DOI:10.13878/j.cnki.jnuist.2019.05.008

孙回[1,2]　程徐[1,2]　黄琤[1,2]　陈付龙[1,2]

基于医疗联盟链的数据安全保护方法

摘要

随着互联网的飞速发展,医疗数据爆炸性增长,大量的医疗数据面临着安全共享问题.本文提出了一种基于医疗联盟链的数据安全保护方法,其中包括提出了一种安全认证与访问控制模型,并将查询逻辑分离存储技术引入该模型中,同时描述了基于医疗联盟链的认证凭据和访问权限数据的存储和访问.基于医疗联盟链的安全认证与访问控制模型包含了三个角色,第一角色是患者,第二角色是医护人员,第三角色是医疗联盟链.通过查询逻辑分离存储技术保护患者数据隐私,查询逻辑分离技术与医疗联盟链技术紧密结合,满足了不同医院之间医疗数据共享的需求,保障了患者的数据隐私和医护人员查阅数据的权限.

关键词

医疗联盟链;数据安全;安全认证;访问控制

中图分类号 TP309.2

文献标志码 A

收稿日期 2019-09-09

资助项目 国家自然科学基金(61972438)

作者简介

孙回,女,硕士生,研究方向为信息物理融合系统.sunhui@ahnu.edu.cn

陈付龙(通信作者),教授,研究方向为嵌入式与普适计算、信息物理融合系统、高性能计算机体系结构、物联网安全.long005@ahnu.edu.cn

1 安徽师范大学 计算机与信息学院,芜湖,241002

2 网络与信息安全安徽省重点实验室,芜湖,241002

0 引言

在现代社会,医学数据传播的关键驱动力在于专业人员对医疗数据进行数字化、电子存储和远程访问[1].随着技术时代的到来,以及随后大量数据的收集,这些数据已经进入了大数据时代,共享数据为仍在探索中的前景提供了诱人的价值[2].如果把敏感数据(医疗记录等)存放在由他人控制的云存储环境中,随着云存储使用者增多,数据安全问题会日趋严重[3].传输安全和存储安全是保护数据安全中重要的部分,存储信息的泄露将会导致非常严重的后果,因此必须保证其安全性[4].在云存储中,用户通常既不知道其数据的确切位置,也不知道与其一起存储的其他数据源[5].这从某种意义上来说,对数据安全起到一定的保护作用.

当前医疗行业存在医疗数据难以共享的难题,大量的医疗数据主要储存在中心化的少数权威机构中,并且由于数据储存的标准与系统不同,共享这些医疗数据是一件非常困难的事情.医疗数据在诊断、治疗、康复和医疗事故调查中具有重要意义,而医疗数据的完整性和可用性是这些活动顺利开展的基本保证,因此医疗数据的隐私性是医疗数据敏感性的自然要求[6].

互联网在提高生产力、效率等方面具有促进经济增长和全球竞争力的潜力.这一最新的技术变革浪潮将给我们的社会带来新的机遇和新的风险[7].大规模的数据在传输、存储和访问过程中面临着数据泄露的风险[8].随着移动互联网与物联网技术的发展,网络空间承载了海量数据,必须保证其安全性和隐私性[9].

在卡巴斯基 2016 年的安全公告中显示,医疗保健行业处于被勒索软件袭击的前 10 名行业.2017 年 4 月,勒索病毒 WannaCry 使英国的近 80 个国家卫生服务机构瘫痪,造成重要信息被窃取、个人隐私被偷拍等灾难性的破坏[10].在黑市上,个人医疗信息的价值比信用卡信息高 50 倍.如何在共享个人医疗数据的同时保障个人隐私与安全,是现今医疗大数据发展的一个非常关键的痛点.

随着区块链[11]、大数据、移动互联等技术的高速发展,医疗大数据对安全性的要求也越来越高.区块链通过集成 P2P 协议、非对称加密、共识机制、块链结构等多种技术,解决了数据的可信问题.通过应用区块链技术,无需借助任何第三方可信机构,互不了解、互不信任的多方可实现可信、对等的价值传输[12].由于攻击区块链必须在纳米级时间内完

成51%的节点攻击[13],所以攻击区块链的难度过大、成本过高,区块链中存储的数据无法被轻易篡改.利用区块链的这些特性,就可以将医疗数据长期保存并且对各项数据以数字签名的方式进行标记,实现数据的可追溯性.区块链技术可利用其可溯源性质来实现医疗记录和健康档案的实时保护.黄铭钧等创立的Medilot团队开发了一款医疗区块链,取名美迪乐.美迪乐使用收集的数据用于预测性健康报告等,提出私有区块链框架BlockBench[14]和用于区块链和分叉应用的高效存储引擎ForkBase[15],并且得到新加坡国立大学和多家医疗机构的支持.Gem公司开发了医疗和供应链管理的区块链应用.Gem医疗网络是基于以太坊开发的,通过许可链增加安全性,以便患者控制访问,同时任何更改都记录在一个共享的记账系统中.

