(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116383867 A
(43)申请公布日 2023.07.04

(21)申请号 202310118592.6

(22)申请日 2023.01.30

(71)申请人 北京京东拓先科技有限公司
地址 100176 北京市大兴区北京经济技术开发区科创十一街18号院1号楼7层701室

(72)发明人 李冬雪

(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
专利代理师 李阳 徐敏

(51)Int.Cl.
G06F 21/62(2013.01)
G16H 10/60(2018.01)
G16H 50/70(2018.01)

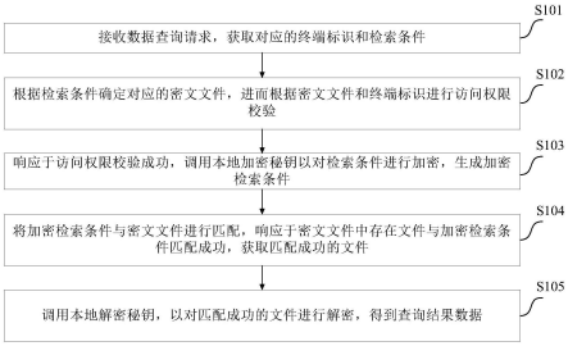
权利要求书2页 说明书12页 附图3页

(54)发明名称

一种数据查询方法、装置、电子设备及计算机可读介质

(57)摘要

本申请公开了数据查询方法、装置、电子设备及计算机可读介质，涉及互联网医疗技术领域，一具体实施方式包括接收数据查询请求，获取对应的终端标识和检索条件；根据检索条件确定对应的密文文件，进而根据密文文件和终端标识进行访问权限校验；响应于访问权限校验成功，调用本地加密秘钥以对检索条件进行加密，生成加密检索条件；加密检索条件与密文文件进行匹配，响应于密文文件中存在文件与加密检索条件匹配成功，获取匹配成功的文件；调用本地解密秘钥，以对匹配成功的文件进行解密，得到查询结果数据。以提高用户信息的安全性，有效防止用户信息被泄漏。



CN 116383867 A

1.一种数据查询方法,其特征在于,包括:

接收数据查询请求,获取对应的终端标识和检索条件;

根据所述检索条件确定对应的密文文件,进而根据所述密文文件和所述终端标识进行访问权限校验;

响应于访问权限校验成功,调用本地加密秘钥以对所述检索条件进行加密,生成加密检索条件;

将所述加密检索条件与所述密文文件进行匹配,响应于所述密文文件中存在文件与所述加密检索条件匹配成功,获取匹配成功的文件;

调用本地解密秘钥,以对所述匹配成功的文件进行解密,得到查询结果数据。

2.根据权利要求1所述的方法,其特征在于,在所述根据所述检索条件确定对应的密文文件之前,所述方法还包括:

获取历史用户信息和历史检索条件;

根据所述历史用户信息确定对应的用户标识,并将所述用户标识和所述历史用户信息映射至目标对象;

对所述目标对象中的字符串类型的属性进行加密,以得到第一加密数据;

基于信息摘要算法对所述第一加密数据进行加密计算,以得到第二加密数据;

基于所述历史检索条件和所述第二加密数据,生成密文文件。

3.根据权利要求2所述的方法,其特征在于,所述基于所述历史检索条件和所述第二加密数据,生成密文文件,包括:

根据所述历史检索条件,确定目标访问地址;

调用字符串哈希函数,以基于所述目标访问地址,计算得到对应的哈希值;

基于所述哈希值,确定字符串位数,进而基于所述字符串位数,生成目标字符串并确定字符串间隔;

基于所述第二加密数据、所述字符串间隔和所述目标字符串,生成密文文件。

4.根据权利要求3所述的方法,其特征在于,所述基于所述第二加密数据、所述字符串间隔和所述目标字符串,生成密文文件,包括:

将所述第二加密数据进行取余计算,得到取余计算结果,进而基于所述取余计算结果和所述字符串间隔,生成第一变换加密数据;

基于所述字符串间隔向所述第一变换加密数据中添加所述目标字符串中的字符,以得到第二变换加密数据;

生成一个随机数,进而基于所述随机数、所述字符串间隔和所述第二变换加密数据,生成密文文件。

5.根据权利要求4所述的方法,其特征在于,所述基于所述随机数、所述字符串间隔和所述第二变换加密数据,生成密文文件,包括:

基于所述随机数对所述第二变换加密数据执行数据翻转操作,以生成第三变换加密数据;

根据所述随机数,生成随机串,进而将所述随机串添加至所述第三变换加密数据的尾部,将所述随机数和所述字符串间隔添加至所述第三变换加密数据的首部;

获取解析规则的序号,进而将所述序号添加至所述第三变换加密数据的尾部,以生成

第四变换加密数据；

基于所述第四变换加密数据，得到密文文件。

6.根据权利要求2所述的方法，其特征在于，所述获取历史用户信息，包括：

获取原始用户信息，对所述原始用户信息进行掩码处理，以得到历史用户信息并获取所述历史用户信息。

7.根据权利要求2所述的方法，其特征在于，所述获取匹配成功的文件，包括：

查找所述密文文件中是否存在与所述加密检索条件相匹配的字符串，若是则遍历所述密文文件的字节数组，得到匹配子串列表，将所述匹配子串列表中每一个元素与所述用户标识对应的密文做差，进而得到匹配成功的文件，若否则返回匹配失败信息。

8.一种数据查询装置，其特征在于，包括：

接收单元，被配置成接收数据查询请求，获取对应的终端标识和检索条件；

校验单元，被配置成根据所述检索条件确定对应的密文文件，进而根据所述密文文件和所述终端标识进行访问权限校验；

加密单元，被配置成响应于访问权限校验成功，调用本地加密秘钥以对所述检索条件进行加密，生成加密检索条件；

匹配单元，被配置成将所述加密检索条件与所述密文文件进行匹配，响应于所述密文文件中存在文件与所述加密检索条件匹配成功，获取匹配成功的文件；

解密单元，被配置成调用本地解密秘钥，以对所述匹配成功的文件进行解密，得到查询结果数据。

9.一种数据查询电子设备，其特征在于，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-7中任一所述的方法。

10.一种计算机可读介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现如权利要求1-7中任一所述的方法。

一种数据查询方法、装置、电子设备及计算机可读介质

技术领域

[0001] 本申请涉及互联网医疗技术领域，尤其涉及一种数据查询方法、装置、电子设备及计算机可读介质。

背景技术

[0002] 目前，互联网医疗作为以互联网为载体和技术手段，开展在线健康教育、医疗信息咨询、远程诊断或会诊、电子处方、电子健康档案等多种形式的健康医疗信息服务的新兴产业，在近几年取得了飞速发展。一方面，互联网医疗在解决医疗资源供需失衡，加速行业竞争，推动医疗服务体系创新，深化医疗改革等方面提供了新的解决途径；另一方面，互联网医疗场景中需要对患者信息进行处理，患者信息的信息安全和隐私管理是当前亟需关注的重点。

