(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 113536359 A
(43)申请公布日 2021.10.22

(21)申请号 202110905669.5

(22)申请日 2021.08.06

(71)申请人 东北大学
地址 110819 辽宁省沈阳市和平区文化路3号巷11号

(72)发明人 杜妍 刘园 张亚男

(74)专利代理机构 沈阳东大知识产权代理有限公司 21109
代理人 李在川

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)

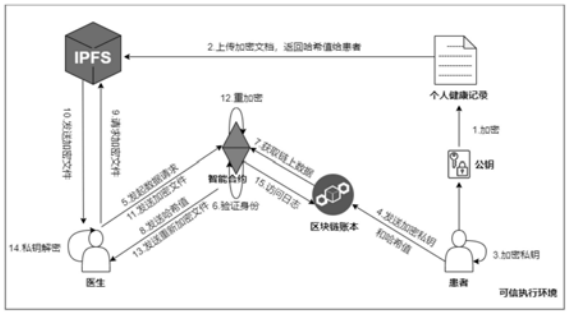
权利要求书2页 说明书5页 附图2页

(54)发明名称

基于区块链的个人健康记录隐私保护和访问系统及方法

(57)摘要

本发明公开一种基于区块链的个人健康记录隐私保护和访问系统及方法，系统包括联盟链网络、患者模块、医生模块、星际文件系统和智能合约；考虑到紧急情况下患者无意识，提前将患者经过加密的私钥上传到区块链上，采用了对称加密技术AES和非对称加密技术RSA先对患者的PHR文档进行加密，医生通过触发智能合约对文档进行重加密，保证在访问控制列表里的医生通过自己的私钥可以解密相应的PHR文档，同时区块链记录了访问者的行为；本发明为了加速医生获取数据，设计了快速响应码存储患者的基本信息，医生通过扫码直接根据患者的基本信息来申请访问数据。此外，采用布隆过滤器来加速医生的身份认证，保证医生能准确且快速地访问到患者的个人健康信息。



CN 113536359 A

1.一种基于区块链的个人健康记录隐私保护和访问系统,其特征在于,包括联盟链网络、患者模块、医生模块、星际文件系统和智能合约;

所述联盟链网络由各个医疗机构的内部私有链和机构之间的公有链共同组成,并负责调用智能合约和记录系统操作日志;

所述患者模块将文件加密后上传至星际文件系统,并生成快速响应码供医生模块获取信息;此外,患者模块调用智能合约在联盟链网络上初始化患者信息,并部署一个解密私钥的智能合约;

所述医生模块包括电脑端和手机端,调用智能合约在联盟链网络上初始化医生信息;此外,通过患者模块生成的快速响应码获取患者存储在星际文件系统中的加密文件,并调用智能合约对加密的文件进行重加密,然后利用自己的私钥解密,得到患者的相关信息。

2.采用权利要求1所述的基于区块链的个人健康记录隐私保护和访问系统进行隐私保护和访问的方法,其特征在于,包括如下步骤:

步骤1:采用对称加密算法AES创建密钥K,用密钥K来加密患者的健康信息文件,生成密文文件C1;

步骤2:采用非对称加密算法RSA为患者生成公私密钥对,并将密钥对保存在本地,利用生成的密钥对中的公钥加密密钥K得到密文,同时将加密密钥K得到的密文写入文件,得到密文文件C2;

步骤3:对密钥对中的私钥采用循环移位加密算法进行简单加密,得到私钥经加密后的密文;

步骤4:搭建星际文件系统IPFS,将密文文件C1和C2上传至星际文件系统,并记录星际文件系统返回的两个哈希值;

步骤5:根据患者输入的身份证号和上传的健康信息文件的格式生成快速响应码,便于急诊医生快速访问;

步骤6:患者模块调用智能合约,将患者的信息在联盟链网络上进行初始化;

步骤7:患者模块部署一个用于解密私钥的智能合约,调用这个智能合约能获得解密的私钥;

步骤8:医生模块调用智能合约初始化医生的信息;

步骤9:采用非对称加密算法RSA为医生模块生成公私密钥对,并将密钥对保存在本地;

步骤10:医生模块扫描快速响应码,调用智能合约,发起对患者的个人健康信息文件的数据请求;