国内外的一些企业也将区块链技术应用在医疗领域.例如,PokitDok公司在2016年10月首次提出区块链计划,叫做DokChain[16],DokChain是一个“医疗领域的财务数据和临床数据的交易处理器的分布式网络”.Patientory公司正在构建一个符合HIPAA标准的、基于区块链的健康信息交换系统(HIE)[17],以增强EMR互操作性以及强化数字安全协议.Chronicled公司为供应链和物联网客户构建了具有独特目的的区块链应用,拥有从医疗设备和制药到包裹追踪的一系列应用.

1 基于医疗联盟链的安全认证与访问控制模型

现代医疗数据的需求主要包括共享需求和安全需求.通过对互联网安全问题的研究发现,现代社会中基因、指纹等重要健康数据一旦被大规模泄露,将会产生灾难性后果.由此,需要设计基于医疗联盟链的安全认证与访问控制模型来保障数据安全,同时引入新的数据隐私保护方法保障医疗大数据的安全.

在敏感数据保护中存在的安全隐患包含信息篡改、删除、错误升级等,将区块链技术引入可以保证医疗数据的真实完整,并能完全记录医疗数据变更过程,从而实现医疗记录和健康档案的实时保护.同时,设计数据采集过程,建立数据安全传输通道,可以保障数据在联盟链上的安全存储.将医疗联盟链和数据隐私保护技术相结合,可以保障医疗大数据的安全.

现有医疗物理信息融合系统难以实现医疗数据共享,通过结合区块链透明开放的特征可实现医疗数据的安全共享.因此,本文提出了一种基于医疗联盟链的安全认证与访问控制模型,如图1所示.在本文提出的基于医疗联盟链的安全认证与访问控制模型中,主要包含3个角色:患者、医护人员、医疗联盟链.患者与医疗联盟链之间的操作主要包括:请求认证、数据上传.医护人员与医疗联盟链之间的操作主要包括:请求认证、数据下载.医疗联合体负责为医疗联盟链提供技术支持,医疗联合体主要包括:区域内的三级医院、二级医院、社区医院、村医院等.患者通过认证后上传数据到医疗联盟链,医护人员通过安全认证后从医疗联盟链上下载数据,医护人员与患者安全认证之后获得数据逻辑的访问权限,完整的患

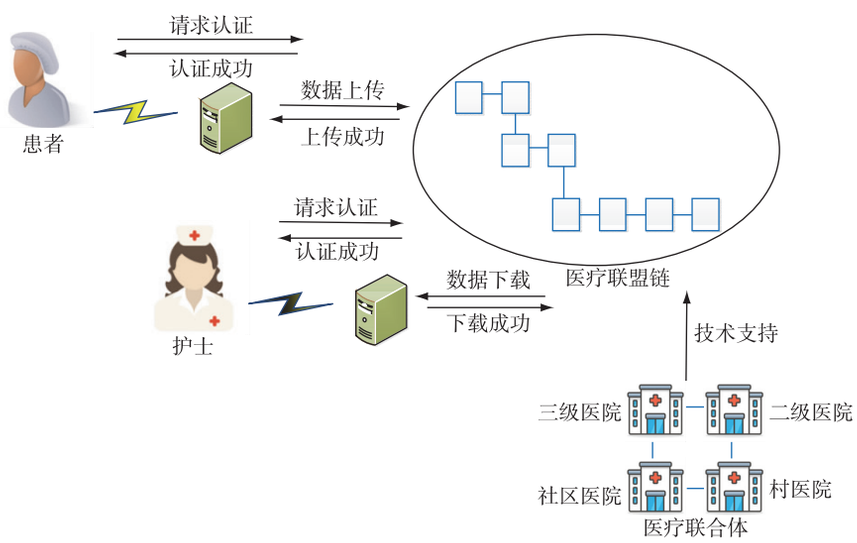

图1 基于医疗联盟链的安全认证与访问控制模型

Fig. 1 Security authentication and access control model based on medical alliance chain

者病历数据=数据(从医疗联盟链上下载)+数据逻辑(从患者处获取).