发明内容

[0003] 有鉴于此，本申请实施例提供一种数据查询方法、装置、电子设备及计算机可读介质，能够加强对患者信息的保护力度，患者信息更安全。

[0004] 为实现上述目的，根据本申请实施例的一个方面，提供了一种数据查询方法，包括：

[0005] 接收数据查询请求，获取对应的终端标识和检索条件；

[0006] 根据检索条件确定对应的密文文件，进而根据密文文件和终端标识进行访问权限校验；

[0007] 响应于访问权限校验成功，调用本地加密秘钥以对检索条件进行加密，生成加密检索条件；

[0008] 将加密检索条件与密文文件进行匹配，响应于密文文件中存在文件与加密检索条件匹配成功，获取匹配成功的文件；

[0009] 调用本地解密秘钥，以对匹配成功的文件进行解密，得到查询结果数据。

[0010] 可选地，在根据检索条件确定对应的密文文件之前，方法还包括：

[0011] 获取历史用户信息和历史检索条件；

[0012] 根据历史用户信息确定对应的用户标识，并将用户标识和历史用户信息映射至目标对象；

[0013] 对目标对象中的字符串类型的属性进行加密，以得到第一加密数据；

[0014] 基于信息摘要算法对第一加密数据进行加密计算，以得到第二加密数据；

[0015] 基于历史检索条件和第二加密数据，生成密文文件。

[0016] 可选地，基于历史检索条件和第二加密数据，生成密文文件，包括：

[0017] 根据历史检索条件，确定目标访问地址；

[0018] 调用字符串哈希函数，以基于目标访问地址，计算得到对应的哈希值；

[0019] 基于哈希值，确定字符串位数，进而基于字符串位数，生成目标字符串并确定字符

串间隔；

[0020] 基于第二加密数据、字符串间隔和目标字符串，生成密文文件。

[0021] 可选地，基于第二加密数据、字符串间隔和目标字符串，生成密文文件，包括：

[0022] 将第二加密数据进行取余计算，得到取余计算结果，进而基于取余计算结果和字符串间隔，生成第一变换加密数据；

[0023] 基于字符串间隔向第一变换加密数据中添加目标字符串中的字符，以得到第二变换加密数据；

[0024] 生成一个随机数，进而基于随机数、字符串间隔和第二变换加密数据，生成密文文件。

[0025] 可选地，基于随机数、字符串间隔和第二变换加密数据，生成密文文件，包括：

[0026] 基于随机数对第二变换加密数据执行数据翻转操作，以生成第三变换加密数据；

[0027] 根据随机数，生成随机串，进而将随机串添加至第三变换加密数据的尾部，将随机数和字符串间隔添加至第三变换加密数据的首部；

[0028] 获取解析规则的序号，进而将序号添加至第三变换加密数据的尾部，以生成第四变换加密数据；

[0029] 基于第四变换加密数据，得到密文文件。

[0030] 可选地，获取历史用户信息，包括：

[0031] 获取原始用户信息，对原始用户信息进行掩码处理，以得到历史用户信息并获取历史用户信息。

[0032] 可选地，获取匹配成功的文件，包括：

[0033] 查找密文文件中是否存在与加密检索条件相匹配的字符串，若是则遍历密文文件的字节数组，得到匹配子串列表，将匹配子串列表中每一个元素与用户标识对应的密文做差，进而得到匹配成功的文件，若否则返回匹配失败信息。

[0034] 另外，本申请还提供了一种数据查询装置，包括：

[0035] 接收单元，被配置成接收数据查询请求，获取对应的终端标识和检索条件；

[0036] 校验单元，被配置成根据检索条件确定对应的密文文件，进而根据密文文件和终端标识进行访问权限校验；

[0037] 加密单元，被配置成响应于访问权限校验成功，调用本地加密秘钥以对检索条件进行加密，生成加密检索条件；

[0038] 匹配单元，被配置成将加密检索条件与密文文件进行匹配，响应于密文文件中存在文件与加密检索条件匹配成功，获取匹配成功的文件；

[0039] 解密单元，被配置成调用本地解密秘钥，以对匹配成功的文件进行解密，得到查询结果数据。

[0040] 可选地，数据查询装置还包括密文文件生成单元，被配置成：

[0041] 获取历史用户信息和历史检索条件；

[0042] 根据历史用户信息确定对应的用户标识，并将用户标识和历史用户信息映射至目标对象；

[0043] 对目标对象中的字符串类型的属性进行加密，以得到第一加密数据；

[0044] 基于信息摘要算法对第一加密数据进行加密计算，以得到第二加密数据；

[0045] 基于历史检索条件和第二加密数据，生成密文文件。

[0046] 可选地，密文文件生成单元进一步被配置成：

[0047] 根据历史检索条件，确定目标访问地址；

[0048] 调用字符串哈希函数，以基于目标访问地址，计算得到对应的哈希值；

[0049] 基于哈希值，确定字符串位数，进而基于字符串位数，生成目标字符串并确定字符串间隔；

[0050] 基于第二加密数据、字符串间隔和目标字符串，生成密文文件。

[0051] 可选地，密文文件生成单元进一步被配置成：

[0052] 将第二加密数据进行取余计算，得到取余计算结果，进而基于取余计算结果和字符串间隔，生成第一变换加密数据；

[0053] 基于字符串间隔向第一变换加密数据中添加目标字符串中的字符，以得到第二变换加密数据；

[0054] 生成一个随机数，进而基于随机数、字符串间隔和第二变换加密数据，生成密文文件。

[0055] 可选地，密文文件生成单元进一步被配置成：

[0056] 基于随机数对第二变换加密数据执行数据翻转操作，以生成第三变换加密数据；

[0057] 根据随机数，生成随机串，进而将随机串添加至第三变换加密数据的尾部，将随机数和字符串间隔添加至第三变换加密数据的首部；

[0058] 获取解析规则的序号，进而将序号添加至第三变换加密数据的尾部，以生成第四变换加密数据；

[0059] 基于第四变换加密数据，得到密文文件。

[0060] 可选地，密文文件生成单元进一步被配置成：

[0061] 获取原始用户信息，对原始用户信息进行掩码处理，以得到历史用户信息并获取历史用户信息。

[0062] 可选地，匹配单元进一步被配置成：

[0063] 查找密文文件中是否存在与加密检索条件相匹配的字符串，若是则遍历密文文件的字节数组，得到匹配子串列表，将匹配子串列表中每一个元素与用户标识对应的密文做差，进而得到匹配成功的文件，若否则返回匹配失败信息。

