(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 113555076 A
(43)申请公布日 2021.10.26

(21)申请号 202110929966.3

(22)申请日 2021.08.13

(71)申请人 同济大学
地址 200092 上海市杨浦区四平路1239号

(72)发明人 刘儿兀 杨昌鑫

(74)专利代理机构 上海科律专利代理事务所(特殊普通合伙) 31290
代理人 叶凤

(51)Int.Cl.
G16H 10/60(2018.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)
G06F 16/27(2019.01)
G06F 21/60(2013.01)

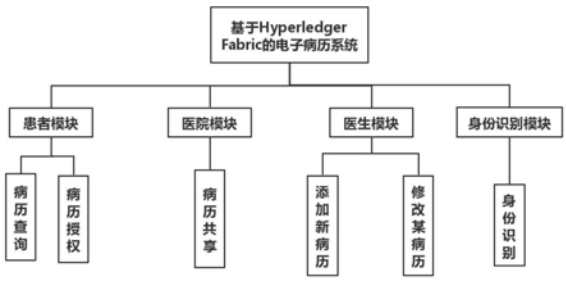
权利要求书1页 说明书6页 附图4页

(54)发明名称

一种基于hyperledger fabric(联盟链)的电子病历系统

(57)摘要

本发明涉及区块链、联盟链hyper l edger fabr ic领域,应用于电子病历系统。提出了一种基于hyper l edger fabr ic(联盟链)的电子病历系统,其特征在于,包含以下四大子模块:(1)患者模块(2)医院模块(3)医生模块(4)身份识别模块。本系统有益效果:(1)私密性:基于Hyper l edger Fabr ic的电子病历系统中每个用户都有自己的公私钥,避免了账号-密码体系带来的安全性问题,同时,电子病历信息是经过hash加密后存储在区块中。一方面可以保证信息的流通,同时还能避免节点的隐私泄露问题。(2)不可篡改;(3)去中心化。



CN 113555076 A

1.一种基于hyperledger fabric(联盟链)的电子病历系统,其特征在于,包含以下四大子模块:

(1)患者模块

患者可登录系统查询自己的病历信息,其中应至少支持查询全部病历信息;此外,患者还可在医生需要对某个病例进行修改时,将某个病历的权限授权给医生;

(2)医院模块

医院作为系统的参与实体,是整个系统的最基础的设施,根据联盟链的特点,医院作为Peer节点,各自拥有分布式账本的拷贝,患者的病历信息可在医院间安全自由的共享;

(3)医生模块

医生在经得患者同意后,可给患者在系统中添加新病历;此外,在患者授权后,医生可以修改病历,并且只有患者授权给医生,医生才能修改病历,患者本身或者其他任何人都无法修改病历;

(4)身份识别模块

考虑到系统对于不同角色的用户应进行信息隐藏,所以身份识别模块用来识别用户是医生或者患者角色,然后根据用户角色显示不同的内容页。

一种基于hyperledger fabric(联盟链)的电子病历系统

技术领域

[0001] 本发明涉及区块链、联盟链hyperledger fabric领域,应用于电子病历系统。

背景技术

[0002] 电子病历系统(EMR,Electronic Medical Record),也叫计算机化的病案系统或称基于计算机的病人记录系统(CPR,Computer-Based Patient Record)。它是用电子设备(计算机、健康卡等)保存、管理、传输和重现的数字化的病人的医疗记录,取代手写纸张病历。它的内容包括纸张病历的所有信息。美国国立医学研究所将定义为:EMR是基于一个特定系统的电子化病人记录,该系统提供用户访问完整准确的数据、警示、提示和临床决策支持系统的能力。

[0003] 病历是病人在医院诊断治疗全过程的原始记录,它包含有首页、病程记录、检查检验结果、医嘱、手术记录、护理记录等等。电子病历不仅指静态病历信息,还包括提供的相关服务。EMR是以电子化方式管理的有关个人终生健康状态和医疗保健行为的信息,涉及病人信息的采集、存储、传输、处理和利用的所有过程信息。

[0004] 最接近的方案提出于申请人为浙江工商大学,发明(设计)人为刘君强、胡逸阳,主分类号为G16H10/60(2018.01)I的在审专利《基于区块链的共享电子病历系统设计与实现》中。其所设计的系统以七个区块链智能合约为核心,通过Web服务来调用部署在区块链上的智能合约,为用户提供用户图形界面操作,实现了电子病历共享。

[0005] 具体的实现步骤为:

[0006] 步骤一:建立Hyperledger Fabric区块链网络,该网络串联起各个医院机构,并设定实施的组织架构是由三个医院组织Org1、Org2、Org3内的同一科室节点Peer1组成,同时这三个科室节点Peer0.Org1、Peer0.Org2、Peer0.Org3处在同一个通道Channel(一种Fabric区块链内部的通信链路)内,同时为各科室节点Peer1内部设定包括病人Client_pt、医生Client_dr、以及科室管理员Client_mgr等三类用户主体,区块链中的账本数据都是由这三类用户来操作。

[0007] 步骤二:将系统的实施分为表示层、逻辑业务层、数据访问层等三层结构:表示层是各类用户可以操作的前端页面;逻辑业务层为系统内的三类用户分别设定不同的操作功能,并以此来对各类用户的用例进行进一步的划分;数据访问层主要是建立HTTP服务器与Fabric交互的数据信息操作层;

[0008] 步骤三:设计电子病历的隐私访问控制策略,由于电子病历本身包含病人的隐私信息,必须设计一套既能保护网络内病人Client_pt的个人隐私,又能为医生Client_dr提供授权的访问控制策略:医生Client_dr在访问病人Client_pt的电子病历前,必须向病人Client_pt请求能查看病历的授权码;病人Client_pt接受到医生Client_dr请求后,为医生Client_dr匹配新的病历授权码,并将病历授权码写入到自己病历本的授权列表中,写入成功后病人Client_pt向医生Client_dr发送授权码;医生Client_dr获取到病历授权码后,就可利用该授权码访问到病人Client_pt的病历详细信息。

[0009] 步骤四:设计病人病历本与病历详细信息分离的保护策略,主要思路为:医生Client_dr创建病历后,将新建的病历编号和与之匹配的授权码(从前面医生向病人请求获得)存入病人Client_pt的病历本记录和医生Client_dr的问诊记录中,这样下次医生或者病人可以通过获取自己管理的记录来同时查看病历信息,避免了医生Client_dr重复向病人Client_pt请求授权;

[0010] 步骤五:依据步骤一的系统架构三类用户的功能用例,并结合步骤三、四中的病历授权访问和保护策略思想,设计出一套为方法系统内三类用户处理共享电子病历的整体执行流程,针对总体业务流程,本方法主要分为三个阶段来做处理,即系统初始化阶段、就诊准备阶段、就诊问诊阶段:在系统初始化阶段中,主要为三类用户的注册和登录、病人初始化病历本、科室管理员初始化管理合约等功能;在就诊准备阶段中,主要包括科室管理医生列表和病人挂号列表;在就诊问诊就阶段,主要包括医生选择病人创建就诊记录,然后请求病人对其进行授权,接收到授权后医生查看病人历史就诊记录,以及医生新建电子病历并保存病历到病人、医生、科室的就诊记录中。

[0011] 步骤六:依据步骤五设计的整体执行流程,设计不同的链码Chaincode(即智能合约)来操作上述流程,主要是设计各个链码Chaincode内的数据结构和具体操作函数,最后,将链码Chaincode编写并部署到Fabric区块链网络中。

[0012] 步骤七:建立后端的HTTP服务器,编写能调用Fabric区块链中已部署的链码Chaincode内的账本数据的后端操作代码,并为请求和响应的数据编写前端页面来显示地操作数据。

[0013] 已有技术存在的问题:

[0014] 步骤三中的电子病历的隐私访问控制策略中的授权码,授权码的生成机制和防伪机制需要更近一步的考虑,显然此专利并未说明清楚。

[0015] 步骤四中病人病历本和病历详情详细信息分离的保护策略在区块链中实际是不必要的,这增加了查询的时间,实际上可以去病历本化。

[0016] 步骤五中医生在收到病人的授权码后才能新建病历的处理流程实际是不符合现实的,现在中很显然有些病人在病危的情况下很可能不能给予授权然而医生却需要新建病历,因此在新建病历上应给予医生足够的权利

发明内容

[0017] 本发明要解决的问题有以下三个:

[0018] (1)患者病历难共享:在目前的EMR系统中,患者的电子病历会集中存储在其就诊医院的医疗系统中,然而在各医院间患者的电子病历不能共通,这就造成病人在转院治疗中需要重复进行某些基础治疗。

[0019] (2)患者隐私难保护:由于电子病历集中存储在医院的病历系统中,患者本身不持有电子病历,如医院系统遭受黑客攻击或系统管理人员故意泄漏患者数,则容易对患者的财产和安全造成威胁。