步骤11:智能合约根据医生的信息,通过双重认证判断医生是否为急诊医生,若不是则直接无权限访问;若是则根据患者身份证号去链上查询文件C1和C2对应的哈希值,获取了两个经过加密的文件的哈希值;

步骤12:医生模块根据哈希值去星际文件系统中申请经过加密的文件C1和C2,并读取C2的内容,从C2中取出经过加密的对称密钥;

步骤13:调用智能合约来处理经过加密的对称密钥:根据患者身份证号查询患者上传的经过加密的私钥,并调用智能合约对加密的私钥进行解密,获得患者的私钥,并调用使用私钥对密钥K进行解密的智能合约解密得到密钥K;

步骤14:调用加密智能合约,使用医生模块的公钥对密钥K进行加密,并将加密后的密

文C3发送给医生；

步骤15:医生得到密文C3,并利用自己的私钥对C3进行解密得到密钥K；

步骤16:医生根据AES解密算法利用密钥K对文件C1进行解密。

3.根据权利要求2所述的采用基于区块链的个人健康记录隐私保护和访问系统进行隐私保护和访问的方法,其特征在于,所述快速响应码以二维码图片流的形式输出到前端,医生模块通过扫码获取患者基本信息并快速进入认证,加快数据请求过程。

4.根据权利要求2所述的采用基于区块链的个人健康记录隐私保护和访问系统进行隐私保护和访问的方法,其特征在于,所述患者的信息在联盟链网络上进行初始化以一个键对应多个值的形式,其中键为患者身份证号,值为密文文件C1对应的哈希值,密文文件C2对应的哈希值,以及经过加密的私钥。

5.根据权利要求2所述的采用基于区块链的个人健康记录隐私保护和访问系统进行隐私保护和访问的方法,其特征在于,所述患者模块部署的解密私钥的智能合约的调用过程被记录在联盟链网络账本中,即记录了调用这个解密智能合约的医生模块,如果进行了违法操作,患者在恢复意识后追究其法律责任。

6.根据权利要求2所述的采用基于区块链的个人健康记录隐私保护和访问系统进行隐私保护和访问的方法,其特征在于,所述初始化医生的信息以键值对的形式上传,其中键为医生工号,值为医院代码。

7.根据权利要求2所述的采用基于区块链的个人健康记录隐私保护和访问系统进行隐私保护和访问的方法,其特征在于,所述双重认证判断医生是否为急诊医生的方法为:

首先判断医生工号中是否包含“ED”、“ed”、“Ed”或“eD”,若包含上述字符则初步判断为急诊医生,否则不为急诊医生;

然后通过访问控制列表,对医生身份进行进一步认证,过程为:查看急诊医生的工号是否在访问控制列表里面,如果工号不在访问控制列表里面,则系统将拒绝该医生的访问;如果工号在访问控制列表里面,则直接跳转到数据请求界面。

8.根据权利要求7所述的采用基于区块链的个人健康记录隐私保护和访问系统进行隐私保护和访问的方法,其特征在于,所述访问控制列表采用布隆过滤器来存储,缩短医生认证时间。

基于区块链的个人健康记录隐私保护和访问系统及方法

技术领域

[0001] 本发明涉及信息访问技术领域，尤其涉及一种基于区块链的个人健康记录隐私保护和访问系统及方法。

背景技术

[0002] 个人健康记录PHR是每位患者的私人和重要资产。如果医生在诊断前获取到患者的PHR，将能对其予以更精准的治疗。通常情况下，患者可以处理医生的访问请求，只允许主治医生访问PHR，拒绝非法访问；但是处于紧急情况时，患者无意识，需要让医生快速访问到患者的数据，并记录访问者的行为，保护患者隐私。为了保护患者的隐私，通过区块链来记录访问者的所有操作行为以及存储数据。从本质上讲，区块链是一个共享数据库，存储在其中的数据，具有“不可伪造”“全程留痕”“可以追溯”“公开透明”等性质，故可用于保护数据隐私。