[0064] 另外，本申请还提供了一种数据查询电子设备，包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当一个或多个程序被一个或多个处理器执行，使得一个或多个处理器实现如上述的数据查询方法。

[0065] 另外，本申请还提供了一种计算机可读介质，其上存储有计算机程序，程序被处理器执行时实现如上述的数据查询方法。

[0066] 上述发明中的一个实施例具有如下优点或有益效果：本申请通过接收数据查询请求，获取对应的终端标识和检索条件；根据检索条件确定对应的密文文件，进而根据密文文件和终端标识进行访问权限校验；响应于访问权限校验成功，调用本地加密秘钥以对检索条件进行加密，生成加密检索条件；加密检索条件与密文文件进行匹配，响应于密文文件中存在文件与加密检索条件匹配成功，获取匹配成功的文件；调用本地解密秘钥，以对匹配成功的文件进行解密，得到查询结果数据。以提高用户信息的安全性，有效防止用户信息被泄

漏。

[0067] 上述的非惯用的可选方式所具有的进一步效果将在下文中结合具体实施方式加以说明。

附图说明

[0068] 附图用于更好地理解本申请,不构成对本申请的不当限定。其中:

[0069] 图1是根据本申请一个实施例所提供的数据查询方法的主要流程的示意图;

[0070] 图2是根据本申请一个实施例所提供的数据查询方法的主要流程的示意图;

[0071] 图3是根据本申请一个实施例所提供的数据查询方法的应用场景示意图;

[0072] 图4是根据本申请实施例的数据查询装置的主要单元的示意图;

[0073] 图5是本申请实施例可以应用于其中的示例性系统架构图;

[0074] 图6是适于用来实现本申请实施例的终端设备或服务器的计算机系统的结构示意图。

具体实施方式

[0075] 以下结合附图对本申请的示范性实施例做出说明,其中包括本申请实施例的各种细节以助于理解,应当将它们认为仅仅是示范性的。因此,本领域普通技术人员应当认识到,可以对这里描述的实施例做出各种改变和修改,而不会背离本申请的范围和精神。同样,为了清楚和简明,以下的描述中省略了对公知功能和结构的描述。需要说明的是,本公开的技术方案中,所涉及的用户个人信息的采集、收集、更新、分析、处理、使用、传输、存储等方面,均符合相关法律法规的规定,被用于合法的用途,且不违背公序良俗。对用户个人信息采取必要措施,防止对用户个人信息数据的非法访问,维护用户个人信息安全、网络安全和国家安全。

[0076] 图1是根据本申请一个实施例所提供的数据查询方法的主要流程的示意图,如图1所示,数据查询方法包括:

[0077] 步骤S101,接收数据查询请求,获取对应的终端标识和检索条件。

[0078] 本实施例中,数据查询方法的执行主体(例如,可以是服务器)可以通过有线连接或无线连接的方式,接收数据查询请求。数据查询请求,例如可以是对需要保密的数据进行查询的请求,例如对病患数据进行查询的请求。本申请实施例对数据查询请求的内容不做具体限定。执行主体在获取数据查询请求后,可以获取该请求中携带的终端标识和检索条件。

[0079] 其中,终端标识可以是用户发起数据查询请求时所使用的客户端编号、客户端名称等,本申请实施例对终端标识不做具体限定。检索条件,例如可以是包含用户名、用户检索关键词的检索语句,本申请实施例对检索条件的内容不做具体限定。

[0080] 步骤S102,根据检索条件确定对应的密文文件,进而根据密文文件和终端标识进行访问权限校验。

[0081] 访问控制系统可以调用各个密文文件,以将数据查询请求中携带的检索条件与调用的各个密文文件进行匹配,具体可以是将数据查询请求中携带的检索条件与调用的各个密文文件所关联的历史检索条件进行匹配,将匹配到的历史检索条件所对应的密文文件确

定为数据查询请求中携带的检索条件对应的密文文件。

[0082] 执行主体在确定出数据查询请求中携带的检索条件对应的密文文件后,可以调用权限校验程序以将数据查询请求对应的终端标识与确定出的密文文件进行匹配,以基于匹配结果进行访问权限校验。

[0083] 步骤S103,响应于访问权限校验成功,调用本地加密秘钥以对检索条件进行加密,生成加密检索条件。

[0084] 当执行主体确定终端标识对应的终端对密文文件有访问权限,则可以用本地密钥加密检索条件到密文文件中进行匹配。

[0085] 步骤S104,将加密检索条件与密文文件进行匹配,响应于密文文件中存在文件与加密检索条件匹配成功,获取匹配成功的文件。

[0086] 当加密检索条件在密文文件中匹配到需要检索的文件后,下载匹配成功的需要检索的密文文件到本地。

[0087] 具体地,获取匹配成功的文件,包括:查找密文文件中是否存在与加密检索条件相匹配的字符串,若是则遍历密文文件的字节数组,得到匹配子串列表,将匹配子串列表中每一个元素与用户标识对应的密文做差,用户标识,例如可以是用户序号,执行主体可以将用户序号做用户信息签名,进而得到匹配成功的文件,若否则返回匹配失败信息。

[0088] 步骤S105,调用本地解密秘钥,以对匹配成功的文件进行解密,得到查询结果数据。

[0089] 在下载匹配成功的需要检索的密文文件到本地后,再使用本地密钥解密匹配成功的需要检索的密文文件,得到最终检索到的查询结果数据。

[0090] 本实施例通过接收数据查询请求,获取对应的终端标识和检索条件;根据检索条件确定对应的密文文件,进而根据密文文件和终端标识进行访问权限校验;响应于访问权限校验成功,调用本地加密秘钥以对检索条件进行加密,生成加密检索条件;加密检索条件与密文文件进行匹配,响应于密文文件中存在文件与加密检索条件匹配成功,获取匹配成功的文件;调用本地解密秘钥,以对匹配成功的文件进行解密,得到查询结果数据。以提高用户信息的安全性,有效防止用户信息被泄漏。

[0091] 图2是根据本申请一个实施例所提供的数据查询方法的主要流程示意图,如图2所示,在根据检索条件确定对应的密文文件之前,数据查询方法还包括:

[0092] 步骤S201,获取历史用户信息和历史检索条件。

[0093] 具体地,获取历史用户信息,包括:

[0094] 获取原始用户信息,对原始用户信息进行掩码处理,以得到历史用户信息并获取历史用户信息。

[0095] 示例的,将原始的用户信息,以用户昵称为例(对应互联网医院中的患者昵称),在代码中编写一个方法maskNameWith8Star,在方法中利用字符串拼接append方法,将用户昵称的首尾进行保留,而中间部分进行“*”代替,操作完成后,可得到掩码处理后的用户昵称信息,并作为历史用户信息。

