(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 106682530 A
(43)申请公布日 2017.05.17

(21)申请号 201710016484.2

(22)申请日 2017.01.10

(71)申请人 杭州电子科技大学
地址 310018 浙江省杭州市下沙高教园区2号大街

(72)发明人 何必仕 沈伟富 徐哲 吴锋 陈晖

(74)专利代理机构 杭州奥创知识产权代理有限公司 33272
代理人 王佳健

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

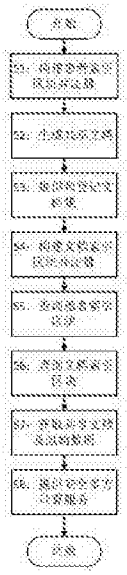
权利要求书1页 说明书5页 附图2页

(54)发明名称

一种基于区块链技术的医疗信息共享隐私保护方法及装置

(57)摘要

本发明公开了一种基于区块链技术的医疗信息共享隐私保护方法及装置。本发明的方法从基于区块链技术隐私保护、医疗数据在链结合脱链存储、强制隐私保护安全多方计算三方面出发，防止医疗数据非法获取、使用和篡改，实现医疗信息共享、大数据分析利用以及患者隐私的保护。本发明的装置，包括数据储存模块，采用三层数据存储架；基于区块链技术提供的服务模块，主要包括强制隐私保护安全多方计算；以及对外提供调用服务模块。本发明主要应用医疗信息共享、医疗大数据分析等领域，基于区块链技术既实现了医疗信息共享同时也给患者的隐私保护提供了技术上的保障。



CN 106682530 A

1.一种基于区块链技术的医疗信息共享隐私保护方法，其特征在于该方法包括以下三方面：

区块构建：区块构建主要分为两个部分，一个部分是将患者交叉索引信息生成区块并注册到区块链上，另一部分是将共享的医疗信息形成标准文档，并把文档的索引生成区块并注册到区块链上；

其中的患者交叉索引信息区块构建，为每个患者生成一对基于ECDSA椭圆曲线算法公钥和私钥地址，使用设定的主公钥地址向患者公钥地址发送消息，生成区块写入到区块链中，完成患者的登记注册；

其中的共享医疗信息文档索引区块构建，医疗机构将患者的医疗信息使用业内的标准进行封装，然后使用患者的私钥地址对这些数据进行数字签名，再传送到脱链的可信存储库；存储库首先会检查区块链中的登记备案信息，确定患者医疗信息的合法性；然后利用区块链中的患者注册的公钥地址对数据的电子签名进行核对，只有通过核对的数据，可信存储库才认可上传的患者医疗信息是合法的；在合法性得到认证后，使用SHA256哈希算法对共享医疗信息的索引信息形成数字指纹，再将该数字指纹作为数据交易的脚本信息连同索引信息一起形成区块并写入到区块链中；

区块链在链结合脱链存储：索引信息和交易信息采用区块链存储，共享医疗信息按照标准形成文档脱链存储，原始数据由医疗机构存储；

强制隐私保护安全多方计算：在分布式存储的环境下，计算请求方生成计算请求后用自己的证书签名，再带上加密公钥，一并提交到区块链上；每个区块链节点在收到请求后，通过区块链事件机制通知所有医疗机构，医疗机构在请求真实性进行验证之后，查询自己的原始数据并根据请求的计算内容进行计算，并将计算结果用请求方公钥加密返回；最后计算请求方解密来自不同医疗机构的计算结果并进行合并从而得到最终的结果。

2.根据权利要求1所述的一种基于区块链技术的医疗信息共享隐私保护方法，其特征在于：只要涉及到患者个人公钥地址的交易，包括时间、发送的主公钥地址以及接收公钥地址都会形成唯一的标识符被记录到区块链中，任何时候患者本人都可以对数据进行校验和审计。

3.根据权利要求2所述的一种基于区块链技术的医疗信息共享隐私保护方法，其特征在于：对于共享医疗信息按照标准形成文档，在对数据的完整性和合法性进行校验后采用key-value的存储模式进行脱链存储，通过网络层的安全的点对点通道、公钥加密手段来保证数据安全和隐私保护。