[0003] 文章“向前，钟世彬，徐海华，黄琳，安正源，杨筱筱.区块链技术在个人电子健康信息管理中的应用[J].产业科技创新，2020，2(06):38-40.”提供了一种通过构建两种链式来实现患者个人健康信息隐私保护的方法。此文在个人健康信息管理系统中引入私有链和公有链以存储和管理用户的个人健康信息，每个医疗机构都有独自运营和维护的私有区块，存储患者的原始健康信息，医疗机构联盟共同协商管理公有区块链，该公有区块链保存个人健康信息的安全索引记录，机构内部私有链和机构之间公有链共同组成联盟链，大大降低了信息泄露的风险。上述技术方案在实现患者个人健康信息隐私保护的同时并未考虑患者无意识的情况，患者需要在就诊时将身份识别码告知医生，并授权医生，医生才有访问数据的权限，由于未考虑紧急情况，也就未设计让医生快速通过认证的方法。

[0004] 所以，亟需一种在紧急情况下既能保证医生能准确且快速地访问到患者的个人健康记录，又能保护患者隐私的系统和方法。

发明内容

[0005] 针对上述现有技术的不足，本发明提供一种基于区块链的个人健康记录隐私保护和访问系统及方法。

[0006] 为解决上述技术问题，本发明所采取的技术方案是：一种基于区块链的个人健康记录隐私保护和访问系统，包括联盟链网络、患者模块、医生模块、星际文件系统和智能合约；

[0007] 所述联盟链网络由各个医疗机构的内部私有链和机构之间的公有链共同组成，并负责调用智能合约和记录系统操作日志；

[0008] 所述患者模块将文件加密后上传至星际文件系统，并生成快速响应码供医生模块获取信息；此外，患者模块调用智能合约在联盟链网络上初始化患者信息，并部署一个解密私钥的智能合约；

[0009] 所述医生模块包括电脑端和手机端，调用智能合约在联盟链网络上初始化医生信

息;此外,通过患者模块生成的快速响应码获取患者存储在星际文件系统中的加密文件,并调用智能合约对加密的文件进行重加密,然后利用自己的私钥解密,得到患者的相关信息。

[0010] 另一方面,本发明还提供一种采用上述基于区块链的个人健康记录隐私保护和访问系统进行隐私保护和访问的方法,包括如下步骤:

[0011] 步骤1:采用对称加密算法AES创建密钥K,用密钥K来加密患者的健康信息文件,生成密文文件C1;

[0012] 步骤2:采用非对称加密算法RSA为患者生成公私密钥对,并将密钥对保存在本地,利用生成的密钥对中的公钥加密密钥K得到密文,同时将加密密钥K得到的密文写入文件,得到密文文件C2;

[0013] 步骤3:对密钥对中的私钥采用循环移位加密算法进行简单加密,得到私钥经加密后的密文;

[0014] 步骤4:搭建星际文件系统IPFS,将密文文件C1和C2上传至星际文件系统,并记录星际文件系统返回的两个哈希值;

[0015] 步骤5:根据患者输入的身份证号和上传的健康信息文件的格式生成快速响应码,便于急诊医生快速访问;

[0016] 所述快速响应码以二维码图片流的形式输出到前端,医生模块通过扫码获取患者基本信息并快速进入认证,加快数据请求过程。

[0017] 步骤6:患者模块调用智能合约,将患者的信息在联盟链网络上进行初始化;

[0018] 所述患者的信息在联盟链网络上进行初始化以一个键对应多个值的形式,其中键为患者身份证号,值为密文文件C1对应的哈希值,密文文件C2对应的哈希值,以及经过加密的私钥。

[0019] 步骤7:患者模块部署一个用于解密私钥的智能合约,调用这个智能合约能获得解密的私钥;

[0020] 所述患者模块部署的解密私钥的智能合约的调用过程被记录在联盟链网络账本中,即记录了调用这个解密智能合约的医生模块,如果进行了违法操作,患者在恢复意识后追究其法律责任。

[0021] 步骤8:医生模块调用智能合约初始化医生的信息;

[0022] 所述初始化医生的信息以键值对的形式上传,其中键为医生工号,值为医院代码。

[0023] 步骤9:采用非对称加密算法RSA为医生模块生成公私密钥对,并将密钥对保存在本地;

[0024] 步骤10:医生模块扫描快速响应码,调用智能合约,发起对患者的个人健康信息文件的数据请求;

[0025] 步骤11:智能合约根据医生的信息,通过双重认证判断医生是否为急诊医生,若不是则直接无权限访问;若是则根据患者身份证号去链上查询文件C1和C2对应的哈希值,获取了两个经过加密的文件的哈希值;