[0096] 历史检索条件例如可以包括历史用户信息对应的各个历史用户所输入的检索关键词、用户名称等,本申请实施例对历史检索条件不做具体限定。

[0097] 步骤S202,根据历史用户信息确定对应的用户标识,并将用户标识和历史用户信

息映射至目标对象。

[0098] 每个用户有一个唯一标识序号,用此序号做患者信息签名,即历史用户信息对应的用户标识。目标对象,例如可以是bean对象,将相应的历史用户信息和用户标识,映射在bean对象内,进行存储。

[0099] 步骤S203,对目标对象中的字符串类型的属性进行加密,以得到第一加密数据。

[0100] 对用户信息bean中所有为字符串类型的属性全部进行加密,以得到第一加密数据。

[0101] 步骤S204,基于信息摘要算法对第一加密数据进行加密计算,以得到第二加密数据。

[0102] 基于信息摘要算法对加密后得到的第一加密数据进行处理,即进行MD5处理,其中,MD5处理是调用Apache commons codec对第一加密数据实现MD5加密,计算MD5摘要并返回值为32个字符的十六进制字符串,即第二加密数据。

[0103] 步骤S205,基于历史检索条件和第二加密数据,生成密文文件。

[0104] 对历史检索条件和第二加密数据映射在目标对象(例如bean对象)内,将目标对象内所有字符串类型的属性全部进行加密。

[0105] 具体地,基于历史检索条件和第二加密数据,生成密文文件,包括:根据历史检索条件,确定目标访问地址;调用字符串哈希函数,以基于目标访问地址,计算得到对应的哈希值;基于哈希值,确定字符串位数,进而基于字符串位数,生成目标字符串并确定字符串间隔;基于第二加密数据、字符串间隔和目标字符串,生成密文文件。

[0106] 示例的,将原始的用户信息,以用户个人身份识别码(Personal identification number,pin)为例(对应互联网医院中的患者pin),使用MD5加密成32位的密文p,p为接收的传统密文,设如下所示:

[0107] p=2510c39011c5be704182423e3a695e91;

[0108] 将用户要访问的服务端IP地址(即目标访问地址)使用字符串哈希函数处理,得到哈希值x,将x中的所有数字取平均数,得到值y,根据y*4的数值判断与8、16、32中的哪一个值最接近,来决定随机生成一串8或者16或者32位的字符串,字符串中字符的取值范围为[0,f](16进制),比如平均数y=5则5*4=20最接近16,则生成16位的字符串为r,字符串的长度定为r.lenth,比如r=2db95e8e1a9267b7,则r.lenth=16;取间隔i=32/r.lenth,此处i=2。基于第二加密数据、字符串间隔和目标字符串,生成密文文件。

[0109] 具体地,基于第二加密数据、字符串间隔和目标字符串,生成密文文件,包括:将第二加密数据进行取余计算,得到取余计算结果,进而基于取余计算结果和字符串间隔,生成第一变换加密数据;基于字符串间隔向第一变换加密数据中添加目标字符串中的字符,以得到第二变换加密数据;生成一个随机数,进而基于随机数、字符串间隔和第二变换加密数据,生成密文文件。

[0110] p按照原始字符取余数并增加i值的操作进行变换,设原始字符x,变换后为y,则y=x的余数+i,生成变换表如下:

[0111] 原始x 0 1 2 3 4 5 6 7 8 9a b c d e f取余f e d c b a 9 8 7 6 5 4 3 2 10终值y 1 0f e d c b a 9 8 7 6 5 4 3 2

[0112] p按照如上变换表变换,则p变换后变为第一变换加密数据p1=fc015e81005c63a

1d09fdfe3e7b8c380

[0113] 在上述变换基础上，在p字符串中，每隔i位均匀添加一个r中的字符，此处i＝2因此相当于每隔2位插入一个字符，总计插入16位，得到的第二变换加密数据p2如下；

[0114] p2＝fc(2)01(d)5e(b)81(9)00(5)5ce63(8)a1(e)d0(1)9f(a)df(9)e3(2)e7(6)

[0115] b8(7)c3(b)80(7)；

[0116] 其中括号中的字符即为字符串r中的各字符；

[0117] 在上述变换基础上，生成一个随机数j，取值范围为[2,15]，比如说j＝7。

[0118] 基于随机数j、字符串间隔i和第二变换加密数据

[0119] p2＝fc(2)01(d)5e(b)81(9)00(5)5ce63(8)a1(e)d0(1)9f(a)df(9)e3(2)e7(6)b8(7)c3(b)80(7)，生成密文文件。

[0120] 具体地，基于随机数、字符串间隔和第二变换加密数据，生成密文文件，包括：基于随机数对第二变换加密数据执行数据翻转操作，以生成第三变换加密数据；根据随机数，生成随机串，进而将随机串添加至第三变换加密数据的尾部，将随机数和字符串间隔添加至第三变换加密数据的首部；获取解析规则的序号，进而将序号添加至第三变换加密数据的尾部，以生成第四变换加密数据；基于第四变换加密数据，得到密文文件。

[0121] 示例的，根据j＝7变换上述第二变换加密数据p2字符串，每隔7位翻转一次，最后不够7位的也全部翻转，处理后的第三变换加密数据p字符串如下：

[0122] p3＝5d102cf-00918be-836ec55-910de1a-3e9fdaf-78b67e2-708b3c；

[0123] 在上述变换基础上，根据j生成一个随机串s，长度为j，内容取值范围为[0,f]，例如s＝f46a91c；

[0124] 将字符串s追加至字符串p尾部，得到：

[0125] p3’＝5d102cf-00918be-836ec55-910de1a-3e9fdaf-78b67e2-708b3c-f46a91c；

[0126] 将参数j和i加到字符串p首部，得到：

[0127] p3”＝725d102cf-00918be-836ec55-910de1a-3e9fdaf-78b67e2-708b3c-f46a91c；

[0128] 将解析规则的序号k＝2加到第四变换加密数据字符串p尾部，得到：

[0129] p4＝725d102cf-00918be-836ec55-910de1a-3e9fdaf-78b67e2-708b3c-f46a91c2，以此完成对于字符串p的进一步加密，得到结果密文字符串，即密文文件。

[0130] 示例的，以下为一个生成密文文件的整体实施例：

[0131] 获取历史用户信息和历史检索条件；

[0132] 根据历史用户信息确定对应的用户标识，并将历史用户信息映射至目标对象，例如bean对象；

[0133] 对目标对象中的字符串类型的属性进行加密，以得到第一加密数据；

[0134] 基于信息摘要算法对第一加密数据进行加密计算，以得到第二加密数据；

[0135] 根据历史检索条件，确定目标访问地址；

[0136] 调用字符串哈希函数，以基于目标访问地址，计算得到对应的哈希值；

[0137] 将哈希值中的数字取平均数，以得到平均值；

[0138] 根据平均值和预设值(例如8、16、32)，确定字符串位数(例如8位、16位、32位)；

[0139] 根据字符串位数和预设字符取值范围，例如[0,f](16进制)，生成目标字符串(r)；

[0140] 根据字符串位数,确定字符串间隔(i);