2 查询逻辑分离存储技术在医疗联盟链中的应用

Xiao 等[18]提出了一种查询逻辑分离存储的QLDS算法,该算法的核心思想是将提取的查询逻辑存储在用户的客户端,将未集群的位置元组存储在后端服务器,有效保证了用户的轨迹隐私.王涛春等[19]改进了这种QLDS算法用于保护轨迹隐私.本文中也使用到查询逻辑分离存储的思想.

查询逻辑分离技术在医疗联盟中的应用如图2所示,主要思想是将提取的查询逻辑存储在患者的客户端,将加密处理后的数据存储在医疗区块链中,有效地保证了患者的医疗数据隐私.

1)采集患者数据,生成一份完整的电子病历 emr,然后对电子病历进行加密处理 $E(emr,k)$.这里的 $E()$ 表示加密操作,k 表示密钥,emr' 用于表达加密处理后的电子病历.

2)医疗数据切片.患者终端将医疗数据分割为医疗数据元组,操作为 $d(emr')$.$d()$ 表示为切片操作,切片后的数据可以表示为 $data=(x,y,t,l,d,\cdots)$.

3)将医疗数据元组按照地址表 $addr$ 进行数据置换,输入的数组按随机生成的地址表进行重新组合,具体操作如图2所示.但为了患者和医护人员能够对医疗数据进行重建,所以需要存储地址表.经过置换后的数据可以表示为 $data'=(x',y',t',l',d',\cdots)$.

4)数据上传.将 $data'$ 上传到医疗联盟链,由于姓名、位置、医生信息等关键信息都经过加密处理和置换处理,大大降低了数据重建的概率.

对于医护人员,基于医疗联盟链的数据下载如图3所示.

1)数据下载.医护人员在与医疗联盟链认证成功后,在医疗联盟链上下载患者的数据 $data'$.

2)将医疗数据元组按照地址表 $addr$ 进行数据置换,输入的数组地址表进行重新组合,经过置换后的数据可以表示为 $data=(x,y,t,l,d,\cdots)$.

3)置换后的数据组合成加密后的电子病历,对该病例进行解密处理 $D(emr,k)$,生成一份完整的电子病历 emr.

3 基于医疗联盟链的认证凭据和访问权限数据的存储和访问

3.1 基于医疗联盟链的认证凭据和访问权限数据的存储

患者凭据记录保存的是认证凭据,患者使用凭据记录完成与医疗联盟链的认证.患者对于医疗联盟链上的数据有读和写的权限.

