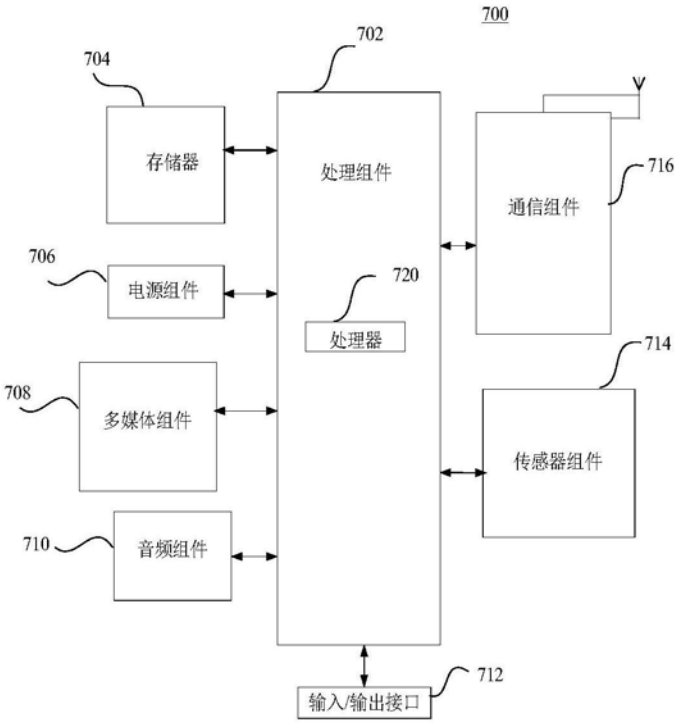

700
702
704
存储器
处理组件
通信组件
716
706
电源组件
720
处理器
714
708
多媒体组件
传感器组件
710
音频组件
712
输入/输出接口

图7

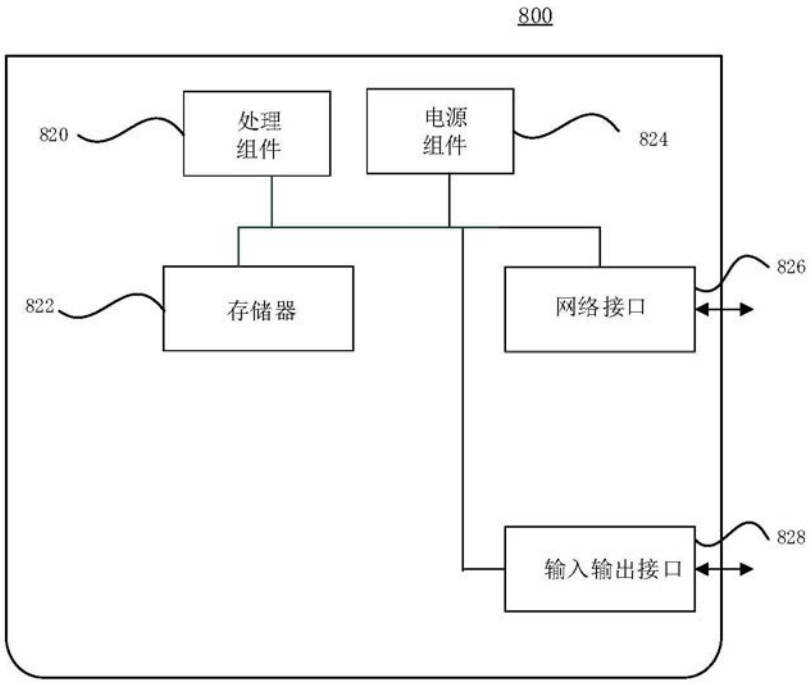

800
820
处理
组件
电源
组件
824
822
存储器
网络接口
826
输入输出接口
828

图8