4.一种基于区块链技术的医疗信息共享隐私保护装置，其特征在于，包括：

数据储存模块，采用三层数据存储架构，第一层为医疗机构内的原始医疗数据；第二层为脱链可信存储库，主要存储按照标准生成的共享文档；第三层为区块链上的数据，主要存储患者索引信息和共享文档索引信息；

基于区块链技术提供的服务模块，主要包括强制隐私保护安全多方计算、身份认证、日志对账、跟踪审计和大数据查询分析；

对外提供调用服模块，针对第三方的开发利用本装置提供多种方式的调用服务，主要方式有OpenAPI、RESTful API、WebService和Web API。

一种基于区块链技术的医疗信息共享隐私保护方法及装置

技术领域

[0001] 本发明涉及医疗信息共享及患者隐私保护领域，具体涉及一种基于区块链技术的医疗信息共享隐私保护的方法及装置。

背景技术

[0002] 如今，医疗信息共享、云医院、移动医疗等应用已经在我国医疗机构广泛应用，医疗行业已经跨入大数据时代。而医疗信息共享、健康云技术的应用使得患者医疗数据更集中、更易得，这给患者就医、医生诊疗和卫生行政管理带来了前所未有便利的同时，也带来了数据泄露的风险。只要区域卫生信息平台或健康云平台某个环节出现漏洞，涉及患者隐私的医疗数据将可能被窃取；同时随着大数据应用，患者群体的隐私泄露也成为一个新的问题，如基因数据、流行病分布、人口敏感信息等群体性的隐私，一旦这些信息被泄露将会带来伦理、法律、国家安全等诸多问题。因此，如何加强大数据背景下患者隐私保护已经成为亟待解决的问题。

[0003] 从IT系统技术层面上看，目前医疗大数据的存储一般是采用集中部署的方式，医疗数据在不同医疗机构之间的交换和共享则倚重于数据加密技术，大数据分析中的个人隐私数据一般采用数据脱敏技术，数据安全保护一般依赖于硬件以及软件的入侵检测系统。从管理角度上看，患者隐私数据保护则一般依赖于相关人员的职业技术操守以及各个部门制定的管理规范制度，这就导致在医疗大数据集中部署背景下很难确保患者隐私不被泄露：第一，集中式部署虽然给管理带来了方便和高效，但是也会经常在软硬件出现问题时候导致数据丢失，同时这种方式的数据透明度也是不够的。第二，采用数据加密技术的医疗数据交换和共享，虽然从一定程度上解决患者隐私数据的安全，但是随着医疗数据互联互通的日益频繁，如何保证所有参与其中的医疗机构都能解决好数据安全问题成为一种不太可能实现的难题。第三，在大数据分析中，虽然针对患者个人隐私数据采用了脱敏和加密技术，但是患者个人是无法知晓个人隐私数据是如何存储和使用的，透明度不够，同时一些非法使用者通过解密推算等方法也能够从大数据中获取一部分患者的隐私数据。第四，人为因素，虽然各个部门对医护人员、IT系统管理员、数据分析工程师等在患者隐私保护上制定了相关的管理规定，但是出于个人利益、商业竞争利益等也很难杜绝患者隐私数据被泄露。

发明内容

[0004] 针对医疗信息共享的患者隐私保护的问题，本发明提出一种基于区块链技术的医疗信息共享隐私保护方法及装置。具体来说就是从基于区块链技术隐私保护、医疗数据在链结合脱链存储、强制隐私保护安全多方计算三方面出发，防止医疗数据非法获取、使用和篡改，实现医疗信息共享、大数据分析利用以及患者隐私的保护。

[0005] 本发明提供了一种基于区块链技术的医疗信息共享隐私保护方法，包括：

区块构建：区块构建主要分为两个部分，一个部分是将患者交叉索引信息生成区块并注册到区块链上，另一部分是将共享的医疗信息形成标准文档，并把文档的索引生成区块

并注册到区块链上。

[0006] 根据所述区块构建，其中患者交叉索引信息区块构建，为每个患者生成一对基于ECDSA椭圆曲线算法公钥和私钥地址，然后使用设定的主公钥地址向患者公钥地址发送消息，生成区块写入到区块链中，完成患者的登记注册。由于私钥地址无法由公钥地址计算推出，只要患者个人不要把私钥地址泄露出去，患者的医疗数据及隐私数据的安全性和完整性就能得到保证；同时只要涉及到患者个人公钥地址的交易，包括时间、发送的主公钥地址以及接收公钥地址都会形成唯一的标识符被记录到区块链中，任何时候患者本人都可以对数据进行校验和审计。

