山西大学学报(自然科学版)48(6):1152—1160,2025
Journal of Shanxi University(Nat. Sci. Ed.)

DOI:10.13451/j.sxu.ns.2024033

基于联盟链和商密九号算法的安全可共享电子病历方案

赵鹏,张少康*,李笑,唐静芸,赵伟
(太原师范学院 计算机科学与技术学院,山西 晋中 030619)

摘 要:针对电子病历系统存在的隐私保护、数据安全和存储、数据共享等方面的问题,提出一种基于联盟链和商密九号算法的解决方案。该方案通过脱敏技术和商密九号算法对电子病历进行隐私保护和加密处理。利用星际文件系统存储电子病历加密文件,采用联盟链存储其索引,实现电子病历的轻量化存储。同时,采用智能合约对文件进行搜索和访问控制,并通过商密九号算法加密序列密钥,以实现电子病历的安全共享。最后对该方案进行了全面的性能分析,并与现有方案进行了全面对比。对比结果显示,在结构方面,本方案采用单链结构,相较双链结构方案,降低了系统的复杂性;在存储方面,采用星际文件系统传输模式,相较于传统的文件传输模式,大病历文件的上传时间平均缩短了13倍左右;在通信方面,相较于未使用商密九号算法的方案,本方案一次通信时间缩短了30多毫秒。

关键词:隐私保护;数据共享;脱敏技术;星际文件系统;智能合约;访问控制
中图分类号:TP309.7 **文献标志码**:A **文章编号**:0253-2395(2025)06-1152-09

Secure and Shareable Electronic Medical Record Scheme Based on Consortium Blockchain and SM9

ZHAO Peng, ZHANG Shaokang*, LI Xiao, TANG Jingyun, ZHAO Wei
(*School of Computer Science and Technology, Taiyuan Normal University, Jinzhong* 030619*, China*)

Abstract: In view of the problems of privacy protection, data security and storage, data sharing and other aspects in the electronic medical record system, a solution based on the consortium chain and the SM9 algorithm is proposed. This solution uses desensitization technology and the SM9 algorithm to protect the privacy and encrypt the electronic medical records. The encrypted electronic medical record files are stored using the InterPlanetary File System (IPFS), and the consortium chain is used to store its index to achieve lightweight storage of electronic medical records. At the same time, smart contracts are used to search and access control files, and the SM9 algorithm is used to encrypt the serial key to achieve secure sharing of electronic medical records. Finally, a comprehensive performance analysis of the solution is conducted, and it is comprehensively compared with existing solutions. The comparison results show that in terms of structure, this solution adopts a single-chain structure, which reduces the complexity of the system compared with the double-chain structure solution. In terms of storage, the IPFS transmission mode is adopted, which shortens the upload time of large medical records by an average of 13 times compared with traditional file transmission modes. In terms of communication, compared with solutions that do not use the SM9 algorithm, this solution shortens the communication time by more than 30 milliseconds.

Key words: privacy protection; data sharing; desensitization technology; IPFS; smart contract; access control

收稿日期:2023-09-16;**接受日期**:2024-03-08
作者简介:赵鹏(1973—),男,山西太原人,博士,教授,研究方向为区块链技术。E-mail:13935134499@139.com
* **通信作者**:张少康(ZHANG Shaokang),E-mail:15225075987@163.com
引文格式:赵鹏,张少康,李笑,等.基于联盟链和商密九号算法的安全可共享电子病历方案[J].山西大学学报(自然科学版),2025,48(6):1152-1160. DOI:10.13451/j.sxu.ns.2024033.

0 引言

在21世纪医疗领域,电子病历(Electronic Medical Records,EMRs)已经取代传统的纸质病历,成为病患管理的关键工具。电子病历的引入有效地解决了存储、查询、数据共享以及医疗错误等方面的问题,为患者提供了更全面的诊断信息[1]。然而,当前的电子病历系统面临着数据安全和共享方面的多重挑战。传统的存储和共享方式存在着数据泄露、篡改和未经授权访问的风险,这不仅可能导致个人身份信息的泄露,还可能对患者的隐私和安全构成威胁。此外,医疗机构之间的数据共享也面临着隐私保护和数据一致性的问题。目前存在的一些电子病历系统方案设计复杂,实施起来较为困难。

为解决这些问题,区块链技术作为一种新兴的分布式账本技术,在医疗领域得到了广泛的应用。区块链以其去中心化、不可篡改和匿名性等特点,为电子病历提供了平台支持,并提供了多种解决方案来应对电子病历系统中的数据安全和共享问题[2]。薛腾飞等[3]提出了一种基于区块链的医疗数据共享模型,该模型通过代理重加密的方式实现了数据安全共享。毕娅等[4]通过双链结构实现了医疗数据的安全共享,文献[5]采取了一种无证书的基于身份和类型的加密方式,利用DPOS(Delegated Proof of Stake,委托权益证明)共识算法选取代理节点,以此来抵抗身份伪装或者重放攻击,从而保证数据的安全。周正强等[6]提出了一种基于联盟链的医疗数据共享模型,该模型通过云存储器存储加密数据,利用联盟链存储数据的元数据,并通过属性加密技术实现数据的安全共享。文献[7]则采用智能合约的方式实现对病历数据的访问控制。