[0020] (3)患者数据难防伪:有的医院仍使用纸质病历,纸质病历极易篡改,现在大多数医院使用电子病历,信息没有足够强大的机制去防止篡改。

[0021] 相应的,本发明要解决的技术问题主要为:

[0022] (1)中心化存储。由于病人的电子病历存储在中心化的服务器上,且各个中心化的服务器之间往往不能共享数据,因此,中心化存储所导致的病历难以共享是亟需解决的问题。

[0023] (2)对称加密访问机制以及管理员权限模型。在现在的电子病历系统中管理员的权限过大,很难对管理员的行为作出规范和限制,且普通患者登录系统访问病历数据往往采用对称加密机制,如病人密码设置过于简单,易造成病人数据的泄露。

[0024] (3)数据结构不安全。现行的电子病历系统中,其所采用的数据结构大多是存储在数据库中的一条记录,这种数据结构难以自证未被篡改

[0025] 业务解决方案:

[0026] (1)医生、患者、医院三种用户及身份证书设计以及使用ABAC进行权限控制的用户身份解决方案。

[0027] (2)无授权码的病人隐私访问控制策略。

[0028] (3)操作实体为“病历”,无“病历本”实体的病历相关智能合约的设计和实现。

[0029] (4)以病人为核心,医生为辅助(主要表现形式为病人授权,医生操作)的电子病历增、改、查的解决方案。

[0030] 技术方案:

[0031] 一种基于hyperledger fabric(联盟链)的电子病历系统,其特征在于,包含以下四大子模块:

[0032] (1)患者模块

[0033] 患者可登录系统查询自己的病历信息,其中应至少支持查询全部病历信息。此外,患者还可在医生需要对某个病例进行修改时,将某个病历的权限授权给医生。

[0034] (2)医院模块

[0035] 医院作为系统的参与实体,是整个系统的最基础的设施,根据联盟链的特点,医院作为Peer节点,各自拥有分布式账本的拷贝,患者的病历信息可在医院间安全自由的共享。

[0036] (3)医生模块

[0037] 医生在经得患者同意后,可给患者在系统中添加新病历。此外,在患者授权后,医生可以修改病历,并且只有患者授权给医生,医生才能修改病历,患者本身或者其他任何人都无法修改病历。

[0038] (4)身份识别模块

[0039] 考虑到系统对于不同角色的用户应进行信息隐藏,所以身份识别模块用来识别用户是医生或者患者角色,然后根据用户角色显示不同的内容页。

[0040] 有益效果

[0041] 本系统有益效果:

[0042] (1)私密性:基于Hyperledger Fabric的电子病历系统中每个用户都有自己的公私钥,避免了账号-密码体系带来的安全性问题,同时,电子病历信息是经过hash加密后存储在区块中。一方面可以保证信息的流通,同时还能避免节点的隐私泄露问题。

[0043] (2)不可篡改;基于Hyperledger Fabric的电子病历系统依靠强大的共识机制来保证数据不可篡改,联盟链的每个参与节点都有一份独立的分布式账本,如果账本的数据被恶意篡改,在节点连接到区块链网络进行同步时,便可以发现数据被篡改并自动更正。

[0044] (3)去中心化;基于Hyperledger Fabric的电子病历系统建立在分布式的P2P网络的基础上,每个Peer节点均有分布式账本的备份,用户的电子病历信息不再单独存储在某个中心化的服务器上,而是存储在多个服务器节点上,这不仅保证了去中心化,而且用户的电子病历信息可以在不同的节点上进行共享。

附图说明

[0045] 图1系统功能模块

[0046] 图2身份识别模块:身份识别程序流程图

[0047] 图3病历查询程序流程图

[0048] 图4病历授权程序流程图

[0049] 图5病历创建程序流程图

[0050] 图6病历修改程序流程图

具体实施方式

[0051] 系统包含以四大子模块:

[0052] (1)身份识别模块

[0053] 考虑到系统对于不同角色的用户应进行信息隐藏,所以身份识别模块用来识别用户是医生或者患者角色,然后根据用户角色显示不同的内容页。

[0054] 如果登录客户端的用户是医生,则用户登录后展示与医生相关的内容页;如果登录客户端的用户是患者,则用户登录后展示与患者相关的内容页。具体的实现依赖于两部分:一是用户身份证书属性的设计,二是使用智能合约的ABAC(Attribute Based Access Control)来实现身份识别。

