文章编号:1005-0523(2020)05-0121-06

基于区块链的医疗记录安全共享方案

张利华[1],付东辉[2],万源华[2]

(华东交通大学 1. 软件学院;2.电气与自动化工程学院,江西 南昌 330013)

摘要:目前电子医疗记录存放在不同的医院中,这阻碍了患者医疗数据的共享并使患者的隐私面临严重威胁。提出了一种基于区块链的医疗记录安全共享方案SMRSBC。在SMRSBC中,原始的EMR被安全地存放在云存储服务器中,索引被保留在防篡改联盟区块链中。这样可以大大降低医疗数据泄露的风险,同时,区块链中的索引确保了EMR不能被任意修改。通过患者的预定义访问权限,可以通过区块链的智能合约自动完成电子医疗记录的安全共享。此外,在患者的电子医疗记录存储和提取阶段采用非对称加密技术,能够很好的保护患者的隐私。SMRSBC能够实现EMR安全有效的共享,并且能保证病人的隐私不被泄露。

关键词:区块链;医疗记录;隐私保护;存储与共享;智能合约

中图分类号:TP311 **文献标志码**:A

本文引用格式:张利华,付东辉,万源华. 基于区块链的医疗记录安全共享方案[J]. 华东交通大学学报,2020,37(5):124-129.

Citation format:ZHANG L H,FU D H,WAN Y H. A secure medical record sharing scheme based Blockchain[J]. Journal of East China Jiaotong University,2020,37(5):124-129.

DOI:10.16749/j.cnki.jecjtu.2020.05.018

个人健康信息和电子医疗记录已成为可能影响个人生活质量的资产。世界卫生组织的报告已经将个人健康信息确定为资产[1],电子医疗记录(electronic medical records,EMR)的共享远远超出了其基本医疗用途。然而,由于医院和医疗保健提供者网络中的个人健康数据的碎片化和隔离[2],受行业和政府法规保护,充分把这些数据进行共享非常困难。最早出现的一种解决方案是建立数字健康信息交换机构,使护理人员和机构之间的患者病历数字化传输成为常态。这已经解决了一些问题,包括多余的测试和相关成本,更好地协调患者护理,降低了总体管理成本且改善了患者的生活质量。

然而,尽管有一些解决措施,但仍然存在一些挑战,并没有办法解决,其中一些涉及到互操作性[3],数据的安全性和私密性以及传输到请求者后的数据控制。当前的方法几乎不能控制所请求的数据进行操作或计算。对于错误或不道德地使用所请求信息会受到法律制裁,当该行为被监管部门检测到,但此时,对个人利益的损害可能已无法弥补。再者,尽管存在异构数据源的挑战,但医疗领域的网络化趋势仍将继续存在[4]。区块链是比特币加密货币的基础,是分布式账本技术,为共享后的数据和操作提供了控制机会。有效巧妙地使用密码学加密技术和共识机制相结合,为在多个领域中的应用提供了执行计算的安全平台[5]。

近年来,由于区块链在数据管理方面的优势,即区块链的不变性和内在自治性,其在电子健康领域能够保障个人健康数据的安全性和隐私性越来越受到人们的关注。

软件服务平台Patientory,通过向患者提供个人档案,患者可以安全地访问自己的医疗记录。医疗信息存储在符合HIPAA的区块链平台上,为患者和护理人员提供安全的数据点。通过使用Patientory,护理人员可以审查医疗计划、患者的医疗信息,并与患者进行交流,而患者又可以与其他病情相似的患者建立联系。

收稿日期:2020-01-09

基金项目:国家自然科学基金项目(61563016);江西省教育厅科技项目(GJJ14371)