[0141] 将第二加密数据进行取余计算,得到取余计算结果,进而基于取余计算结果和字符串间隔,生成第一变换加密数据p1;

[0142] 基于字符串间隔向第一变换加密数据中添加目标字符串中的字符,以得到第二变换加密数据p2;

[0143] 生成一个随机数,进而基于随机数对第二变换加密数据执行数据翻转操作,以生成第三变换加密数据p3;

[0144] 根据随机数,生成随机串,进而将随机串添加至第三变换加密数据的尾部,将随机数和字符串间隔添加至第三变换加密数据的首部,进而将解析规则的序号添加至第三变换加密数据的尾部,以生成第四变换加密数据p4;

[0145] 基于第四变换加密数据,得到密文文件。

[0146] 示例的,将原始的用户信息,以用户pin为例(对应互联网医院中的患者pin),使用MD5加密成32位的密文p,p为接收的传统密文,设如下所示:

[0147] p=2510c39011c5be704182423e3a695e91;

[0148] 将用户要访问的服务端IP地址使用字符串哈希函数处理,得到哈希值x,将x中的所有数字取平均数,得到值y,根据y*4的数值判断与8、16、32中的哪一个值最接近,来决定随机生成一串8或者16或者32位的字符串,字符串中字符的取值范围为[0,f](16进制),比如平均数y=5则5*4=20最接近16,则生成16位的字符串为r,字符串的长度定为r.lenth,比如r=2db95e8e1a9267b7,则r.lenth=16;

[0149] 取字符串间隔i=32/r.lenth,此处i=2;

[0150] p按照原始字符取余数并增加i值的操作进行变换,设原始字符x,变换后为y,则y=x的余数+i,生成变换表如下:

[0151] 原始x 0 1 2 3 4 5 6 7 8 9a b c d e f取余f e d c b a 9 8 7 6 5 4 3 2 10终值y 1 0f e d c b a 9 8 7 6 5 4 3 2

[0152] p按照变换表变换,则p变换后变为p=fc015e81005c63a1d09fdfe3e7b8c380

[0153] 在上述变换基础上,在p字符串中,每隔i位均匀添加一个r中的字符,此处i=2因此相当于每隔2位插入一个字符,总计插入16位,得到的结果p如下;

[0154] p2=fc(2)01(d)5e(b)81(9)00(5)5ce63(8)a1(e)d0(1)9f(a)df(9)e3(2)e7(6)

[0155] b8(7)c3(b)80(7);

[0156] 其中括号中的字符即为r中的各字符;

[0157] 在上述变换基础上,生成一个随机数j,取值范围为[2,15],比如说j=7。

[0158] 根据j=7变换上述p字符串,每隔7位翻转一次,最后不够7位的也全部翻转,处理后的p字符串如下:

[0159] p3=5d102cf-00918be-836ec55-910de1a-3e9fdaf-78b67e2-708b3c;

[0160] 在上述变换基础上,根据j生成一个随机串s,长度为j,内容取值范围为[0,f],例如s=f46a91c;

[0161] 将字符串s追加至字符串p尾部,得到:

[0162] p3'=5d102cf-00918be-836ec55-910de1a-3e9fdaf-78b67e2-708b3c-f46a91c;

[0163] 将参数j和i加到字符串p首部,得到:

[0164] p3”＝725d102cf-00918be-836ec55-910de1a-3e9fdaf-78b67e2-708b3c-f46a91c；

[0165] 将解析规则的序号k＝2加到字符串p尾部，得到：

[0166] p4＝725d102cf-00918be-836ec55-910de1a-3e9fdaf-78b67e2-708b3c-f46a91c2，以此完成对于字符串p的进一步加密，得到结果密文字符串，即密文文件。

[0167] 图3是根据本申请一个实施例所提供的数据查询方法的应用场景示意图。本申请实施例的数据查询方法，可以应用于对加密数据进行查询的场景。如图3所示，将医疗数据和检索条件一起使用客户端本地密钥进行加密，以密文的方式存储在存储模块上，这样可以保证服务端是无法知道密文医疗文件中包含的信息的；当客户端进行检索时，用户通过客户端(Client)使用检索条件进入访问控制系统中，由访问控制系统决定客户端是否有对密文文件的访问权限。如果没有权限，则直接返回；如果拥有访问权限，则客户端直接用本地密钥加密检索条件到密文文件中进行匹配，找到需要检索到的文件后，下载到本地，再使用本地密钥解密密文文件，得到最终检索到的结果。

[0168] 数据安全模块通过两层的安全技术防护，在保护医疗数据的隐私性方面有了很大进步。访问控制系统的防护功能可以有效阻止一部分用户的非法访问，保护了医疗数据的完整性：采用了可搜索的对称加密方案，使用本地密钥进行加密，以提高信息访问安全系数。通过多重加密与签名，并把存在数据库的信息都加密的方法来增加病患信息安全性。数据库存储的都是加密后的数据，通过普通查询无法查出真实的用户信息。要获得用户真实信息，必须从数据库中取出加密数据后，再进行解密，才能查到正确的用户信息。对数据的加密过程可以包括如下方式：1、输入：不定长度信息(要加密的信息)。2、输出：固定长度128-bits。由四个32位分组组成，将这四个32位分组级联后将生成一个128位散列值。3、基本方式为：求余、取余、调整长度、与链接变量进行循环运算，得出结果。

[0169] 图4是根据本申请实施例的数据查询装置的主要单元的示意图。如图4所示，数据查询装置400包括接收单元401、校验单元402、加密单元403、匹配单元404和解密单元405。

[0170] 接收单元401，被配置成接收数据查询请求，获取对应的终端标识和检索条件；

[0171] 校验单元402，被配置成根据检索条件确定对应的密文文件，进而根据密文文件和终端标识进行访问权限校验；

[0172] 加密单元403，被配置成响应于访问权限校验成功，调用本地加密秘钥以对检索条件进行加密，生成加密检索条件；

[0173] 匹配单元404，被配置成将加密检索条件与密文文件进行匹配，响应于密文文件中存在文件与加密检索条件匹配成功，获取匹配成功的文件；

[0174] 解密单元405，被配置成调用本地解密秘钥，以对匹配成功的文件进行解密，得到查询结果数据。

[0175] 在一些实施例中，数据查询装置还包括图4中未示出的密文文件生成单元，被配置成：获取历史用户信息和历史检索条件；根据历史用户信息确定对应的用户标识，并将用户标识和历史用户信息映射至目标对象；对目标对象中的字符串类型的属性进行加密，以得到第一加密数据；基于信息摘要算法对第一加密数据进行加密计算，以得到第二加密数据；基于历史检索条件和第二加密数据，生成密文文件。