[0055] (2)患者模块

[0056] 患者可登录系统查询自己的病历信息,其中应至少支持查询全部病历信息。此外,患者还可在医生需要对某个病例进行修改时,将某个病历的权限授权给医生。

[0057] 如果登录客户端的用户是医生,由于医生不拥有任何病历,故查询结果为空,如果登录客户端的用户是患者,则返回查询到的患者所属的所有病历信息。见病历查询程序流程图、病历授权程序流程图。

[0058] 如果登录客户端的用户是医生,由于医生不拥有任何病历,故医生无须进行病历授权;如果登录客户端的用户是患者,则可以将某个病历的修改权限授权给某个医生。

[0059] (3)医院模块

[0060] 医院作为系统的参与实体,是整个系统的最基础的设施,联盟链的底层结构决定了医院作为Peer节点,各自拥有分布式账本的拷贝,患者的病历信息可在医院间安全自由的共享。

[0061] (4)医生模块

[0062] 医生在经得患者同意后,可给患者在系统中添加新病历。此外,在患者授权后,医生可以修改病历,并且只有患者授权给医生,医生才能修改病历,患者本身或者其他任何人都无法修改病历。见病历创建程序流程图、病历修改程序流程图。

[0063] 如果登录客户端的用户是医生,医生可添加相关病历信息;如果登录客户端的用

户是患者,则无法进行添加病历操作。

[0064] 如果登录客户端的用户是医生,医生可修改相关病历信息,注意,只有被患者授权后的医生才有权限修改病历。

[0065] 具体的,如身份识别模块的实现:

[0066] 在用户角色设计中,可知身份识别模块的实现即是根据不同用户角色进行不同内容页的展示。

[0067] (1)身份识别模块的设计目标:根据客户端识别的不同的用户角色进行不同内容页的展示,即实现功能模块中的身份识别子功能。

[0068] (2)身份识别模块的实现过程:如果登录客户端的用户是医生,则用户登录后展示与医生相关的内容页;如果登录客户端的用户是患者,则用户登录后展示与患者相关的内容页。具体的实现依赖于两部分:一是用户身份证书属性的设计;二是使用智能合约的ABAC(Attribute Based Access Control)来实现身份识别,相关程序流程图如图所示:

[0069] (1)用户证书的设计

[0070] 用户证书主要包括公钥证书和私钥证书,Hyperledger Fabric提供了一个可选的CA服务即Fabric CA来进行身份证书的设计与生成。Fabric CA是一个私有根CA提供程序,能够管理具有X.509证书形式的用户的数字证书。

[0071] Hyperledger Fabric提供了ABAC(Access Based Access Control)模块进行身份证书属性的设计和识别,在Fabric CA生成用户身份证书时,添加相关的属性,在智能合约中可使用相关识别模块的函数获取相关的属性值。

[0072] 医生或患者的身份证书属性设计如表4-2所示:

[0073] 表4-2用户证书属性设计表

[0074]

用户角色	属性	值	含义
医生(Doctor)	UserId	d01	01号医生
患者(Patient)	UserId	p01	01号患者

[0075] 其核心代码如下:

[0076] fabric_ca_client.register({enrollmentID:'user2',affiliation:'org1.department1',role:'client',attrs:[{name:'userid',value:'d01',ecert:true}]},admin_user);

[0077] (2)用户识别程序的设计

[0078] 在进行用户身份证书属性设计后,在智能合约中也需实现相应的功能函数来识别在用户身份证书的属性,进而识别不同的用户类型,具体如表4-3所示:

[0079] 表4-3识别用户证书函数设计表

[0080]

函数名称	参数列表	返回值	函数功能	函数调用者
identityRecognize	用户身份数字证书	Bytes	根据用户数字身份证书中的UserId属性识别用户身份是医生还是患者	客户端

[0081] 其核心代码如下：

[0082] //注入ABAC模块

[0083] sinfo,err:＝cid.New(APIstub)

[0084] //获得用户身份证书属性“userid”

[0085] dv,df,err:＝sinfo.GetAttributeValue("userid")

[0086] //根据获得的属性返回不同值来标记身份，

[0087] //如果是“患者”,则返回“p”,如果是“医生”,则返回“d”

[0088] var buffer bytes.Buffer

[0089] if strings.Contains(dv,"p"){

[0090] buffer.WriteString("p")

[0091] }else if strings.Contains(dv,"d"){

[0092] buffer.WriteString("d")

[0093] }else{

[0094] buffer.WriteString("null")