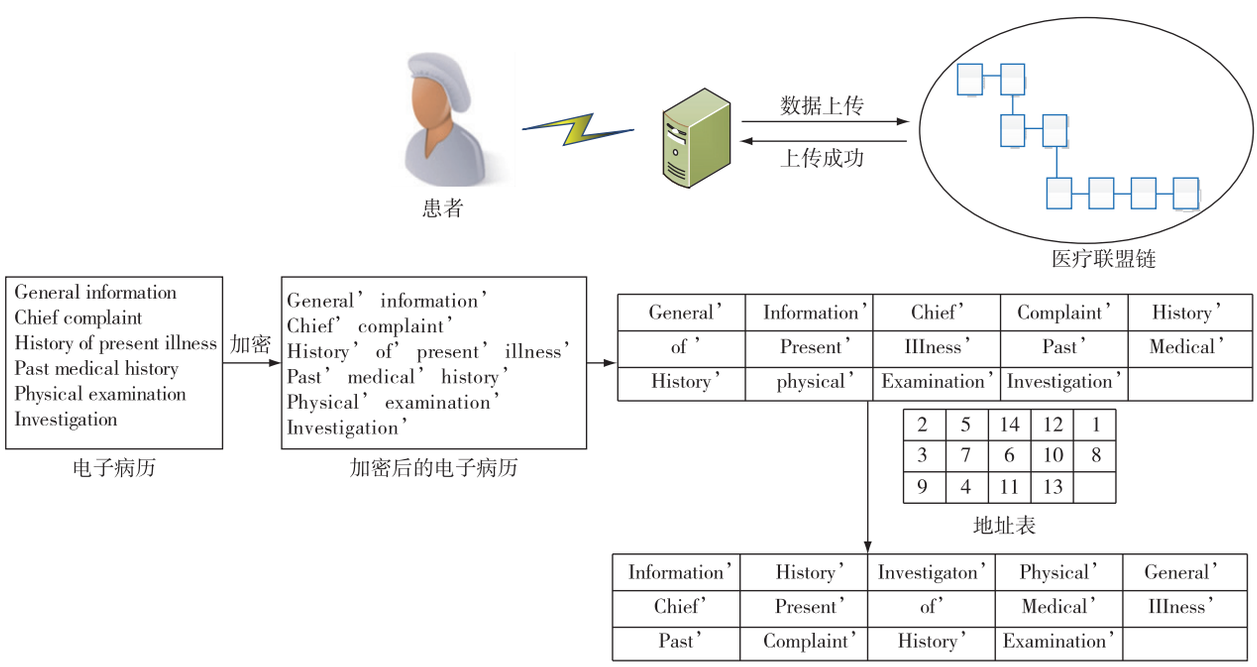

图2 基于医疗联盟链的数据上传

Fig. 2 Data upload based on medical alliance chain

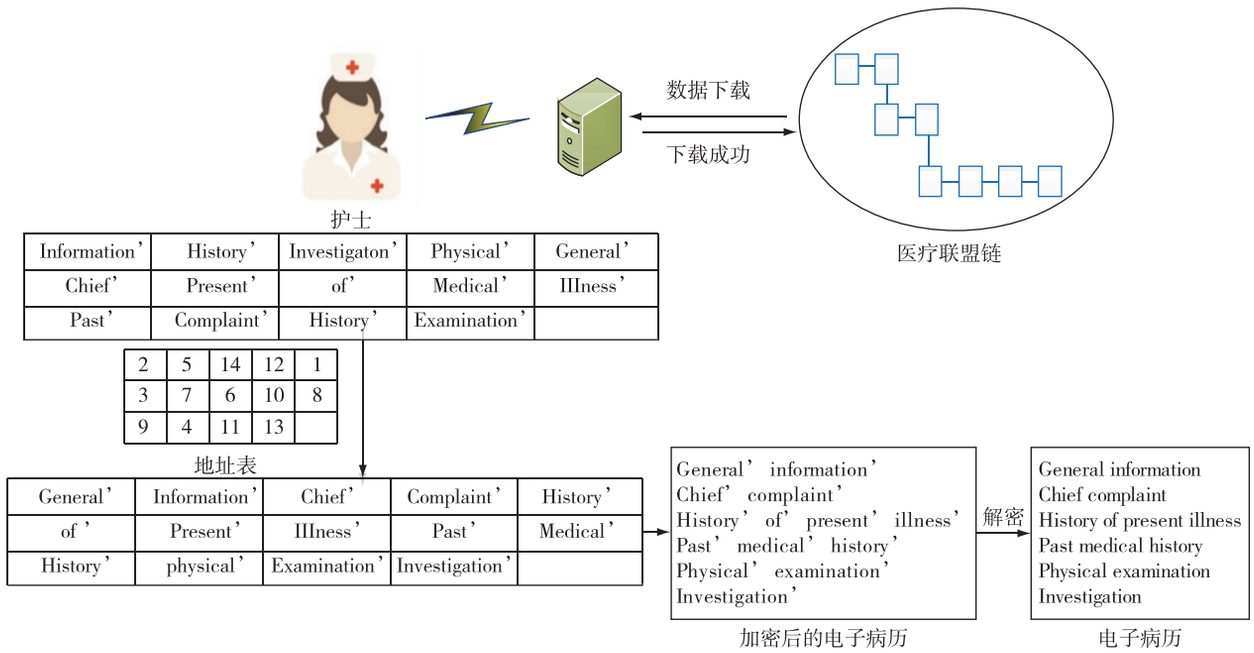

图 3　基于医疗联盟链的数据下载

Fig. 3　Data download based on medical alliance chain

医护人员的权限凭据记录保存的是医护人员的权限凭据,医护人员使用权限凭据记录完成与医疗联盟链的认证.医护人员对于医疗联盟链上的数据有读的权限.