作者简介:张利华(1972—),男,副教授,博士,研究方向为区块链技术。E-mail:lhzhangbuaa@163.com。

Xiao等[6]提出了一个基于区块链的健康信息系统架构,通过引入的健康数据网关,旨在使患者能够通过区块链控制和共享其医疗数据。夏琦等[7]提出了一种针对敏感医疗数据存储库池的安全医疗数据访问与共享框架BBDS,他们使用区块链网络作为访问控制层,只有授权用户才能对数据执行操作,存储每个交易的副本并将其附加到区块链。然而,只有在Xia[8]的研究中讨论了实现数据来源和审计,作者调查了智能合约和区块链技术的使用。MeBoice的设计是BBDS的一个逻辑扩展,它集成了现有的无信任的云提供商和其他数据监护人,它们希望以防篡改的方式将数据从一个实体传输到另一个实体。MedRec[9]是另一个使用区块链技术的分散记录管理系统,MedRec是一个模块化设计,用于管理身份验证、机密性、责任性和数据共享。与MedRec类似,Ancile[10]是另一个记录管理系统,它利用智能合约和基于以太坊的区块链来提高访问控制和数据混淆。尽管使用区块链技术在改进医疗数据访问、共享和许可管理方面具有巨大潜力,但仍缺乏以数据为中心的研究,缺乏对网络中从一个实体传输到另一个实体后的数据控制的明确研究。为了遵守行业相关规定,确保患者数据安全和隐私对于健康信息交换的持续维持至关重要。从请求数据到系统发送应开始响应用户对系统中交互的监视。只有当数据达到了用户提出请求的目的或检测到违规行为时,这种监视才应终止。

区块链技术具有去中心化、不易篡改的特点,提出了一种基于区块链的医疗记录安全共享方案,其底层机制可以监控和执行附加到患者数据的可接受使用策略。系统中的患者在注册时创建策略,以确定对其个人健康信息的允许操作。这些策略存储在系统中,并与智能合约一起咨询,以确定何时可以共享数据或以其他方式共享数据。参与的医疗机构的处理节点、智能合约和安全监视器进行合作,以确保患者数据安全免受未经授权的访问和计算。

1 医疗记录共享方案

1.1 符号说明

方案主要涉及的变量符号和意义如表1所示。

1.2 系统模型

系统由患者(Patient)、医疗机构(Hospital)、区块链(Blockchain)3个部分构成,如图1所示。

患者:电子医疗记录的产生者,并对这些记录拥有所有权与控制权,患者可以在多个医疗机构间进行诊断治疗。

医疗机构:为医生与病人提供治疗的平台,负责保管医疗记录,同时可以跟其它医疗机构维持数据共享的关系。

区块链:将保存患者的医疗记录在分布式数据库当中的存储地址。区块链中的每笔交易都会返回一个标识符。交易标识符将帮助用户进一步访问数据。

表1 方案中的变量符号和意义

Tab.1 Symbols and its notions in our scheme

变量符号	意义
P	病人
ID_p	病人身份
P_p	病人公钥
S_p	病人私钥
EMR	电子医疗记录
$H(.)$	哈希函数
$Cert_p$	患者证书
T_0	时间戳

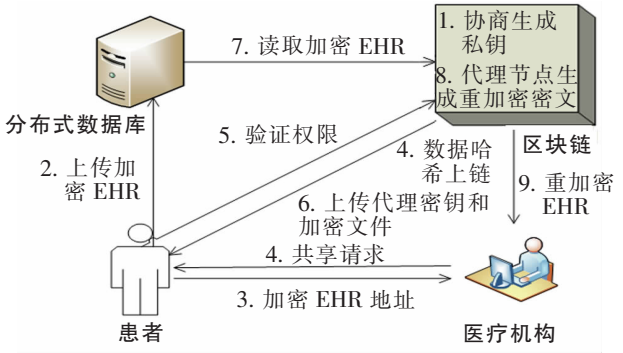

图1 基于区块链的电子医疗记录共享模型

Fig.1 Blockchain-based electronic health record sharing model

1.3　共享协议

根据提出的系统模型,采用一种基于证书的代理重新加密方案来做为电子医疗记录共享协议。具体的电子医疗记录共享协议由以下几个步骤组成:系统初始化,患者注册,加密医疗数据,数据共享,数据恢复。

1) 系统初始化:系统服务器给定特定的安全参数 k。首先,系统选择一个 k 位素数 q。 接下来,生成阶数为 q 的 ECC,并且定义相应的生成元点 P,用 G 表示 ECC 点组。选择一个随机值 $\alpha \in F_q^*$ 并计算 $P_\alpha=\alpha P$。选取 4 个不同的哈希函数。$H_1:G\times\{0,1\}^{32}\rightarrow F_q^*$,$H_2:F_q^*\times\{0,1\}^{64}\rightarrow F_q^*$,$H_3:G\times\{0,1\}^{64}\rightarrow F_q^*$,$H_4:F_q^*\times\{0,1\}^{64}\rightarrow F_q^*$,输出公共参数 $params=\{G,q,P,P_\alpha,H_1,H_2,H_3,H_4\}$和主密钥 $msk=\alpha$。