然而,尽管区块链技术在解决电子病历系统中的安全和共享问题上具有潜力,但仍存在一些挑战。首先,传统的公钥密码体制中,需要通过第三方机构(如证书颁发机构)签发数字证书来验证公钥的真实性,这增加了系统的复杂性和成本。其次,现有的加密算法可能存在着密钥过长、加解密效率低下等问题,不太适用于医疗领域中对实时性和效率要求较高的场景。

因此,为了克服这些问题,本文提出了一种基于联盟链和商密九号算法的安全可共享电子病历方案。商密九号算法(简称SM9)是一种基于双线性对的标识密码体制,与传统公钥密码体制不同,它避免了需要CA(Certificate Authority)中心签发数字证书的过程,降低了系统的复杂性和成本[8]。同时,SM9算法具有密钥短、高安全性和高效的加解密特性,非常适用于医疗领域的电子病历数据和患者身份信息的保护[9-18]。此外,本方案利用星际文件系统(InterPlanetary File System,IPFS)进行文件存储,通过联盟链存储索引,形成了"链下存储,链上索引"的轻量化存储模式,并通过SM9算法加密序列密钥实现了安全共享。

本文工作安排如下:第1节介绍准备工作;第2节描述本系统方案的具体设计过程;第3节是对系统方案的功能和效率分析;第4节总结和展望。

1 准备工作

1.1 双线性映射

定义:令G_1和G_2为两个阶为素数的乘法循环群,定义一个双线性映射$e:G_1\times G_1\rightarrow G_2$满足以下性质:

1)双线性:对于任意$a,b\in Z_q^*$和$x,y\in G_1$,$e(x^a,y^b)=e(x,y)^{ab}$成立;

2)非退化性:存在$x,y\in G_1$,使得$e(x,y)\neq 1$;

3)可计算性:对于任意的$x,y\in G_1$,存在有效的算法计算$e(x,y)$。

1.2 SM9算法

SM9算法是一种基于双线性对的国密标识密码算法,利用用户标识(如手机号、邮箱号码等)生成密钥对,无需传统PKI(Public Key Infrastructure)体系中的密钥库和CA证书中心签发证书,从而大大降低了计算成本。SM9算法基于双线性对,具有高安全性和较短的密钥长度,加解密和签名速度快,因此,SM9算法在数字签名、加密、密钥交换等密码学应用中得到广泛应用。彭聪等[19]基于SM9算法提出了一种环签名方案,该方案利用SM9算法实现了环

签名,具有通信开销方面的优势,同时能够在保护用户隐私的前提下,对数据进行身份验证并保持数据的匿名性。张超等[20]结合SM9算法设计了一种可搜索加密方案,该方案通过使用SM9算法进行可搜索加密,可以在保护数据安全性和隐私的前提下,实现对加密数据的搜索和检索功能。该方案被证明在安全性和效率方面均表现出较高水平。

1.3 IPFS

IPFS是一种分布式文件系统,旨在创建一个全球性的、点对点的文件传输协议和网络,使用户可以在网络上共享、存储和访问文件,不依赖任何中心化服务器。通过加密和哈希算法,IPFS可以确保数据的安全性和完整性。与传统的HTTP协议不同,IPFS使用哈希值标识文件和数据,而非URL地址,从而提供更快速、更安全和更可靠的文件传输服务。其工作原理是将文件和数据分割成小块后,使用哈希算法对每个小块进行加密和验证,并将它们存储在网络的不同节点上。当用户请求文件时,IPFS会从多个节点上获取对应小块,重新组装成完整的文件并返回给用户。这种分布式存储和传输的方式,可以提高文件的可用性和可靠性,并降低网络拥塞和服务器负载压力。

1.4 联盟链

联盟链是一种特殊的区块链,由多个组织或实体共同维护和管理,这些组织或实体之间有一定的信任关系,并共同管理和控制区块链网络。相较于公共区块链,联盟链具有更高的效率、更好的隐私保护和更强的控制能力。由于其参与者是有限的且预先选定的节点,联盟链可以处理更多的交易,并更快地达成共识。此外,联盟链的成员可以选择隐藏部分信息,以增强隐私保护。最后,联盟链的成员对网络进行更多的控制,包括决定网络准入、规则修改和更新等。

1.5 智能合约

智能合约是一种基于区块链技术的自动化合约,由计算机程序编写而成,旨在控制交易的执行和结果,无需任何中间人或第三方的介入。智能合约具有高度的可靠性、透明性和自动化性。由于它们运行在区块链上,所有的交易记录均为公开,同时也无需第三方进行验证或监管,从而大大降低了交易成本和时间。此外,智能合约还可以避免人为的错误和欺诈行为,从而提高了交易的安全性和可信度。