[0095] }

[0096] 具体的,底层设计方案：

[0097] (1)Hyperledger fabric的底层是分布式数据存储、点对点传输的分布式网络,与传统的分布式存储不同,区块链的分布式存储的独特性主要体现在两个方面:一是区块链每个节点都按照链式结构存储完整的数据,传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的,依靠共识机制保证存储的一致性,而传统分布式存储一般通过中心节点往其他备份节点同步数据。

[0098] (2)Hyperledger fabric采用非对称加密作为数据访问机制。存储在区块链上的交易信息是公开的,但是账户身份信息是高度加密的,只有在数据拥有者授权的情况下才能访问到,从而保证了数据的安全和个人的隐私。

[0099] (3)Hyperledger fabric的原始数据通过哈希(hash),就是把任意长度的输入通过散列算法,变换成固定长度的输出,该输出就是散列值。这种转换是一种压缩映射,简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。梅克尔树是区块链的重要数据结构,其作用是快速归纳和校验区块数据的存在性和完整性。一般意义上来讲,它是哈希大量聚集数据“块”的一种方式,它依赖于将这些数据“块”分裂成较小单位的数据块,每一个bucket块仅包含几个数据“块”,然后取每个bucket单位数据块再次进行哈希,重复同样的过程,直至剩余的哈希总数仅变为1。

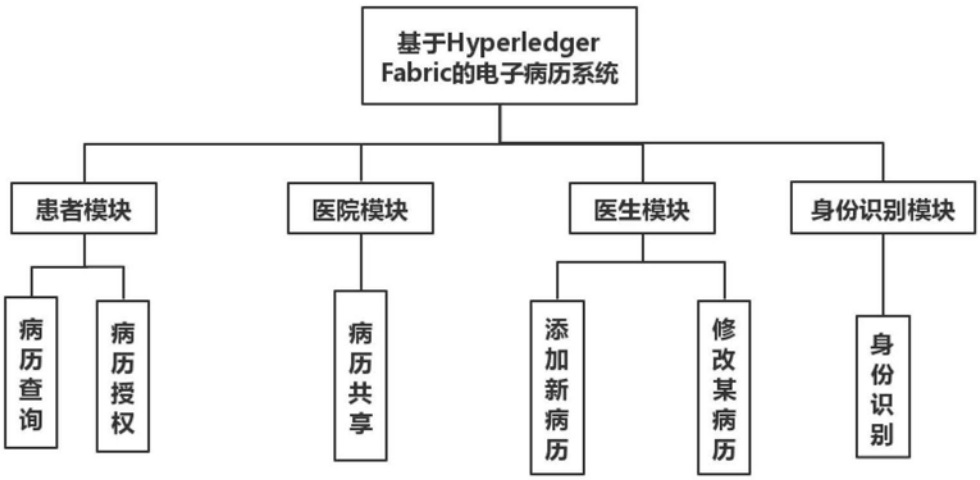

基于Hyperledger Fabric的电子病历系统
患者模块
医院模块
医生模块
身份识别模块
病历查询
病历授权
病历共享
添加新病历
修改某病历
身份识别