[0176] 在一些实施例中，密文文件生成单元进一步被配置成：根据历史检索条件，确定目

标访问地址;调用字符串哈希函数,以基于目标访问地址,计算得到对应的哈希值;基于哈希值,确定字符串位数,进而基于字符串位数,生成目标字符串并确定字符串间隔;基于第二加密数据、字符串间隔和目标字符串,生成密文文件。

[0177] 在一些实施例中,密文文件生成单元进一步被配置成:将第二加密数据进行取余计算,得到取余计算结果,进而基于取余计算结果和字符串间隔,生成第一变换加密数据;基于字符串间隔向第一变换加密数据中添加目标字符串中的字符,以得到第二变换加密数据;生成一个随机数,进而基于随机数、字符串间隔和第二变换加密数据,生成密文文件。

[0178] 在一些实施例中,密文文件生成单元进一步被配置成:基于随机数对第二变换加密数据执行数据翻转操作,以生成第三变换加密数据;根据随机数,生成随机串,进而将随机串添加至第三变换加密数据的尾部,将随机数和字符串间隔添加至第三变换加密数据的首部;获取解析规则的序号,进而将序号添加至第三变换加密数据的尾部,以生成第四变换加密数据;基于第四变换加密数据,得到密文文件。

[0179] 在一些实施例中,密文文件生成单元进一步被配置成:获取原始用户信息,对原始用户信息进行掩码处理,以得到历史用户信息并获取历史用户信息。

[0180] 在一些实施例中,匹配单元404进一步被配置成:查找密文文件中是否存在与加密检索条件相匹配的字符串,若是则遍历密文文件的字节数组,得到匹配子串列表,将匹配子串列表中每一个元素与用户标识对应的密文做差,进而得到匹配成功的文件,若否则返回匹配失败信息。

[0181] 需要说明的是,本申请的数据查询方法和数据查询装置在具体实施内容上具有相应关系,故重复内容不再说明。

[0182] 图5示出了可以应用本申请实施例的数据查询方法或数据查询装置的示例性系统架构500。

[0183] 如图5所示,系统架构500可以包括终端设备501、502、503,网络504和服务器505。网络504用以在终端设备501、502、503和服务器505之间提供通信链路的介质。网络504可以包括各种连接类型,例如有线、无线通信链路或者光纤电缆等等。

[0184] 用户可以使用终端设备501、502、503通过网络504与服务器505交互,以接收或发送消息等。终端设备501、502、503上可以安装有各种通讯客户端应用,例如购物类应用、网页浏览器应用、搜索类应用、即时通信工具、邮箱客户端、社交平台软件等(仅为示例)。

[0185] 终端设备501、502、503可以是具有数据查询处理屏并且支持网页浏览的各种电子设备,包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。

[0186] 服务器505可以是提供各种服务的服务器,例如对用户利用终端设备501、502、503所提交的数据查询请求提供支持的后台管理服务器(仅为示例)。后台管理服务器可以接收数据查询请求,获取对应的终端标识和检索条件;根据检索条件确定对应的密文文件,进而根据密文文件和终端标识进行访问权限校验;响应于访问权限校验成功,调用本地加密秘钥以对检索条件进行加密,生成加密检索条件;加密检索条件与密文文件进行匹配,响应于密文文件中存在文件与加密检索条件匹配成功,获取匹配成功的文件;调用本地解密秘钥,以对匹配成功的文件进行解密,得到查询结果数据。以提高用户信息的安全性,有效防止用户信息被泄漏。

[0187] 需要说明的是,本申请实施例所提供的数据查询方法一般由服务器505执行,相应

地,数据查询装置一般设置于服务器505中。

[0188] 应该理解,图5中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要,可以具有任意数目的终端设备、网络和服务器。

[0189] 下面参考图6,其示出了适于用来实现本申请实施例的终端设备的计算机系统600的结构示意图。图6示出的终端设备仅仅是一个示例,不应对本申请实施例的功能和使用范围带来任何限制。

[0190] 如图6所示,计算机系统600包括中央处理单元(CPU)601,其可以根据存储在只读存储器(ROM)602中的程序或者从存储部分608加载到随机访问存储器(RAM)603中的程序而执行各种适当的动作和处理。在RAM603中,还存储有计算机系统600操作所需的各种程序和数据。CPU601、ROM602以及RAM603通过总线604彼此相连。输入/输出(I/O)接口605也连接至总线604。

[0191] 以下部件连接至I/O接口605:包括键盘、鼠标等的输入部分606;包括诸如阴极射线管(CRT)、液晶征信授权查询处理器(LCD)等以及扬声器等的输出部分607;包括硬盘等的存储部分608;以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分609。通信部分609经由诸如因特网的网络执行通信处理。驱动器610也根据需要连接至I/O接口605。可拆卸介质611,诸如磁盘、光盘、磁光盘、半导体存储器等等,根据需要安装在驱动器610上,以便于从其上读出的计算机程序根据需要被安装入存储部分608。

[0192] 特别地,根据本申请公开的实施例,上文参考流程图描述的过程可以被实现为计算机软件程序。例如,本申请公开的实施例包括一种计算机程序产品,其包括承载在计算机可读介质上的计算机程序,该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中,该计算机程序可以通过通信部分609从网络上被下载和安装,和/或从可拆卸介质611被安装。在该计算机程序被中央处理单元(CPU)601执行时,执行本申请的系统中限定的上述功能。

[0193] 需要说明的是,本申请所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以包括但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于:具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中,计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输,包括但不限于:无线、电线、光缆、RF等等,或者上述的任意合适的组合。

[0194] 附图中的流程图和框图,图示了按照本申请各种实施例的系统、方法和计算机程

序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0195] 描述于本申请实施例中所涉及到的单元可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中，例如，可以描述为：一种处理器包括接收单元、校验单元、加密单元、匹配单元和解密单元。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定。

[0196] 作为另一方面，本申请还提供了一种计算机可读介质，该计算机可读介质可以是上述实施例中描述的设备中所包含的；也可以是单独存在，而未装配入该设备中。上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被一个该设备执行时，使得该设备接收数据查询请求，获取对应的终端标识和检索条件；根据检索条件确定对应的密文文件，进而根据密文文件和终端标识进行访问权限校验；响应于访问权限校验成功，调用本地加密秘钥以对检索条件进行加密，生成加密检索条件；加密检索条件与密文文件进行匹配，响应于密文文件中存在文件与加密检索条件匹配成功，获取匹配成功的文件；调用本地解密秘钥，以对匹配成功的文件进行解密，得到查询结果数据。