大量的认证凭据记录和权限记录构成的哈希树存储在区块链上,认证凭据记录和权限凭据记录存储在医疗联合体构建的云存储平台上,即通过集群存储的方式实现大量认证凭据记录和权限凭据记录的存储.用户通过统一访问接口透明地访问和利用所有存储设备中的凭据记录.

凭据记录中的符号说明如表 1 所示.

表 1　符号说明

Table 1　Symbol description

符号	说明
a	用户账号(地址).地址 a 通常是由公钥计算得来,将公钥作为输入,使用单向加密哈希函数生成地址,这个生成方向是单向的
hs	用户凭据数据摘要
us	用户签名
ds	医生签名,可表示为 $ds=E(hs,pkd)$
pku	用户公钥
pkd	医生公钥
sku	患者私钥,即随机选出 256 位二进制数字.私钥代表用户对数据的所有权,若私钥丢失,则数据所有权(数据访问权限包括访问权限、授权访问权限等)也丢失

凭据记录可表示为 $\{a,hs,us,ds,pku,pkd\}$. 患者在医院的计算中心注册、身份认证后可以获得私钥 sku.公钥是用户的账户.公钥用于生成地址,同时也进行签名的验证.公钥可以生成对应的唯一地址,通过该地址可以确认用户的凭据数据存放位置.

用户签名可表示为 $us=E(hs||(pku'||pkd),sku)$,用户使用 sku 加密凭据数据摘要 hs 和下一个用户以及参与本次诊疗的医生的公钥 $pku'||pkd$,确定消息的完整性.大量凭据记录组成了一个区块,由全医疗系统中的医院计算中心节点采用竞争机制来争夺区块记账权.竞争机制以工作量证明为基础,一般是要求用户进行一些耗时适当的复杂运算,并且答案能被服务方快速验算,以此耗用的时间、设备与能源作为担保成本,以确保服务与资源是被真正的需求所使用.

获取区块记账权的医院计算中心节点将获得一定的奖励,每个区块的第一笔交易进行特殊化处理,该交易产生一枚由该区块创造者拥有的代币.区块链是所有的区块以双向链表的方式链接起来的链表,且每个区块都会保存其上一个区块的 Hash 值,保障区块之间的顺序不可篡改,这一技术保障了区块链的安全性.

3.2　基于医疗联盟链的认证凭据和访问权限数据的访问

$us=E(hs||(pku'||pkd),sku)$,每一位所有

者通过对前一条凭据数据摘要和下一位拥有者(患者和参与本次诊疗的医生)的公钥签署一个随机散列的数字签名,并将这个签名附加在这条凭据记录的末尾.这条凭据记录可以表示为{a,hs,us,ds,pku,pkd},发送给下一位所有者.而下一位所有者通过对签名进行检验,就能够验证该凭据记录的所有者.

用户查询一条凭据数据时,需要向医院服务中心提出查询申请,提供自己的私钥sku用于定位存储在各医院服务器上的凭据数据,服务中心使用哈希算法生成凭据数据摘要 $hs' = h(a,hs,us,ds,pku,pkd)$.同时,用户使用自己的私钥在链上进行认证,获取自己在链上存储的凭据记录中的凭据数据摘要.通过对比两个凭据数据摘要的一致性 $verify(hs,hs')$ 来实现患者的身份认证.

4 结论

随着医疗物联网的发展和5G时代的到来,医疗大数据的存储安全问题会得到更多的关注,将区块链技术应用到医疗共享问题的解决方案中,可以有效地保障患者隐私.同时,医疗数据还需要更多高效、安全的保护方法,尤其在数据采集、数据传输过程中,都存在着一定的数据泄露风险.本文提出了一种基于医疗联盟链的安全认证与访问控制模型,同时将查询逻辑分离存储技术应用在医疗联盟链,为医疗数据的安全访问、存储提供了一种新思路.