[0007] 根据所述区块构建，其中共享医疗信息文档索引区块构建，医疗机构将患者的医疗信息使用业内的标准进行封装，如电子病历使用HL7 CDA标准，关键影像信息使用Dicom标准进行封装，然后使用患者的私钥地址对这些数据进行数字签名，再传送到脱链的可信存储库。存储库首先会检查区块链中的登记备案信息，确定患者医疗信息的合法性；然后利用区块链中的患者注册的公钥地址对数据的电子签名进行核对，只有通过核对的数据，可信存储库才认可上传的患者医疗信息是合法的。在合法性得到认证后，使用SHA256哈希算法对共享医疗信息的索引信息形成数字指纹，再将该数字指纹作为数据交易的脚本信息连同索引信息一起形成区块并写入到区块链中。由于区块链的有极高的防篡改性以及数字指纹计算的高不可逆性，只要在区块链中找到数字指纹符合的索引信息，结合索引信息的注册时间戳，就可以保证患者共享的医疗信息是真实有效的。

[0008] 区块链在链结合脱链存储(称为存储库)：由于区块链采用冗余方式进行存储，而医疗共享数据具有数据量大数据结构复杂的特点，因此采用区块链技术存储所有医疗数据并不适合，同时区块链技术在大规模数据分析计算的情况下，也不能适应复杂事务的处理。因此提出了索引信息和交易信息采用区块链存储，共享医疗信息按照标准形成文档脱链存储，原始数据由医疗机构存储的三层存储方案。对于原始的医疗数据，不改变原有的存储架构，由医疗机构自身来保证数据的安全和隐私保护；对于共享医疗信息按照标准形成文档，在对数据的完整性和合法性进行校验后采用key-value的存储模式进行脱链存储，通过网络层的安全的点对点通道、公钥加密等手段来保证数据安全和隐私保护。

[0009] 强制隐私保护安全多方计算：在医疗信息共享的基础上，医疗机构需要借助已有的大数据进行分析利用，在分布式的环境下方法引入安全多方计算的方法来保护患者的隐私。如分析一组患者在不同医疗机构中某段时间的平均血压，利用安全多方计算，就可以在不知晓真实的原始血压数据的情况下得到计算结果。安全多方计算基本思想是：在分布式存储的环境下，计算请求方生成计算请求后用自己的证书签名，再带上加密公钥，一并提交到区块链上；每个区块链节点在收到请求后，通过区块链事件机制通知所有医疗机构，医疗机构在请求真实性进行验证之后，查询自己的原始数据并根据请求的计算内容进行计算，并将计算结果用请求方公钥加密返回；最后计算请求方解密来自不同医疗机构的计算结果并进行合并从而得到最终的结果。由于每个参与方都是获得加密输入，同时安全多方计算各方都不能获得其他方的原始数据信息，从而可以防范不诚实的参与者通过计算查询的方式盗取隐私数据。

[0010] 本发明提供了一种基于区块链技术的医疗信息共享隐私保护装置，包括：

数据储存模块，采用三层数据存储架构，第一层为医疗机构内的原始医疗数据；第二层

为脱链可信存储库，主要存储按照标准生成的共享文档；第三层为区块链上的数据，主要存储患者索引信息和共享文档索引信息。

[0011] 基于区块链技术提供的服务模块，主要包括强制隐私保护安全多方计算、身份认证、日志对账、跟踪审计、大数据查询分析等。

[0012] 对外提供调用服务模块，针对第三方的开发利用本装置提供多种方式的调用服务，主要方式有OpenAPI、RESTful API、WebService、Web API等。

[0013] 与当前医疗信息共享平台中的患者隐私保护方法相比，本发明具有以下优势：

首先，本发明采用了基于区块链技术数据存储访问控制的方法。区块链技术是维护一个不断增长的数据记录的分布式数据库，通过密码学技术和之前被写入的所有数据关联，使得第三方甚至是节点的拥有者难以篡改。区块链技术具有去中心化、非实名、数据匿名编码到数字地址等特点，可以防止数据泄露带来的隐私问题；同时数据只能通过私钥访问，从技术角度保证了隐私不被泄露。对患者来说，通过区块链技术可以对数据的使用进行审计，随时掌握个人数据的使用情况，患者也可以根据自身的保密需求对数据的使用进行约束。