2) 患者注册:如果有新患者到达医院接受治疗,则患者必须先进行注册,然后再去看医生。 由于这是一次注册,因此他们需要使用他们的移动设备提供其详细信息,例如其身份 ID_p,其公钥 PK_p 和治疗他们的医生 PK_d 的公钥。为了便于解释,我们只考虑一位医生。并且亲戚也可以参与其中,其方式与医生相同,但仅具有阅读权限。接下来,系统将患者的 ID_p 和公钥 PK_p 发送给区块链。患者的证书和密钥生成采用一种基于椭圆曲线证书机制算法,包括以下三个阶段:

第一阶段:患者注册获得自己唯一的身份标识符 ID_U 并生成一个随机数 $r_U \in F_q^*$,并且计算 $R_U=r_UG$。接下来,将元组(ID_U,R_U)发送给系统。

第二阶段:系统收到(ID_U,R_U)后,将检查 ID_U 的合法性。接下来,它还会选择一个随机值 $r_t \in F_q^*$ 并且计算 $R_t=r_tP$。然后得出证书患者的证书 $Cert_U=R_U+R_t$。最后,通过 $r_\alpha=H_1(Cert_U\|ID_U)r_t+\alpha$ 计算得出有关实体的私钥的辅助信息。将元组$(r_\alpha,Cert_U)$发送给患者。

第三阶段:患者收到元组$(r_\alpha,Cert_U)$后,根据等式 $S_U=H_1(Cert_U\|ID_U)r_U+r_\alpha$ 计算出其私钥。由私钥得出患者的公钥为 $P_U=S_UP$。如果 $P_U=H_1(Cert_U\|ID_U)Cert_U+P_\alpha$。则患者接受密钥对$(S_U,P_U)$。

3) 加密医疗数据:为电子医疗数据 EMR 生成元数据 $meta=(ID_U\|T_0)$。接下来计算,进行以下计算

$$r=H_2(S_A\|meta),R=rP$$

$$C_A=M\oplus H_3(meta\|rP_A)$$

$$h_A=H_4(C_A\|meta)$$

$$s_A=r-h_AS_A$$

得到医疗记录的密文 C_A,该算法的输出结果为 C,$C=(C_A,meta,h_A,s_A)$。将 C_A 存储在分布式云服务器当中。患者作为 EMR 的拥有者对其进行签名,并将签名的 EMR、EMR 的哈希值,云存储地址和访问控制策略等写入区块链交易,然后将交易进行全网广播。由审核节点验证交易且验证通过后把该交易写入区块链当中。

4) 数据共享:当医疗机构 A 想读取医疗机构 B 的某一份 EMR 时,医疗机构 A 作为数据请求方,在区块链当中发布请求信息{askEMR},医疗机构 B 收到{askEMR}后,验证医疗机构 A 的身份是否合法,并且检查请求信息的访问控制策略,如果医疗机构 A 的身份合法且拥有电子医疗记录的读取权限。进行以下操作。首先,$r=H_2(S_A\|meta)$由 C 导出。然后 ID_B 的公钥 $P_B=H_1(Cert_B\|ID_B)Cert_B+P_\alpha$。得到电子医疗记录共享密钥 $rk_{AB}=H_3(meta\|rP_A)\oplus H_3(meta\|rP_B)$。此后,医疗机构 B 会将共享密钥、EMR 的云存储地址传送给代表节点,代表节点根据云存储地址提取分布式云存储数据库上的加密 EMR 文件。接着,代表节点使用共享密钥 rk_{AB} 对加密的 EMR 文件再次进行加密,将密文 C_A 转换为 C_B(其中 $C_B=rk_{AB}\oplus C_A$)。最后代表节点将 C_B 发送给医疗机构 A。