参考文献

References

[1] Kavsak P A. The International committee of medical journal editors proposal for sharing clinical trial data and the possible implications for the peer review process[J]. Annals of Translational Medicine,2016,4(6):115-116

[2] Chen M, Mao S W, Liu Y H. Big data: a survey[J]. Mobile Networks and Applications, 2014, 19(2): 171-209

[3] 薛矛,薛巍,舒继武,等.一种云存储环境下的安全存储系统[J].计算机学报,2015,38(5):987-998
XUE Mao, XUE Wei, SHU Jiwu, et al. A secure storage system over cloud storage environment[J]. Chinese Journal of Computers,2015,38(5):987-998

[4] 王小康,杨明.安全存储技术的进展和思考[J].计算机与信息技术,2006,14(增刊1):92-95
WANG Xiaokang, YANG Ming. Progress and consideration of secure storage technology[J]. Computer and Information Technology,2006,14(sup1):92-95

[5] Kaufman L M. Data security in the world of cloud computing[J]. IEEE Security & Privacy Magazine,2009,7(4): 61-64

[6] Tian H B, He J J, Ding Y. Medical data management on blockchain with privacy[J]. Journal of Medical Systems, 2019,43(2):26

[7] Choo K K R, Gritzalis S, Park J H. Cryptographic solutions for industrial Internet-of-Things: research challenges and opportunities[J]. IEEE Transactions on Industrial Informatics,2018,14(8):3567-3569

[8] Chen F L, Luo Y L, Zhang J, et al. An infrastructure framework for privacy protection of community medical Internet of Things[J]. World Wide Web,2018,21(1): 33-57

[9] 陈烨,许冬瑾,肖亮.基于区块链的网络安全技术综述[J].电信科学,2018,34(3):10-16
CHEN Ye, XU Dongjin, XIAO Liang. Overview of block chain-based network security technologies[J]. Telecommunications Science,2018,34(3):10-16

[10] 刘杰杰.计算机病毒的发展趋势分析及防控策略探究[J].科技展望,2017(3):11
LIU Jiejie. Trend analysis of computer virus development and exploration of prevention and control strategy[J]. Prospect of Science and Technology,2017(3):11

[11] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].(2017-02-03)[2019-08-08].https://bitcoin.org/bitcoin.pdf

[12] 张健.区块链:定义未来金融与经济新格局[M].北京:机械工业出版社,2016
ZHANG Jian. Block chain: defining the new financial and economic pattern in the future[M]. Beijing: Machinery Industry Press,2016

[13] Lee I, Sokolsky O, Chen S J, et al. Challenges and research directions in medical cyber-physical systems[J]. Proceedings of the IEEE,2012,100(1):75-90

[14] Dinh T T A, Wang J, Chen G, et al. Blockbench: a framework for analyzing private blockchains[C]// Proceedings of the 2017 ACM International Conference on Management of Data. ACM,2017:1085-1100

[15] Wang S, Dinh T T A, Lin Q, et al. Forkbase: an efficient storage engine for blockchain and forkable applications[J]. Proceedings of the VLDB Endowment, 2018, 11(10):1137-1150

[16] 医疗区块链蓄势待发,2017年取得10大关键突破[J].医学信息学杂志,2018(2):93

[17] Willoughby S. Tech & health care[J]. Network Journal, 2019,26(1):10-11

[18] Xiao Z, Yang J J, Huang M, et al. QLDS: a novel design scheme for trajectory privacy protection with utility guarantee in participatory sensing[J]. IEEE Transactions on Mobile Computing,2018,17(6):1397-1410

[19] 王涛春,刘盈,金鑫,等.群智感知中基于k-匿名的位置及数据隐私保护方法研究[J].通信学报,2018,39(增刊1):176-184
WANG Taochun, LIU Ying, JIN Xin, et al. Research on k-anonymity-based location and data privacy protection methods in group intelligence perception[J]. Journal of Communications,2018,39(sup1):176-184

Data security protection method based on medical alliance chain

SUN Hui[1,2] CHENG Xu[1,2] HUANG Zheng[1,2] CHEN Fulong[1,2]
1 School of Computer and Information, Anhui Normal University, Wuhu 241002
2 Anhui Provincial Key Laboratory of Network and Information Security, Wuhu 241002

Abstract With the rapid development of Internet and explosive growth of medical data, the sharing of medical data results in serious security concerns. A data security protection method based on Medical Alliance Chain (MAC) is proposed, which includes a security authentication and access control model. The query logic detached storage technology is introduced into the model to protect patients' data privacy. The storage and access of authentication credentials and access authority data are elaborated based on MAC. The security authentication and access control model based on MAC involves three roles of patients, medical staff, and the MAC. The query logic detached technology and the MAC are closely integrated to meet the needs of secure medical data sharing between different hospitals, and to protect patients' data privacy as well as the right of medical staff to access data.

Key words medical alliance chain; data security; security authentication; access control