2 系统方案总体设计

2.1 系统方案框架设计

在本方案中,由医院之间组成联盟链,并组成IPFS集群。方案采用SM9算法对电子病历进行加密,并将加密后的文件上传至IPFS节点存储,IPFS节点返回文件索引值并上传至联盟链存储。然后使用智能合约对数据进行搜索,最后使用SM9算法加密序列密钥的方式进行安全共享。在本方案中,共涉及六个实体,包括患者、医生、医院、IPFS集群、联盟链和第三方用户。方案框架如图1所示。

1)患者:患者首先在医院服务器上注册,在注册过程中,患者需设置自己的账号、密码以及身份信息,并创建一个唯一的标识,同时,患者需要保存由密钥生成中心(Key Generation Center,KGC)生成的私钥,以及在加密病历时生成的序列密钥。患者可根据自己的标识获取加密后的电子病历,然后通过私钥进行解密,得到自己的电子病历。

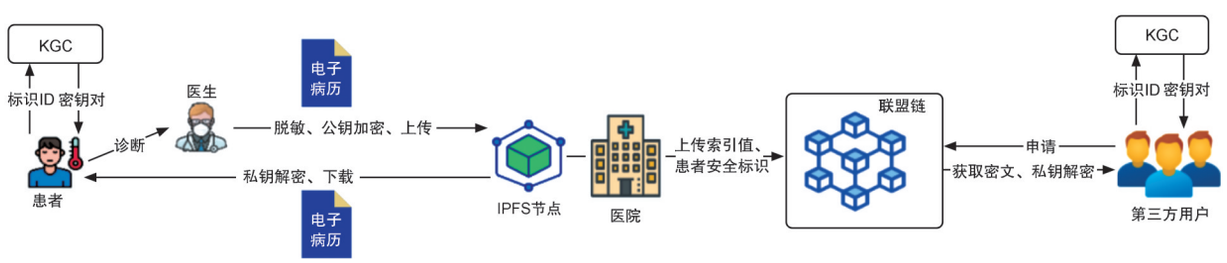

图1 电子病历系统模型图

Fig. 1 System model of electronic medical record

2)医生:医生首先运行脱敏算法,对电子病历进行处理。然后,医生使用公钥将电子病历加密。在SM9算法加密的过程中,会生成一个序列密钥用于加密明文,这个序列密钥由患者保管。医生将加密后的电子病历存储在医院的IPFS节点中,并在得到患者授权的情况下,进行电子病历的管理。

3)医院:医院将IPFS为加密电子病历生成的索引值和对应的患者的安全标识一并上传至联盟链节点。

4)IPFS集群:该集群由各医院共同组成,用于存储加密后的电子病历文件。

5)联盟链:联盟链由各大医院机构共同构建,用于存储由IPFS生成的索引值和所对应患者加密后的标识,可使用智能合约通过标识查询索引值,并通过索引值查询IPFS上存储的密文。

6)第三方用户:第三方用户需要将自己加密后的标识和公钥通过智能合约发送给患者。若得到患者授权,患者则在本地运行SM9算法,使用第三方用户公钥加密保存的序列密钥,通过智能合约返回被授权用户,被授权用户通过私钥解密序列密钥,通过序列密钥解密明文得到电子病历。

2.2 具体方案设计

(1)系统初始化

(a)初始化参数

系统选择256位BN(Barreto-Naehrig)椭圆曲线,选取G_1和为两个素数N阶的循环加群,G_T是素数N阶的乘法循环群,P_1和P_2分别是群G_1和G_2的生成元。存在G_1到G_2的同态映射ϕ使得$\phi(P_2)=P_1$,双线性对e是$G_1\times G_2\rightarrow G_T$的映射且满足$e([a]P_1,[b]P_2)=e(P_1,P_2)^{ab}$。

(b)密钥生成

由密钥生成中心KGC为患者生成随机数$k\in[1,N-1]$,作为加密主私钥,通过计算G_1中元素$Pub_k=k\times P_1$作为加密主公钥,患者在注册时选取自己的唯一标识,譬如手机号、身份证号等作为标识用户的信息,通过KGC生成患者私钥d_k,其过程为:$t_{k1}=H(ID_k\|hid,N)+k$,$t_{k2}=k\times t_{k1}^{-1}$,$d_k=t_{k2}\times P_2$。

同理,密钥生成中心KGC为第三方用户生成随机数$u\in[1,N-1]$,加密主公钥$Pub_u=u\times P_2$,第三方用户私钥生成过程为:$t_{u1}=H(ID_u\|hid,N)+u$,$t_{u2}=u\times t_{u1}^{-1}$,$d_u=t_{u2}\times P_2$。

(2)病历加密和存储

(a)病历加密

患者在注册过信息后,会选择自己唯一的标识ID_k,KGC会根据ID_k生成加密公钥Pub_k,患者在进行诊断后,生成电子病历M,系统会对M进行脱敏处理,然后医生根据患者公钥Pub_k对M进行加密。