[0014] 其次，本发明采用了区块链在链结合脱链的数据存储方法，解决了区块链技术采用冗余方式进行存储并不适合于大规模的数据存储，以及区块链技术在大规模数据分析计算的情况下，并不能适应复杂事务的处理等问题，既利用了区块链技术保护隐私的优势，同时也规避了区块链技术的劣势。

[0015] 最后，本发明提出了强制隐私保护安全多方计算方法。在大数据背景下，进行大数据分析前提条件就是医疗信息数据要共享，而共享和隐私保护从本质上就是对立的，本发明的强制隐私保护安全多方计算就是将公共索引数据在区块链上进行计算，原始的私有数据以脱链的方式进行多方计算，相比传统的计算模式，在无需解密隐私数据的情况下，实现直接利用隐私数据的密文进行身份验证，从而保证数据计算和处理的隐私性。

附图说明

[0016] 图1 示出了本发明一实施例的基于区块链技术的医疗信息共享隐私保护方法的流程图；

图2 示出了本发明一实施例的基于区块链技术的医疗信息共享隐私保护装置的示意图。

具体实施方式

[0017] 以下结合附图对本发明实施例作进一步说明。

[0018] 本发明提供一种基于区块链技术的医疗信息共享隐私保护方法及装置，通过区块链技术、区块链在链结合脱链存储以及多方安全计算等方法实现了患者医疗信息共享，解决了患者医疗数据泄露及患者隐私保护的问题。

[0019] 实施例：

参见图1，本实施例提供方法流程包括：

步骤S1：构建患者索引区块并注册。按照IHE(Integrating the Healthcare Enterprise)标准，提取患者索引信息，包括姓名、通讯地址、性别、出生年月、就诊卡号、手机号、身份证号、类别、保密级别等患者个人信息，并对敏感信息进行加密处理，然后为每个

患者生成一对基于ECDSA椭圆曲线算法公钥和私钥地址，然后使用特定的主公钥地址向患者公钥地址发送消息，生成区块写入到区块链中，完成患者的登记注册。

[0020] 步骤S2：生成共享文档。本发明装置针对医疗信息共享是以文档的形式提供共享服务，因此需要将患者的电子病历、健康档案、检查报告、影像等信息按照业内的标准形成文档。其中电子病历采用HL7 CDA标准，健康档案采用卫计委颁布的健康档案基本架构与数据标准，影像采用Dicom标准，当然针对每个医疗机构的不同情况，也可以采用相适应的标准来生成共享文档。

[0021] 步骤S3：提供和登记文档集。在生成共享文档后，使用患者的私钥地址对这些数据进行数字签名，再传送到脱链的可信存储库，存储库首先会检查区块链中的登记备案信息，确定患者医疗信息的合法性；然后利用区块链中的患者注册的公钥地址对数据的电子签名进行核对，只有通过核对的数据，可信存储库才认可上传的患者医疗信息是合法的，在合法性得到认证后，文档按照key-Value的形式存储到存储库，完成提供和登记文档集这一事务。

[0022] 步骤S4：构建文档索引区块并注册。这一步骤主要由脱链可信存储库来完成，存储完成共享文档安全存储后，需要提取共享文档的索引信息，包括，文档创建者、创建时间、文档类别、保密级别、文档唯一号、格式、哈希值、患者索引、服务开始时间、服务结束时间、标题、URI等，提取后使用SHA256哈希算法对共享文档提取的信息形成数字指纹，再将该数字指纹作为数据交易的脚本信息连同索引信息一起形成区块并写入到区块链中，完成文档索引区块的构建和注册。

[0023] 步骤S5：查询患者索引区块。患者或者医生如果需要获取共享的医疗信息，前提是要查询得到患者索引的信息。在这一步骤中，一般从患者的就诊卡、市民卡等芯片卡取得患者的数字证书。然后使用患者的证书签名，再带上加密公钥，一并提交到区块链上，区块链节点在收到查询请求后，将患者的索引信息使用公钥加密返回给患者或就医的医生。