5) 数据恢复:当医疗机构 A 收到 C_B 时,使用自己的私钥 S_B 对 C_B 进行解密,解密后就可以得到 EMR 的的明文文件 M。具体解密过程如下:首先医疗机构 A 计算 $R=S_AP+h_AP_A$,然后计算 $M=C_B\oplus H_3(meta\|S_BR)$,计算所得 M 即为 EMR 的明文文件。如果患者想要查看自己的电子医疗记录,获取 EMR 的明文和上面类似,还需要进行以下计算

$$r=H_2(S_A||meta)$$

$$M=C_A\oplus H_3(meta||rP_A)$$

患者进行上面两步计算就可以获得自己的EMR文件的明文。

2 SMRSBC方案分析

2.1 正确性分析

2.3.1 患者密钥对的正确性

SMRSBC方案在患者注册阶段,把患者的证书和身份标识进行哈希加密生成患者的私钥,然后用患者的私钥计算出患者的公钥。患者可以验证等式$P_U=H_1(Cert_U||ID_U)Cert+P_\alpha$是否成立,如果成立,则患者接受密钥对$(S_U,P_U)$,否则这拒绝接受密钥对。

2.3.2 密文的正确性

在SMRSBC方案中,由于患者的电子医疗记录是存储在云服务器当中,患者的医疗记录虽然经过加密处理,但是云环境并不是可信的安全环境。恶意的攻击者可能会篡改加密之后的电子医疗数据,这样就会导致医疗机构B解密获得的明文并不是正确的。代表节点通过验证等式$h_A=H_4(C_A||meta)$是否成立,如果等式成立,则密文没有被篡改,否则密文已经被篡改过了。

2.2 安全性分析

1) 防篡改

在SMRSBC中,EMR是不可变的,不能任意修改。由于每个数据块都包含当前时间戳和前一个块的哈希,因此按时间顺序嵌套的块可确保事务无法更改,除非有人可以同时占据整个网络计算能力。此外,每个访问请求和访问活动都记录在区块链中,对数据的任何更改都可以进行审核和跟踪。因此,提出的SMRSBC可以确保防篡改特性。

2) 隐私保护

由于EMR是患者的高度敏感的私人数据,因此,它们不希望未经许可而被披露。在SMRSBC中,由于以下功能,确保了隐私属性:匿名,云储存。

匿名:每个参与者都会生成一个带有随机公钥的唯一帐户。因此,区块链上的每笔交易都是匿名的。另外,用户对不同的事务使用不同的公共密钥,这使得同一用户请求的多个事务无法链接。

云储存:原始EMR被加密并存储在云存储中。这样,不仅解决了区块链存储容量有限的问题,而且大大降低了原始医疗记录泄漏的风险。

3) 数据安全存储和共享

数据存储和共享的安全性是SMRSBC的重要功能。在此方案中,患者可以完全控制自己的EMR。从数据获取到数据共享的过程都是安全的。

数据存储:患者对原始EMR进行加密并将其存储在云中。在云中使用分布式存储可确保医疗数据的安全性。

数据发布:首先,EMR的索引保留在防篡改区块链中,不能随意修改。其次,区块链是一个没有单点故障的分布式数据库,每个节点都有交易记录的副本。此外,数字签名还为每笔交易提供身份验证,完整性和不可否认性。

数据共享:在SMRSBC中,数据访问权限是在智能合约中预设的。仅授权用户或机构可以使用EMR。执行的访问记录存储在区块链中以跟踪数据的行为。一旦有人违反了访问规则或权限,数据所有者便有权撤销其访问权限。

2.3 方案对比

表2将SMRSBC方案和现有其它方案进行特性对比。从表2中的特性对比可以看出,SMRSBC方案和其它方案相比具有一定的优势。

表 2　方案对比
Tab.2　Scheme comparison

方案	区块链	访问控制	隐私保护	智能合约
Patientory[8]	√	√	√	×
BBDS[10]	×	√	√	×
MedRec[12]	×	√	√	×
Ancile[13]	√	√	√	×
SMRSBC	√	√	√	√

在传统的方案当中,要么把医疗记录存放在可信第三方的数据库当中,要么把区块链当成一个数据库,直接把医疗记录存放在区块链当中。把医疗记录存放在可信第三方的数据库当中,容易发生单点故障的问题,而直接把医疗记录存放在区块链当中,由于区块链的存储容量有限,一旦区块链网络当中的节点数量过多,现有数据存储技术,将存储不了完整的区块链账本,方案的可扩展性不强。而 SMRSBC 方案通过用区块链记录患者的医疗记录在云存储当中的地址,而把加密之后的患者医疗记录存储在分布式云存储服务器当中,可以很好的解决区块链存储数据容量有限的问题,并且该方案具有良好的扩展性。