加密过程:

(1)计算G_1中元素$Q=\left[H(ID_k\|hid,N)\right]P_1+Pub_k$。

(2)产生随机数$r\in[1,N-1]$,并计算G_1元素$C_1=[r]Q$。

(3)计算G_T中元素$g=e(Pub_k,P_2)$、$w=g^r$。

(4)计算$klen=m_len+K_2_len$,然后计算$K=KDF(C_1\|w\|ID_k,klen)$(K_1令为K最左边的m_len比特,K_2为剩下的K_2_len比特),患者保存K_1值。

(5)计算$C_2=M\oplus K_1$。

(6)计算$C_3=MAC(K_2,C_2)$。

(7)输出密文$C=C_1\|C_3\|C_2$。

(b)患者安全标识生成

患者在注册身份信息后,系统会根据患者ID_k计算患者唯一安全标识,本方案采取*hash*256的方式,即$SID=hash256(ID_k)$。

(c)数据存储

在加密过电子病历后,系统会将加密后的电子病历存储至医院IPFS节点,存储成功后,IPFS会生成一段唯一的hash值h_M,用于当作加密病历索引值和患者安全标识SID一并上传至联盟链。联盟链数据结构如表1所示。

表1 联盟链数据结构

Table 1 Structure of consortium chain data

时间戳	块标识	块大小	前块哈希	患者标识	病历索引	块创建者身份	块创建者签名
t	联盟链块*ID*	*size*	*hash*	*SID*	h_M	医院*ID*	医院签名

(3)数据访问

(a)情形1:当患者访问病历时,需要输入标识ID_k,联盟链上的智能合约会自动将ID_k转换为SID',并运行搜索算法,在联盟链进行对比

搜索,若搜索到$SID'=SID$,则对比成功,然后智能合约根据区块上SID对应的病历索引h_M,在IPFS节点上查找到加密电子病历C返回给患者,患者输入私钥d_k解密得到电子病历M'。若医生需要病历时,患者可将M'发送给医生。智能合约算法如算法1所示。

解密过程:

(1)从密文C中取出C_1,验证$C_1\in G_1$是否成立,若不成立则报错退出。

(2)计算G_T中元素$w'=e(C_1,d_k)$。

(3)计算整数$klen=m_len+K_2_len$,然后计算$K'=KDF(C_1\|w'\|ID_k,klen)$(令$K_1'$为$K'$最左边的$m_len$比特,$K_2'$为剩下的$K_2_len$比特)。

(4)计算$M'=C_2\oplus K_1'$。

(5)计算$u=MAC(K_2',C_2)$,并从C中取出C_3,若$u\neq C_3$,则报错并退出。

(6)输出明文M'。

算法1 智能合约获取*ipfs*索引值和密文C

输入:患者*id*
输出:密文C
1: $h=0$; //初始化一个参数h;
2: $sid1=hash256(id)$; //对患者标识进行*hash*运算;
3: for ($i=0;i<peers.length;i++$) do //对节点*peers*进行循环;
4: if ($sid1==peers[i].SID$) then
5: $h=peers[i].h_M$; //获取此节点的*ipfs*索引值;
6: end if
7: end for
8: if ($h==0$) then
9: return error; //若$h==0$,返回错误;
10: end if
11: $C=GetIpfs(h)$; //根据索引值获取密文;
12: return C。

(b)情形2:当第三方用户U需要访问患者数据时,需携带自己的标识$UID(hash256(ID_u))$、公钥Pub_u和所需要访问的患者SID,向智能合约发送访问请求,智能合约根据SID将请求发送给患者,若得到患者授权,由于患者在加密过程中保存了K_1,患者则可在本地客户端输入K_1值并在本地运行SM9加密算法,使用用户U的标识UID和公钥Pub_u对K_1值进行加密,同时智能合约根据SID获取密文C,并将加密过的K_1和C一并发送给用户,用户U根据私钥d_u获得明文M'。智能合约算法如算法2所示。

加解密过程:

(1)加密过程同上述病历加密过程,对K_1进行加密。

(2)解密过程同情形一解密过程,用户U利用自己私钥d_u得到K_1值。

(3)从密文C中获取C_2,并计算$M'=C_2\oplus K_1$。

(4)获得明文M'。

算法2 智能合约发送请求和发送响应

输入:用户U的标识*uid*、公钥*pubu*、访问的患者标识*sid*、患者保存的K_1值。
1: $h=0$; //初始化一个参数h
2: $K_2=0$; //初始化一个参数K_2
3: $permission=false$; //初始化权限为*false*
4: $permission=sendrequest(uid,pubu,sid)$; //发送请求给患者并返回认证权限值
5: if ($permission=false$) then //若没获得权限
6: return error; //返回错误,并退出
7: end if
8: $K_2=sm9(pubu,uid,K_1)$; //本地运行*sm9*算法,返回K_2;
9: for ($i=0;i<peers.length;i++$) do //对节点*peers*进行循环
10: if ($sid==peers[i].SID$) then
11: $h=peers[i].h_M$; //获取此节点的*ipfs*索引值
12: end if
13: end for
14: if ($h==0$) then
15: return *error*; //若$h==0$,返回错误;
16: end if
17: $C=GetIpfs(h)$; //根据索引值获取密文;
18: $sendresponse(K_2,c,uid)$; //向用户U发送响应并将K_2和C一并发送给用户U。