图1

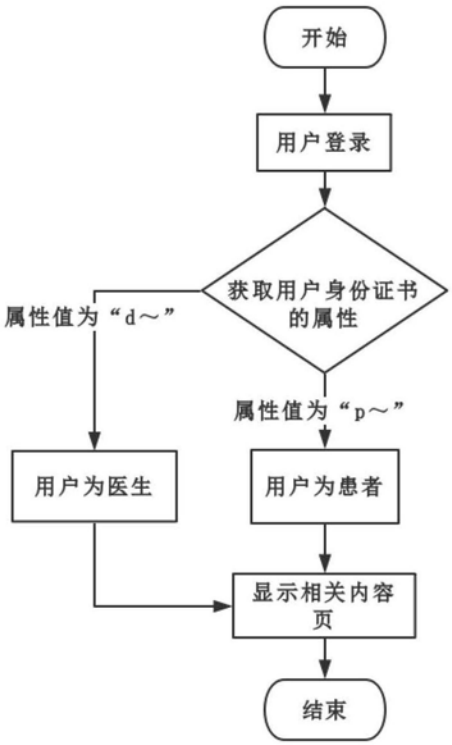

开始
用户登录
获取用户身份证书的属性
属性值为“d～”
属性值为“p～”
用户为医生
用户为患者
显示相关内容页
结束

图2

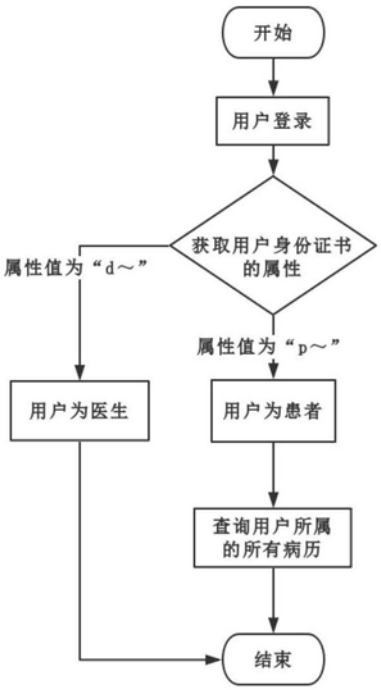

开始
用户登录
获取用户身份证书的属性
属性值为“d～”
属性值为“p～”
用户为医生
用户为患者
查询用户所属的所有病历
结束

图3

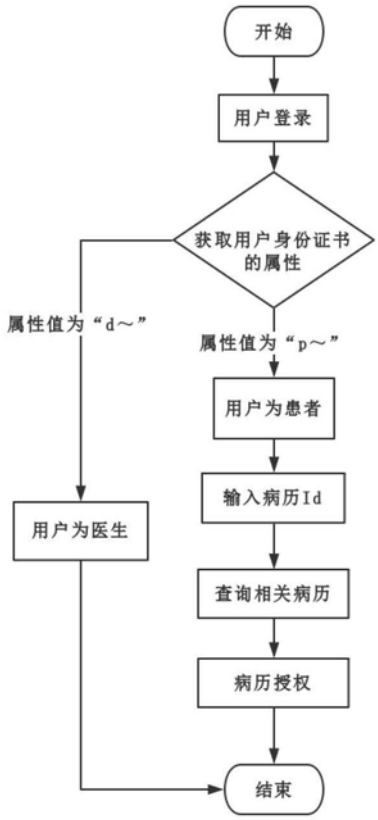

开始
用户登录
获取用户身份证书的属性
属性值为“d～”
属性值为“p～”
用户为患者
输入病历Id
用户为医生
查询相关病历
病历授权
结束

图4

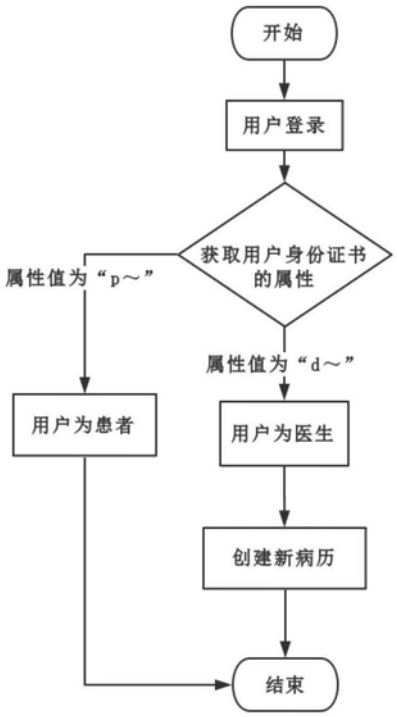


图5

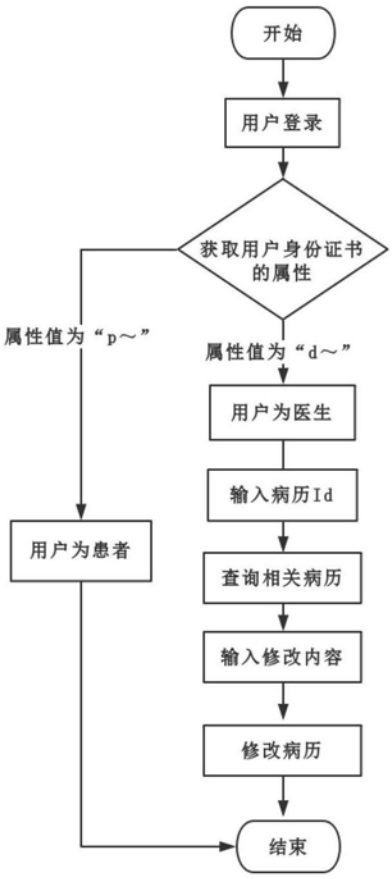

开始
用户登录
获取用户身份证书的属性
属性值为“p～”
属性值为“d～”
用户为医生
输入病历Id
用户为患者
查询相关病历
输入修改内容
修改病历
结束

图6