[0026] 所述双重认证判断医生是否为急诊医生的方法为:

[0027] 首先判断医生工号中是否包含“ED”、“ed”、“Ed”或“eD”,若包含上述字符则初步判断为急诊医生,否则不为急诊医生;

[0028] 然后通过访问控制列表,对医生身份进行进一步认证,过程为:查看急诊医生的工

号是否在访问控制列表里面，如果工号不在访问控制列表里面，则系统将拒绝该医生的访问；如果工号在访问控制列表里面，则直接跳转到数据请求界面。

[0029] 进一步的，所述访问控制列表采用布隆过滤器来存储，缩短医生认证时间。

[0030] 步骤12：医生模块根据哈希值去星际文件系统中申请经过加密的文件C1和C2，并读取C2的内容，从C2中取出经过加密的对称密钥；

[0031] 步骤13：调用智能合约来处理经过加密的对称密钥：根据患者身份证号查询患者上传的经过加密的私钥，并调用智能合约对加密的私钥进行解密，获得患者的私钥，并调用使用私钥对密钥K进行解密的智能合约解密得到密钥K；

[0032] 步骤14：调用加密智能合约，使用医生模块的公钥对密钥K进行加密，并将加密后的密文C3发送给医生；

[0033] 步骤15：医生得到密文C3，并利用自己的私钥对C3进行解密得到密钥K；

[0034] 步骤16：医生根据AES解密算法利用密钥K对文件C1进行解密。

[0035] 采用上述技术方案所产生的有益效果在于：

[0036] 1、本发明提供的系统和方法通过区块链来记录申请访问数据者的所有操作行为，使用星际文件系统来存储患者的PHR文档，实现了对患者个人健康记录的隐私保护。

[0037] 2、本发明通过智能合约来托管患者的私钥和执行重加密过程，同时使用可信执行环境来保证智能合约执行过程中的安全，这样既保证了患者的相对隐私，也保证了医生的访问，从而可以给予患者更精准的治疗。

[0038] 3、本发明在紧急情况下，医生能访问到数据是关键的一个部分，更关键的是能系统能够快速响应医生的请求，争取在最短的时间内获取患者的过往患病信息和身体健康状况，本发明采取了布隆过滤器来加速医生的认证，加快医生获取数据的过程。

附图说明

[0039] 图1为本发明实施例中提供的基于区块链的个人健康记录隐私保护和访问系统结构示意图；

[0040] 图2为本发明实施例中改变数据块大小测试系统不同阶段执行时间的结果图；

[0041] 图3为本发明实施例中改变医生模块的请求数量系统使用布隆过滤器与未使用情况下的认证速度的对比图。

具体实施方式

[0042] 下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明，但不用来限制本发明的范围。

[0043] 如图1所示，本实施例中基于区块链的个人健康记录隐私保护和访问系统如下所述：

[0044] 系统包括联盟链网络、患者模块、医生模块、星际文件系统和智能合约；

[0045] 所述联盟链网络由各个医疗机构的内部私有链和机构之间的公有链共同组成，并负责调用智能合约和记录系统操作日志；

[0046] 所述患者模块将文件加密后上传至星际文件系统，并生成快速响应码供医生模块获取信息；此外，患者模块调用智能合约在联盟链网络上初始化患者信息，并部署一个解密

私钥的智能合约；

[0047] 所述医生模块包括电脑端和手机端，调用智能合约在联盟链网络上初始化医生信息；此外，通过患者模块生成的快速响应码获取患者存储在星际文件系统中的加密文件，并调用智能合约对加密的文件进行重加密，然后利用自己的私钥解密，得到患者的相关信息。

[0048] 本实施例中，为防止非法人员监控智能合约解密过程，采用了英特尔Software Guard Extensions(SGX)来增强安全性，其是对因特尔体系(IA)的一个扩展，SGX是英特尔推出的基于硬件的可信执行环境(TEE)。智能合约的执行过程是公开透明的，可信执行环境可以防止恶意人员监测智能合约执行过程中产生的数据。