3 方案安全性和性能分析

3.1 方案正确性证明

(1)数据访问时情形一:在用户用私钥解密电子病历时,需要验证$M'=M$,而验证$M'=M$,关键需要验证加密时w和解密时的w'是否相等。

加密时:

$w=g^r=e(Pub_k,P_2)^r=e(kP_1,P_2)^r=e(P_1,P_2)^{rk}$。

解密时:

$$w'=e(C_1,d_k)=$$
$$e(r\{[H(ID\|hid,N)]P_1+Pub_k\},$$
$$k[H(ID\|hid,N)+k]^{-1}P_2)=$$

$$e(r\{[H(ID\|hid,N)]P_1+kP_1\},$$
$$k[H(ID\|hid,N)+k]^{-1}P_2)=$$
$$e(r[H(ID\|hid,N)+k]P_1,$$
$$k[H(ID\|hid,N)+k]^{-1}P_2)=$$
$$e(P_1,P_2)^{rk[H(ID\|hid,N)+k][H(ID\|hid,N)+k]^{-1}}=$$
$$e(P_1,P_2)^{rk}=w。$$

由上述证明可知,加密时w与解密时w'相等,因此$K'=KDF(C_1\|w'\|ID,klen)=KDF(C_1\|w\|ID,klen)=K$,又因为$K_1'$为$K'$最左边的$m_len$比特,所以,$K_1'=K_1$,则$M'=C_2\oplus K_1'=M\oplus K_1\oplus K_1'=M$。

(2)对于数据访问时情形二:同(1)证明,证明加密时w与解密时w'相等,最后得到K_1,并计算$M=C_2\oplus K_1$。

3.2 方案安全性分析

(1)密钥安全

在本方案中,无论患者密钥还是第三方用户密钥对都是由随机数生成,并且私钥都是KGC使用用户得唯一标识和主私钥的计算生成,并由用户保存于本地,在病历加密过程中,全部使用公钥加密,保证了密钥的安全。

(2)数据安全

在存储过程中,上传至IPFS的电子病历都进行了加密,并且由IPFS生成的索引哈希值上传至联盟链中,由于区块链的不可篡改的性质,保证了索引哈希值的安全,同时保证了IPFS上电子病历的完整性和一致性。在SM9算法解密过程中需要对密文中消息认证码C_3进行验证,验证成功才可进行解密,保证了密文在加解密和共享时的一致性。同时在加密和共享过程中,都只能用用户的私钥才能完成解密操作,保证了数据的安全。

(3)隐私保护

在智能合约搜索过程和共享过程中,无论患者还是第三方用户标识都用了哈希运算,保证了用户标识的安全,并且电子病历在加密前,都对患者的信息进行了脱敏技术处理,保护了患者的隐私安全。

(4)访问控制

在第三方用户需要访问患者病历时,必须通过患者本人的授权,才能获取患者本人的加密病历,保证了电子病历的安全共享,不会形成数据滥用。

3.3 方案对比分析

在方案对比分析中,主要将本方案与其他方案在功能及性能方面进行了对比分析(见表2)。性能分析主要包括存储分析、算法分析及通信开销分析。

表2 不同方案在功能性上的对比结果

Table 2 Comparison results of different schemes in terms of functionality

功能特性	文献[21]	文献[22]	文献[23]	文献[24]	文献[25]	本文方案
区块链	×	√	√	√	√	√
单链	/	×	×	√	×	√
脱敏技术	×	×	×	×	×	√
第三方数据共享	√	×	√	√	√	√
加密方案	属性加密+代理重加密	可搜索加密	可搜索加密+代理重加密	可搜索加密+属性加密	可搜索加密+代理重加密	智能合约+SM9算法
存储系统	云服务器	×	区块链	云服务器	服务器	IPFS

(1)功能性分析

由表2可知,本方案与文献[21-25]的方案进行了对比分析,表中所有方案都应用于电子病历,其中,文献[21]没有应用区块链,增加了数据被篡改的风险,文献[22-23,25]都使用的双链结构,增加了系统的复杂性,文献[22]不具备数据共享功能,文献[21,23-25]都使用代理重加密的方式进行共享,本方案采取SM9加密密钥方式进行共享,减少了中心化的风险和证书认证的过程,并且本方案采用IPFS方式进行存储,增加了文件的安全性和存储效率,并使用脱敏技术进一步增强了患者的隐私保护。综上所述,本方案在功能方面有一定优势。