[0024] 步骤S6：查询文档索引区块。在得到患者索引信息后，结合文档查询的参数，参数包括，文档的类型代码、创建时间、服务开始时间、服务结束时间、创建人、保密级别、格式代码、文档状态等生成文档查询请求，使用患者证书签名带上公钥发送到区块链中，区块量在收到查询请求后，首先验证查询的真实性和合法性，然后将查询结果用发起者的公钥加密返回给查询的请求者。

[0025] 步骤S7：获取文档及原始数据。在获得共享文档的索引数据之后，使用私钥对数据进行解密，获得共享文档的唯一索引号以及存储库的标识，先从存储库获取文档的详细内容，然后对标准文档的内容进行解析，根据解析的内容通过加密数据通道到相应的医疗机构取得医疗信息的原始数据。

[0026] 步骤S8：提供安全多方计算服务。这一步骤提供的服务主要是针对得到监管部门授权进行大数据查询和分析的医疗机构。首先医疗机构注册并对接自己的数据查询服务，并且得到注册证书；当医疗机构需要查询或分析数据时候，生成查询和计算请求，用自己的证书签名，再带上加密公钥，一起提交到区块链上；每个区块链节点收到请求后，通过区块链事件的机制通知所有相关的医疗机构；医疗机构在对查询计算请求的合法性进行验证后，查询自己的医疗大数据，并根据查询计算请求生成查询结果，并用查询发起者的公钥加密返回；最后同样使用区块链事件机制通知发起查询计算请求的节点；最后查询节点解密

来自不同医疗机构查询以及计算的结果，并对其合并得到最终的结果。

[0027] 本发明实施例还提供了一种基于区块链技术的医疗信息共享隐私保护装置，参见图2。

[0028] 本装置采用三层数据存储架构，第一层为医疗机构，主要存储原始的医疗数据，数据安全和隐私保护策略由医疗机构自身来提供；第二层为脱链可信存储库，主要是存储按照各种标准生成的共享文档；第三层为区块链节点，主要存储患者索引、共享文档索引的信息。本装置基于区块链技术提供的服务模块包括：强制隐私保护安全多方计算、身份认证、日志对账、跟踪审计、大数据查询分析等服务，同时通过OpenAPI、RESTful API、WebService、Web API等方式提供给第三方进行后续相关的医疗信息共享以及大数据等开发应用。

[0029] 综上所述，本发明基于区块链技术的医疗信息共享隐私保护方法及装置，主要应用医疗信息共享、医疗大数据分析等领域，基于区块链技术既实现了医疗信息共享同时也给患者的隐私保护提供了技术上的保障。

[0030] 以上所述，仅是本发明的在医疗信息共享以及患者隐私保护领域较佳实施例而已，并非是对本发明作其它形式的限制，任何熟悉本专业的技术人员可能利用上述揭示的技术内容加以变更或改型为等同变化的等效实施例应用于其它领域，但是凡是未脱离本发明技术方案内容，依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与改型，仍属于本发明技术方案的保护范围。

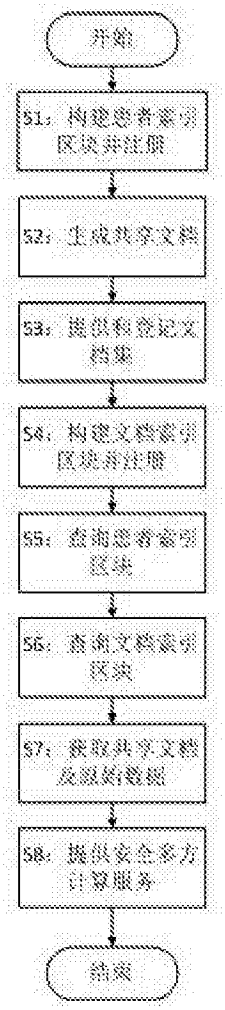

开始
S1：构建患者索引区块并注册
S2：生成共享文档
S3：提供病变记录文档集
S4：构建文档索引区块并注册
S5：查询患者索引区块
S6：查询文档索引区块
S7：获取共享文档及相关数据
S8：提供安全多方计算服务
结束