[0049] 此外，本实施例中还提供一种采用上述系统进行隐私保护和访问的方法，包括如下步骤：

[0050] 步骤1：采用对称加密算法AES创建密钥K，用密钥K来加密患者的健康信息文件，生成密文文件C1；

[0051] 步骤2：采用非对称加密算法RSA为患者生成公私密钥对，并将密钥对保存在本地，利用生成的密钥对中的公钥加密密钥K得到密文，同时将加密密钥K得到的密文写入文件，得到密文文件C2；

[0052] 步骤3：对密钥对中的私钥采用循环移位加密算法进行简单加密，得到私钥经加密后的密文；

[0053] 步骤4：搭建星际文件系统IPFS，将密文文件C1和C2上传至星际文件系统，并记录星际文件系统返回的两个哈希值；

[0054] 步骤5：根据患者输入的身份证号和上传的健康信息文件的格式生成快速响应码，便于急诊医生快速访问；

[0055] 所述快速响应码以二维码图片流的形式输出到前端，医生模块通过扫码获取患者基本信息并快速进入认证，加快数据请求过程。

[0056] 步骤6：患者模块调用智能合约，将患者的信息在联盟链网络上进行初始化；

[0057] 所述患者的信息在联盟链网络上进行初始化以一个键对应多个值的形式，其中键为患者身份证号，值为密文文件C1对应的哈希值，密文文件C2对应的哈希值，以及经过加密的私钥。

[0058] 步骤7：患者模块部署一个用于解密私钥的智能合约，调用这个智能合约能获得解密的私钥；

[0059] 所述患者模块部署的解密私钥的智能合约的调用过程被记录在联盟链网络账本中，即记录了调用这个解密智能合约的医生模块，如果进行了违法操作，患者在恢复意识后追究其法律责任。

[0060] 步骤8：医生模块调用智能合约初始化医生的信息；

[0061] 所述初始化医生的信息以键值对的形式上传，其中键为医生工号，值为医院代码。

[0062] 步骤9：采用非对称加密算法RSA为医生模块生成公私密钥对，并将密钥对保存在本地；

[0063] 步骤10：医生模块扫描快速响应码，调用智能合约，发起对患者的个人健康信息文件的数据请求；

[0064] 步骤11：智能合约根据医生的信息，通过双重认证判断医生是否为急诊医生，若不

是则直接无权限访问;若是则根据患者身份证号去链上查询文件C1和C2对应的哈希值,获取了两个经过加密的文件的哈希值;

[0065] 所述双重认证判断医生是否为急诊医生的方法为:

[0066] 首先判断医生工号中是否包含“ED”、“ed”、“Ed”或“eD”,若包含上述字符则初步判断为急诊医生,否则不为急诊医生;

[0067] 然后通过访问控制列表,对医生身份进行进一步认证,过程为:查看急诊医生的工号是否在访问控制列表里面,如果工号不在访问控制列表里面,则系统将拒绝该医生的访问;如果工号在访问控制列表里面,则直接跳转到数据请求界面。

[0068] 进一步的,所述访问控制列表采用布隆过滤器来存储,缩短医生认证时间。

[0069] 步骤12:医生模块根据哈希值去星际文件系统中申请经过加密的文件C1和C2,并读取C2的内容,从C2中取出经过加密的对称密钥;

[0070] 步骤13:调用智能合约来处理经过加密的对称密钥:根据患者身份证号查询患者上传的经过加密的私钥,并调用智能合约对加密的私钥进行解密,获得患者的私钥,并调用使用私钥对密钥K进行解密的智能合约解密得到密钥K;

[0071] 步骤14:调用加密智能合约,使用医生模块的公钥对密钥K进行加密,并将加密后的密文C3发送给医生;

[0072] 步骤15:医生得到密文C3,并利用自己的私钥对C3进行解密得到密钥K;

[0073] 步骤16:医生根据AES解密算法利用密钥K对文件C1进行解密。

[0074] 本实施例中,使用测试工具Jmeter测试了在单用户情况下,患者上传文件、医生认证、医生获取数据三个阶段的执行时间,相较于使用紧急联系人的传统系统,响应时间缩短很多,有很大提升。

[0075] 实验测试分为两个部分,首先通过设置改变数据块大小来测试系统,在数据块大小分别为64KB、128KB、512KB、2MB、8MB、32MB和128MB的情况下对患者上传文件、医生认证、医生获取数据三个阶段进行测试,测试的实验结果由图2所示,实验结果表明,随着数据块的增大,患者上传文件的时间逐渐加长,医生认证时间维持在一定水平不变,医生获取数据的时间逐渐加长,同时由图可知,当数据块大小超过8MB时,患者上传文件时间和医生获取数据时间有较大幅度增长。