(2)存储分析

存储病历文件方面,文献[21,24]采用了云服务器存储,文献[25]采用了普通服务器存储,若服务器遭到攻击,必然会威胁到病历文

件的安全,文献[23]直接采用区块链存储文件,增加了区块链存储压力,而且一旦某个节点遭到攻击,文件会遭到破坏。在本方案中存储文件采用IPFS存储文件,区块链存储索引值,形成“链下存储,链上索引”。IPFS对文件进行分布式存储,并具有数据冗余特性,即一个节点遭到破坏,也可以在其他节点获得同样的数据,保证了数据的安全。

IPFS具有高效的文件传输特性,本方案中使用Windows10系统,通过创建三个虚拟机进行了仿真测试,主要测试IPFS和一般的服务器的传输模式文件传输模式(File Transfer Protocol,FTP)的上传时间(图2)和下载时间(图3),使用Go语言测出了数据,使用PyCharm画出了仿真图。

由图2和图3可知,IPFS比一般服务器或者云服务器所使用的文件传输模式FTP模式在上传文件和下载文件过程中有着明显的优势,降低了系统的存储开销。

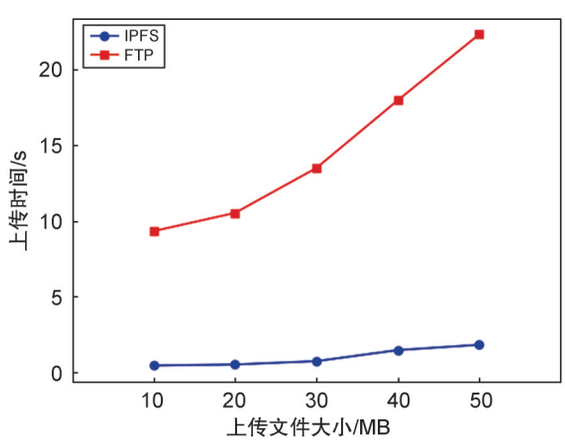

图2 IPFS与FTP下不同大小病历文件的上传时间对比结果

Fig. 2 Comparison results of upload time for medical records of different sizes under IPFS and FTP

(3)算法分析

文献[21,23-25]中都使用了代理重加密算法,增加了数据中心化的风险,本方案采取SM9算法对患者的隐私及病历数据进行了保护,SM9算法与其他常用非对称加密算法比较,包括椭圆曲线密码算法(Elliptic Curve Cryptography, ECC)和RSA加密算法(Rivest-Shamir-Adleman),如表3所示。由表3可知,SM9算法具有密钥短、较高加解密速度、身份识别机制、不需要交换证书、高安全性等特点,极大的增加了系统的效率并降低中心化的风险,保证了数据及患者隐私的安全。在SM9算法解密过程中,具有密文验证的性质,提升了系统的效率和数据安全性。

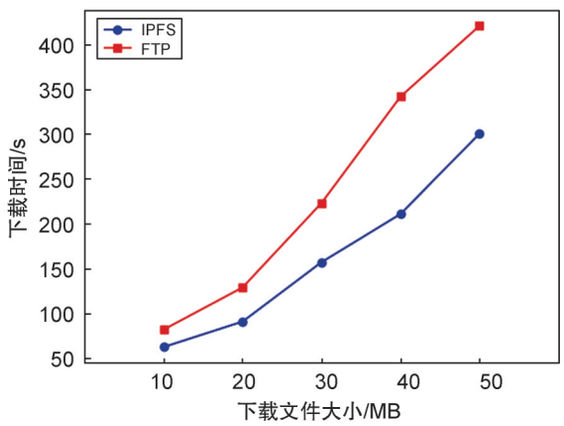

图3 IPFS与FTP下不同大小病历文件的下载时间对比结果

Fig. 3 Comparison results of download time for medical records of different sizes under IPFS and FTP

表3 SM9与ECC、RSA算法在加密解密时间、密钥长度以及是否支持身份验证和密文验证方面的比较结果

Table 3 Comparison results of SM9, ECC, and RSA algorithms in terms of encryption/decryption time, key length, and support for identity and ciphertext verification

算法	加密时间/ms	解密时间/ms	密钥长度/bit	身份认证	密文验证
ECC	0.352	0.860	⩾256	×	×
RSA	0.647	3.424	2 048	×	×
SM9	0.508	1.062	256	√	√

(4)通信开销

基于文献[25]运算成本分析,若添加系统建立时间T_s、证书交换时间T_c、一次上传时间T_u和下载时间T_d可得到一次通信时间。在与文献[25]同等仿真条件下,通过模拟测得证书交换时间为34.83 ms,又通过与文献[25]密码计算成本对比可得$T_c \gg T_p > T_e > T_m > T_h$,其中$T_p$表示双线性对运算时间,$T_e$表示加密运算时间,$T_m$表示乘法运算时间,$T_h$表示hash运算时间。最终在假设系统建立时间一致的情况下,得到一次通信总时间如表4所示,本方案由于在存储方面的优势及不需要证书交换时间,在通信方面有着一定优势。