图1

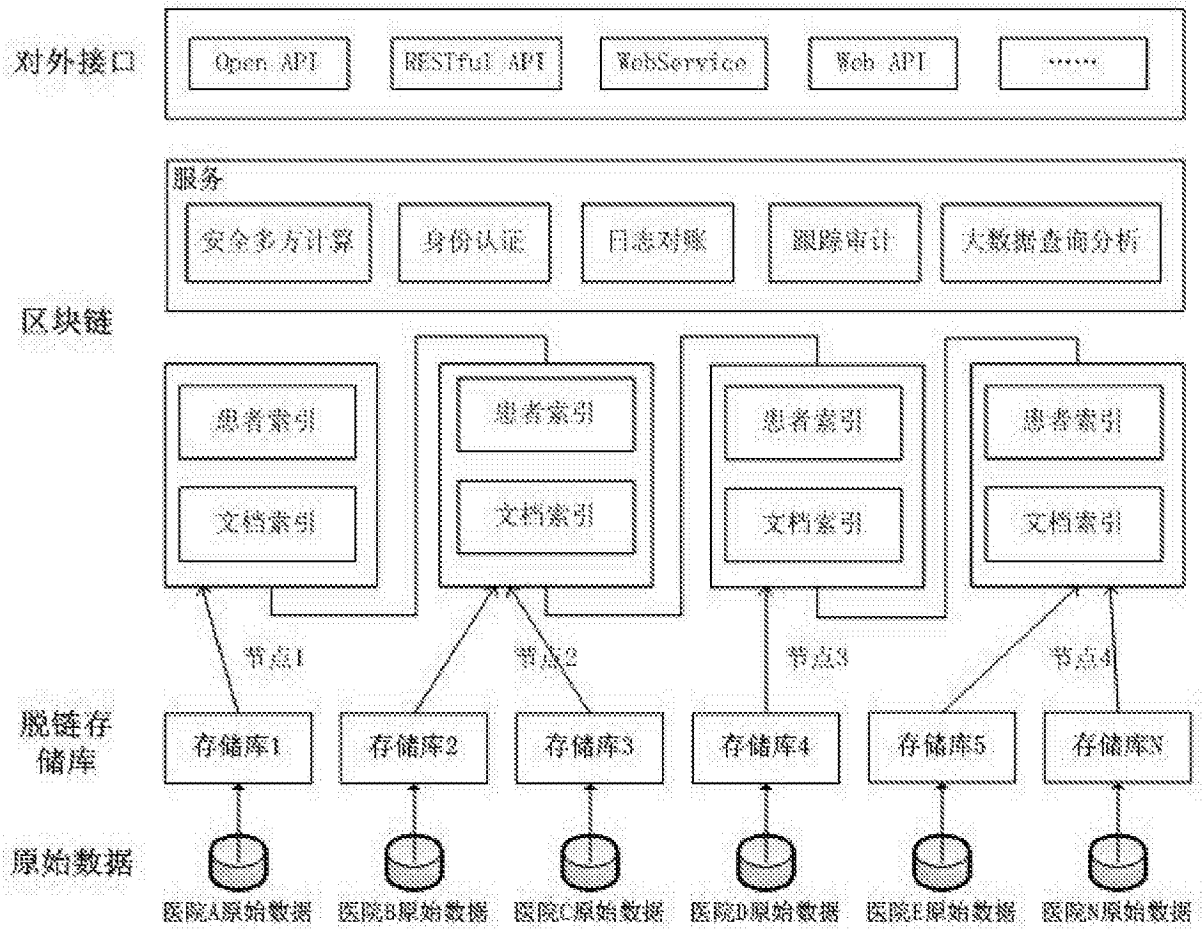

对外接口
Open API
RESTful API
WebService
Web API
……
服务
安全多方计算
身份认证
日志对账
跟踪审计
大数据查询分析
区块链
患者索引
文档索引
患者索引
文档索引
患者索引
文档索引
患者索引
文档索引
节点1
节点2
节点3
节点4
脱链存储库
存储库1
存储库2
存储库3
存储库4
存储库5
存储库6
原始数据
医院A原始数据
医院B原始数据
医院C原始数据
医院D原始数据
医院E原始数据
医院N原始数据

图2