[0076] 第二部分将使用布隆过滤器的框架和未使用布隆过滤器的框架的响应时间进行比较,在并发用户(急诊医生)数分别为20、40、60、80、100、120、140、160情况下进行测试,测试的实验结果如图3所示,实验结果表明,随着并发用户数量的增多,使用了布隆过滤器的框架的医生认证速度优势较未使用布隆过滤器的框架逐渐增大,医生认证速度增快,从而加快了医生获取患者数据整个阶段的速度。

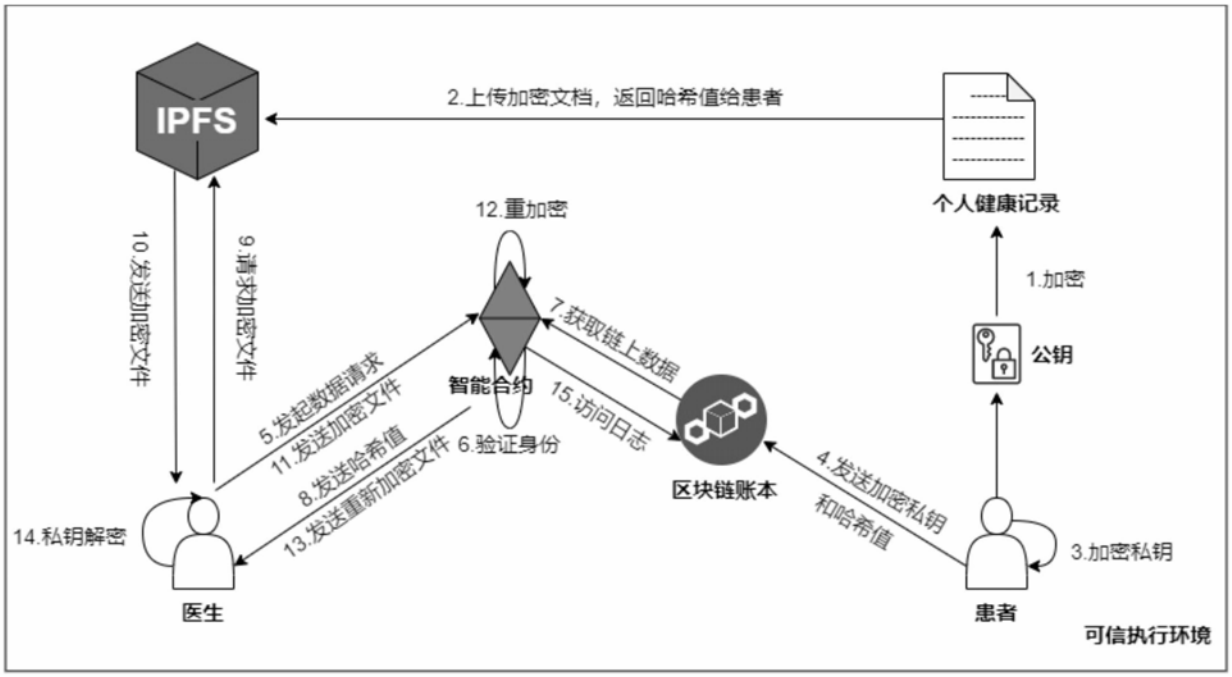

IPFS
2.上传加密文档，返回哈希值给患者
个人健康记录
12.重加密
10.发送加密文件
9.请求加密文件
1.加密
7.获取链上数据
公钥
5.发起数据请求
11.发送加密文件
智能合约
15.访问日志
8.发送哈希值
6.验证身份
区块链账本
4.发送加密私钥
和哈希值
13.发送重新加密文件
14.私钥解密
3.加密私钥
医生
患者
可信执行环境