表4 在相同条件下,系统一次通信时间的对比结果

Table 4 Comparison results of one-time communication time for systems under the same conditions

方案	一次通信总时间
文献[15]	$T_s+T_c+3T_p+8T_e+8T_h+T_u+T_d$
本文方案	$T_s+4T_p+2T_e+9T_h+6T_m+T_u+T_d$

4 总结与展望

本文提出了一种基于联盟链和SM9的安全可共享的电子病历方案。本方案利用区块链技术解决了传统电子病历中存在的数据不一致和数据安全等问题。同时,通过应用脱敏算法和SM9算法解决了患者隐私安全和数据共享难题,并通过使用IPFS提升了系统的存储效率。最后对方案的安全性、功能性和效率等多个方面进行了分析。结果显示,该方案不仅提高了安全性、降低了系统复杂度,而且在时间效率方面也具有显著优势。未来的工作将探索将去中心化标识符(Decentralized Identifier,DID)技术与该方案结合,进一步提升电子病历在共享过程中的安全性和效率。

参考文献:

[1] SHAHNAZ A, QAMAR U, KHALID A. Using Blockchain for Electronic Health Records[J]. *IEEE Access*, 2019, **7**: 147782−147795. DOI: 10. 1109/ACCESS. 2019. 2946373.

[2] 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报, 2019, **45**(1): 206−225. DOI: 10.16383/j.aas.c180710.
HAN X, YUAN Y, WANG F Y. Security Problems on Blockchain: The State of the Art and Future Trends[J]. *Acta Autom Sin*, 2019, **45**(1): 206−225. DOI: 10.16383/j.aas.c180710.

[3] 薛腾飞, 傅群超, 王枞, 等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报, 2017, **43**(9): 1555−1562. DOI: 10.16383/j.aas.2017.c160661.
XUE T F, FU Q C, WANG C, *et al*. A Medical Data Sharing Model via Blockchain[J]. *Acta Autom Sin*, 2017, **43**(9): 1555−1562. DOI: 10.16383/j.aas.2017.c160661.

[4] 毕娅, 周贝, 冷凯君, 等. 基于双链架构的医药商业资源公有区块链[J]. 计算机科学, 2018, **45**(2): 40−47. DOI: 10.11896/j.issn.1002-137X.2018.02.007.
BI Y, ZHOU B, LENG K J, *et al*. Public Blockchain of Pharmaceutical Business Resources Based on Double-chain Architecture[J]. *Comput Sci*, 2018, **45**(2): 40−47. DOI: 10.11896/j.issn.1002-137X.2018.02.007.

[5] YANG X D, LI T, LIU R, *et al*. Blockchain-based Secure and Searchable EHR Sharing Scheme[C]//2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE). New York: IEEE, 2019: 822−8223. DOI: 10. 1109/ICMCCE48743. 2019. 00188.

[6] 周正强, 陈玉玲, 李涛, 等. 基于联盟链的医疗数据安全共享方案[J]. 应用科学学报, 2021, **39**(1): 123−134. DOI: 10.3969/j.issn.0255-8297.2021.01.011.
ZHOU Z Q, CHEN Y L, LI T, *et al*. Medical Data Security Sharing Scheme Based on Consortium Blockchain[J]. *J Appl Sci*, 2021, **39**(1): 123−134. DOI: 10.3969/j.issn.0255-8297.2021.01.011.

[7] ZHUANG Y, SHEETS L R, CHEN Y W, *et al*. A Patient-centric Health Information Exchange Framework Using Blockchain Technology[J]. *IEEE J Biomed Health Inform*, 2020, **24**(8): 2169−2176. DOI: 10. 1109/JBHI. 2020. 2993072.

[8] 殷明. 基于标识的密码算法SM9研究综述[J]. 信息技术与信息化, 2020(5): 88−93. DOI: 10.3969/j.issn.1672-9528.2020.05.026.
YIN M. Overview of Research on Identity-based Cryptography Algorithm SM9[J]. *Inf Technol Informatization*, 2020(5): 88−93. DOI: 10.3969/j.issn.1672-9528.2020.05.026.

[9] CHENG X, CHEN F L, XIE D, *et al*. Design of a Secure Medical Data Sharing Scheme Based on Blockchain [J]. *J Med Syst*, 2020, **44**(2): 52. DOI: 10. 1007/s10916-019-1468-1.

[10] XI P, ZHANG X L, WANG L, *et al*. A Review of Blockchain-based Secure Sharing of Healthcare Data [J]. *Appl Sci*, 2022, **12**(15): 7912. DOI: 10. 3390/app12157912.

[11] ZHANG J, XUE N, HUANG X. A Secure System for Pervasive Social Network-based Healthcare[J]. *IEEE Access*, 1940, **4**: 9239−9250. DOI: 10. 1109/ACCESS. 2016. 2645904.