[0197] 根据本申请实施例的技术方案，可以提高用户信息的安全性，有效防止用户信息被泄漏。

[0198] 上述具体实施方式，并不构成对本申请保护范围的限制。本领域技术人员应该明白的是，取决于设计要求和其他因素，可以发生各种各样的修改、组合、子组合和替代。任何在本申请的精神和原则之内所作的修改、等同替换和改进等，均应包含在本申请保护范围之内。

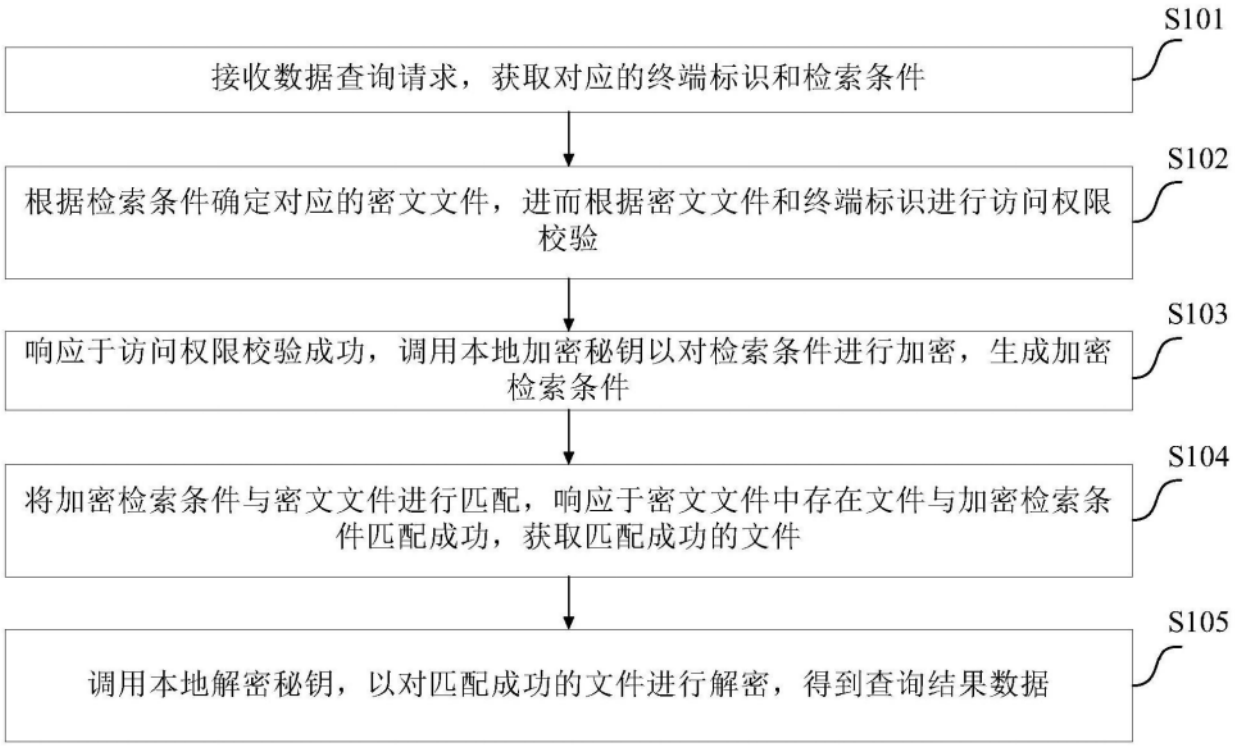

S101
接收数据查询请求，获取对应的终端标识和检索条件
S102
根据检索条件确定对应的密文文件，进而根据密文文件和终端标识进行访问权限校验
S103
响应于访问权限校验成功，调用本地加密秘钥以对检索条件进行加密，生成加密检索条件
S104
将加密检索条件与密文文件进行匹配，响应于密文文件中存在文件与加密检索条件匹配成功，获取匹配成功的文件
S105
调用本地解密秘钥，以对匹配成功的文件进行解密，得到查询结果数据

图1

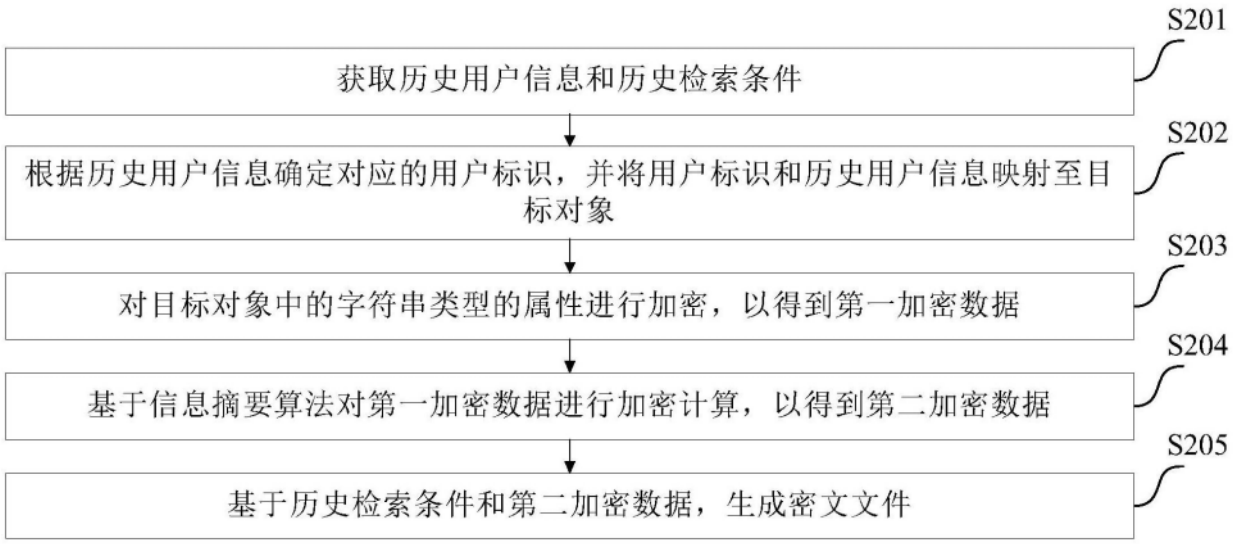

S201
获取历史用户信息和历史检索条件
S202
根据历史用户信息确定对应的用户标识，并将用户标识和历史用户信息映射至目标对象
S203
对目标对象中的字符串类型的属性进行加密，以得到第一加密数据
S204
基于信息摘要算法对第一加密数据进行加密计算，以得到第二加密数据
S205
基于历史检索条件和第二加密数据，生成密文文件