图1

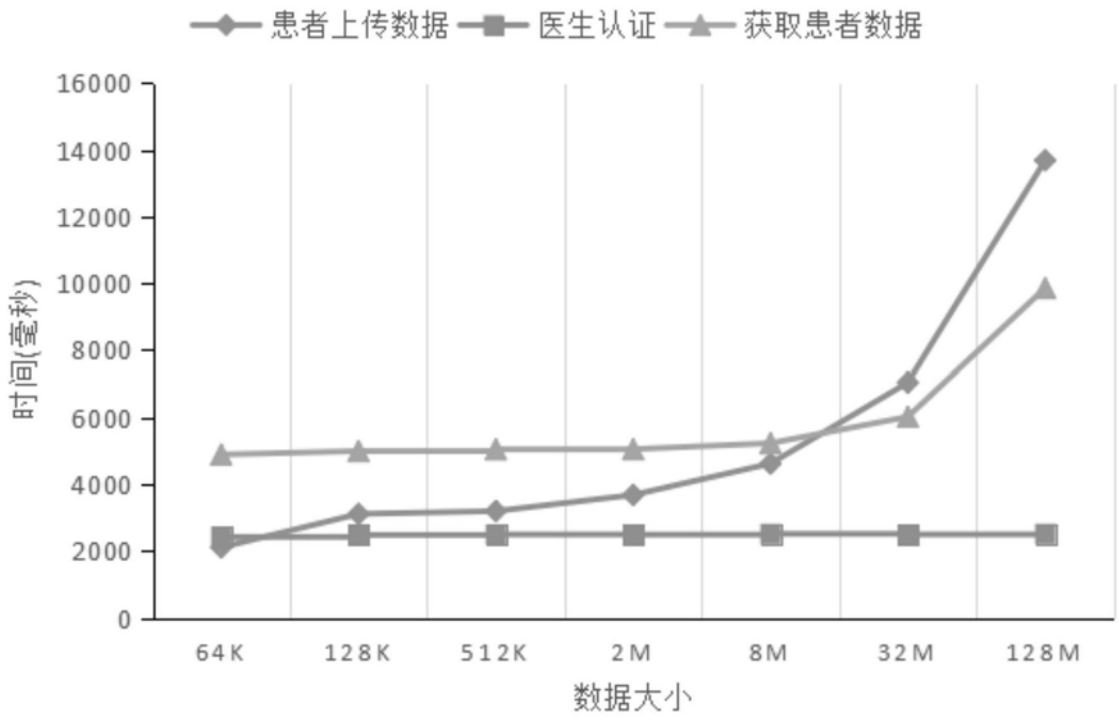

患者上传数据
医生认证
获取患者数据
16000
14000
12000
10000
8000
6000
4000
2000
0
时间(毫秒)
64K
128K
512K
2M
8M
32M
128M
数据大小

图2

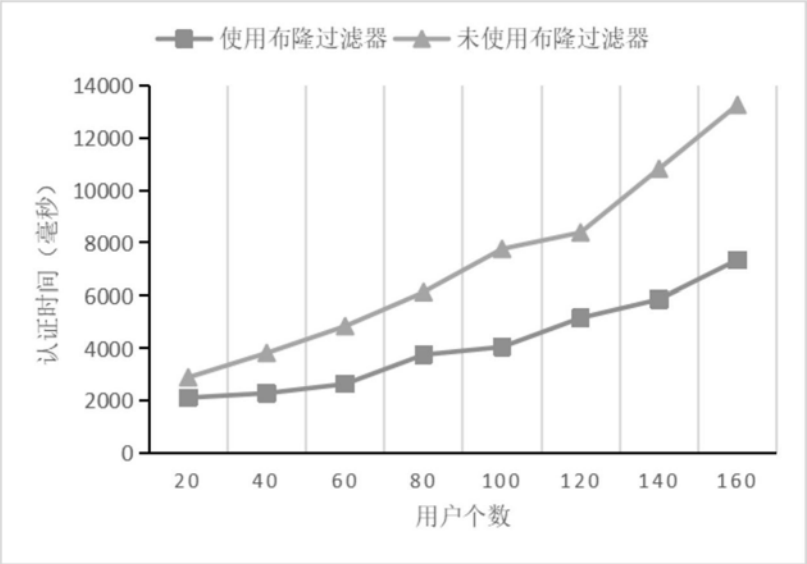

使用布隆过滤器
未使用布隆过滤器
14000
12000
10000
8000
6000
4000
2000
0
认证时间（毫秒）
20
40
60
80
100
120
140
160
用户个数

图3