3　结论

区块链技术的不断发展对传统的行业带来了较大的冲击,过于中心化的系统面临着诸多问题,如容易遭受单点失效、恶意篡改、隐私泄露等威胁。区块链技术的应用可以解决这些问题,区块链拥有跟分布式存储机制相当的容错与容灾性能,同时参与到区块链网络的节点之间并不需要互相信任,且其中所使用的密码体制与算法已经是在当前受到认可且足够安全的, 因此在医疗记录的存储与共享领域具有良好的前景。提出的 SMRSBC 方案将医疗记录的存储与共享分开,既减轻了区块链各个节点的负载,又提高了数据的隐私性,为建立一个保护病人隐私的医疗数据共享与存储生态平台奠定了基础。双链的使用避免了当前很多单链设计应用中吞吐量不高且数据较为混乱的现状, 但在具体的方案实现中可能会遇到一些挑战与问题。此外,当前的医疗记录共享中还面临着一些棘手的问题,例如各个医疗机构的数据不兼容,行业术语不统一,病人对区块链技术安全性的不信任等。

参考文献:

[1] BLESSING V,VARNAI P. Evidence on mechanisms and tools for use of health information for decision-making[M]. World Health Organization,2017.

[2] YUAN B,LIN W,MCDONNELLl C. Blockchains and electronic health records[J]. Mcdonnell mit edu,2016.

[3] ZEINALI N,ASOSHEH A,SETAREH S. The conceptual model to solve the problem of interoperability in health information systems[C]//2016 8th Int. Symp. Telecommun. IEEE,2016:684-689.

[4] ABOUELMEHDI K,BENI-HESSANE A,KHALOUFI H. Big healthcarendata: preserving security and privacy[J]. Journal of Big Data,2019,5(1):1.

[5] GAO J,ASAMOAH K O,SIFAH E B,et al. Grid monitoring:secured sovereign blockchain based monitoring on smart grid[J]. IEEE Access,2018,6:9917-9925.

[6] YUE X,WANG H,JIN D,et al. Healthcare data gateways:found healthcare intelligence on blockchain with novel privacy risk control[J]. Journal of Medical Systerns,2016,40(10):218.

[7] XIA Q,SIFAH E B,SMAHI A,et al. BBDS:Blockchain-based data sharing for electronic medical records in cloud environments [J]. Information,2017,2(8):44.

[8] XIA Q,SIFAH E B,ASAMOAH K O,et al. MeDShare:trust-less medical data sharing among cloud service providers via blockchain[J]. IEEE Access,2017,5:14757-14767.

[9] EKBLAW A,AZARIA A,HALAMKA J D,et al. A case study for blockchain in healthcare:med rec prototype for electronic health records and medical research data[C]//Proceedings of IEEE Open & Big Data Conferenle,2016,13:13.

[10] DAGHER G G,MOHLER J,MILOJKOVIC M,et al. Ancile:privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable Cites and S·ciety,2018,39:283-297.

A Secure Medical Record Sharing Scheme Based Blockchain

Zhang Lihua[1],Fu Donghui[2],Wan Yuanhua[2]

(1. School of Software,East China Jiaotong University,Nanchang 330000,China;
2. School of Electrical and Automation Engineering, East China Jiaotong University,Nanchang 330000,China)

Abstract:Electronic medical records are vital and highly sensitive private information in medical data and need to be shared frequently between hospitals. Sharing medical data is considered a key method to improve the quality of medical services and reduce medical costs. However, electronic medical records are currently stored in different hospitals, which hinders the sharing of patient medical data and poses a serious threat to patient privacy. In order to solve these problems, a secure medical record sharing scheme based blockchain (SMRSBC) is proposed. In SMRSBC, the original EMR is securely stored in the cloud storage server, and the index is kept in the tamper-resistant alliance blockchain. This means that the risk of medical data leakage can be greatly reduced, and at the same time, the index in the blockchain ensures that the EMR cannot be arbitrarily modified. Through the patient´s predefined access rights, the secure sharing of electronic medical data can be automatically completed through smart contracts on the blockchain. In addition, the use of elliptic curve encryption and asymmetric encryption technology in the patient´s electronic medical data storage and extraction phases can protect the patient´s privacy well. Analysis shows that SMRSBC is a safe and effective method to realize EMR data sharing.

Key words: blockchain;medical record;privacy protection;storage and sharing