图2

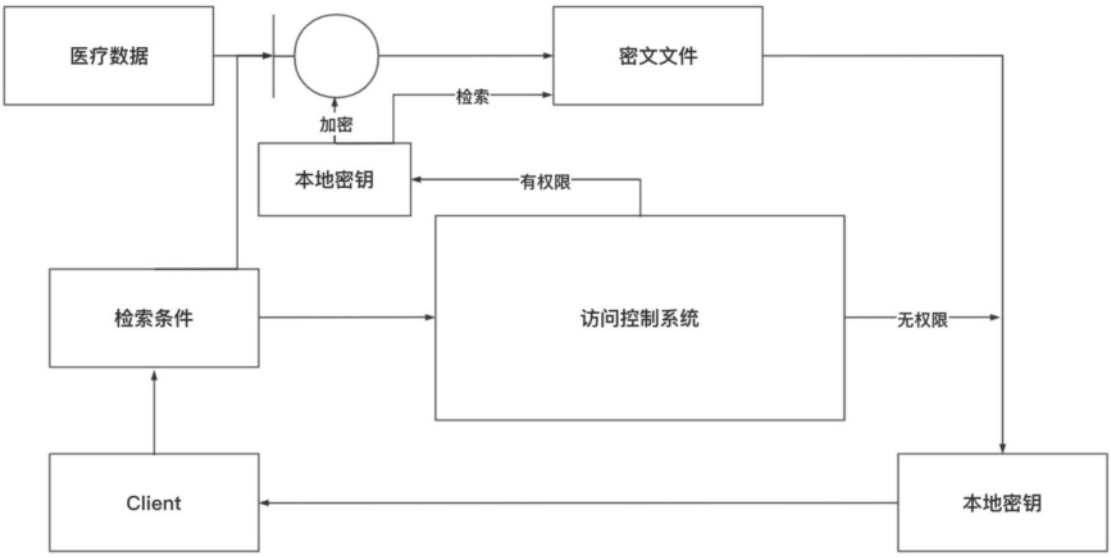

医疗数据
加密
密文文件
检索
本地密钥
有权限
检索条件
访问控制系统
无权限
Client
本地密钥

图3

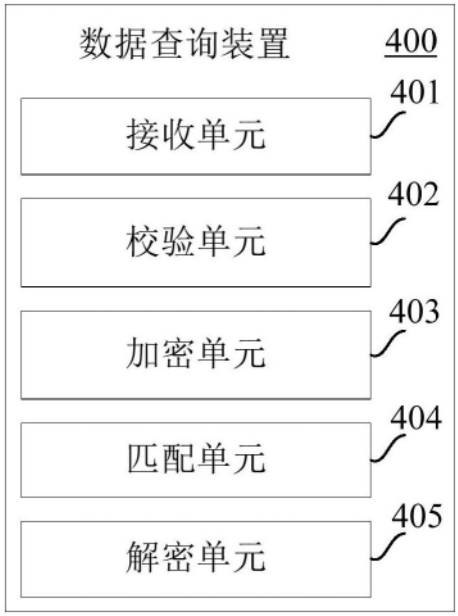

数据查询装置
400
401
接收单元
402
校验单元
403
加密单元
404
匹配单元
405
解密单元

图4

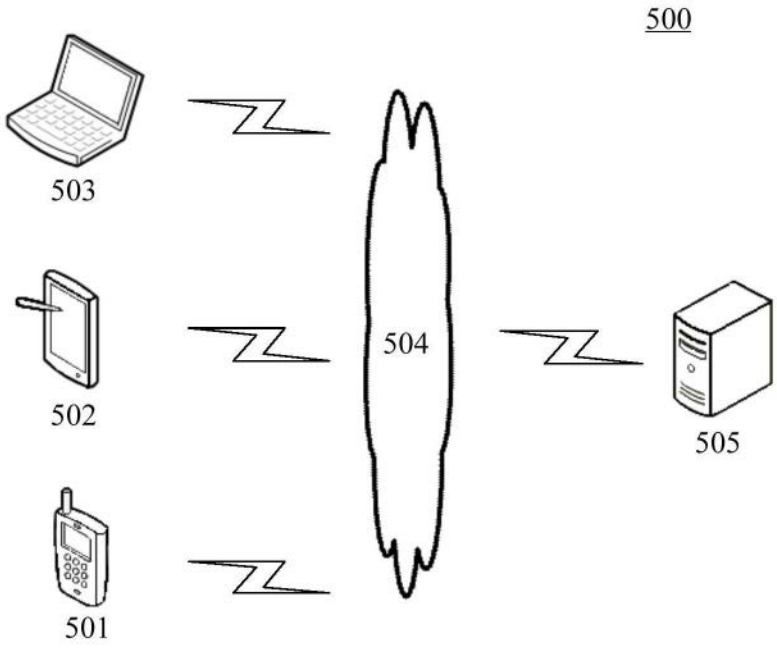

500
503
502
501
504
505

图5

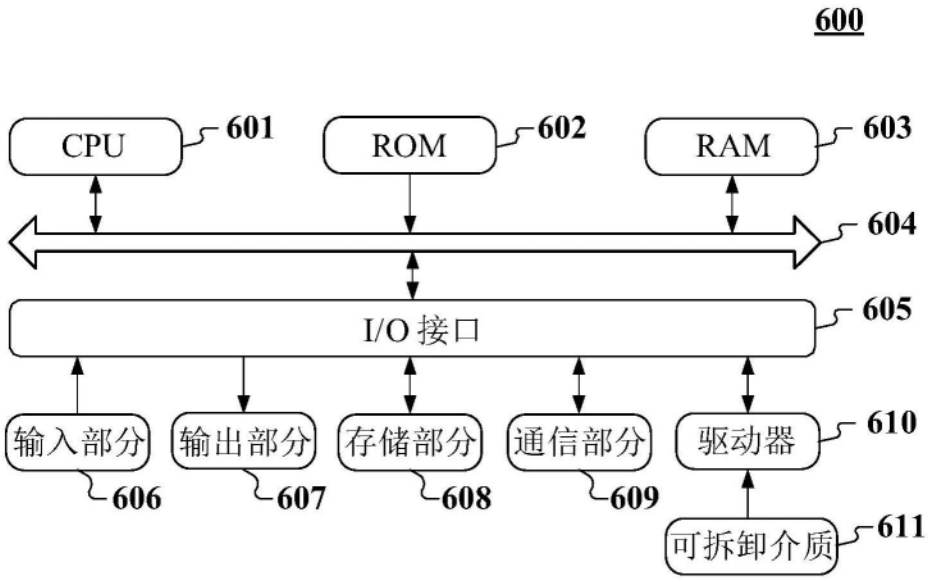

600
CPU
601
ROM
602
RAM
603
604
I/O 接口
605
输入部分
606
输出部分
607
存储部分
608
通信部分
609
驱动器
610
可拆卸介质
611

图6