[12] TANG F, MA S, XIANG Y, *et al*. An Efficient Authentication Scheme for Blockchain-based Electronic Health Records[J]. *IEEE Access*, 2019, **7**: 41678−41689. DOI: 10. 1109/ACCESS. 2019. 2904300.

[13] KHEZR S, MONIRUZZAMAN M, YASSINE A, *et al*. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research[J]. *Appl Sci*, 2019, **9**(9): 1736. DOI: 10. 3390/app9091736.

[14] MAYER A H, DA COSTA C A, RIGHI R D R. Electronic Health Records in a Blockchain: A Systematic Review[J]. *Health Informatics J*, 2020, **26**(2): 1273−1288. DOI: 10. 1177/1460458219866350.

[15] 朱西平, 赖宇, 龙文涛, 等. 基于区块链的电子病历共

享与可验证方案[J]. 科学技术与工程, 2023, **23**(14): 6113−6122.
ZHU X P, LAI Y, LONG W T, *et al*. Electronic Medical Record Sharing and Verifiable Scheme Based on Blockchain[J]. *Sci Technol Eng*, 2023, **23**(14): 6113−6122.

[16] CHEN W Z, ZHU S Z, LI J M, *et al*. Authorized Shared Electronic Medical Record System with Proxy re-encryption and Blockchain Technology[J]. *Sensors*, 2021, **21**(22): 7765. DOI: 10. 3390/s21227765.

[17] HASSELGREN A, KRALEVSKA K, GLIGOROSKI D, *et al*. Blockchain in Healthcare and Health Sciences-a Scoping Review[J]. *Int J Med Inform*, 2020, **134**: 104040. DOI: 10. 1016/j. ijmedinf. 2019. 104040.

[18] MCGHIN T, CHOO K K R, LIU C Z, *et al*. Blockchain in Healthcare Applications: Research Challenges and Opportunities[J]. *J Netw Comput Appl*, 2019, **135**(C): 62−75. DOI: 10.1016/j.jnca.2019.02.027.

[19] 彭聪, 何德彪, 罗敏, 等. 基于SM9标识密码算法的环签名方案[J]. 密码学报, 2021, **8**(4): 724−734. DOI: 10.13868/j.cnki.jcr.000473.PENG C,
HE D B, LUO M, *et al*. An Identity-based Ring Signature Scheme for SM9 Algorithm[J]. *J Cryptologic Res*, 2021, **8**(4): 724−734. DOI: 10.13868/j.cnki.jcr.000473.

[20] 张超, 彭长根, 丁红发, 等. 基于国密SM9的可搜索加密方案[J]. 计算机工程, 2022, **48**(7): 159−167. DOI: 10.19678/j.issn.1000-3428.0062771.
ZHANG C, PENG C G, DING H F, *et al*. Searchable Encryption Scheme Based on China State Cryptography Standard SM9[J]. *Comput Eng*, 2022, **48**(7): 159−167. DOI: 10.19678/j.issn.1000-3428.0062771.

[21] LIANG P F, ZHANG L Y, KANG L, *et al*. Privacy-preserving Decentralized ABE for Secure Sharing of Personal Health Records in Cloud Storage[J]. *J Inf Secur Appl*, 2019, **47**(C): 258−266. DOI: 10. 1016/j. jisa. 2019. 05. 012.

[22] ZHANG A Q, LIN X D. Towards Secure and Privacy-preserving Data Sharing in E-health Systems via Consortium Blockchain[J]. *J Med Syst*, 2018, **42**(8): 140. DOI: 10. 1007/s10916-018-0995-5.

[23] 翟社平, 汪一景, 陈思吉. 区块链技术在电子病历共享的应用研究[J]. 西安电子科技大学学报, 2020, **47**(5): 103−112. DOI: 10.19665/j.issn1001-2400.2020.05.014.
ZHAI S P, WANG Y J, CHEN S J. Research on the Application of Blockchain Technology in the Sharing of Electronic Medical Records[J]. *J Xidian Univ*, 2020, **47**(5): 103−112. DOI: 10.19665/j.issn1001-2400.2020.05.014.

[24] 张磊, 郑志勇, 袁勇. 基于区块链的电子医疗病历可控共享模型[J]. 自动化学报, 2021, **47**(9): 2143−2153. DOI: 10.16383/j.aas.c200359.
ZHANG L, ZHENG Z Y, YUAN Y. A Controllable Sharing Model for Electronic Health Records Based on Blockchain[J]. *Acta Autom Sin*, 2021, **47**(9): 2143−2153. DOI: 10.16383/j.aas.c200359.

[25] 牛淑芬, 陈俐霞, 李文婷, 等. 基于区块链的电子病历数据共享方案[J]. 自动化学报, 2022, **48**(8): 2028−2038. DOI: 10.16383/j.aas.c190801.
NIU S F, CHEN L X, LI W T, *et al*. Electronic Medical Record Data Sharing Scheme Based on Blockchain[J]. *Acta Autom Sin*, 2022, **48**(8): 2028−2038. DOI: 10.16383/j.aas.c190801.