计算机科学
COMPUTER SCIENCE

基于 Fabric 的电子病历跨链可信共享系统设计与实现

袁昊男，王瑞锦，郑博文，吴邦彦

引用本文

袁昊男，王瑞锦，郑博文，吴邦彦. 基于 Fabric 的电子病历跨链可信共享系统设计与实现[J]. 计算机科学, 2022, 49(6A): 490-495.

YUAN Hao-nan, WANG Rui-jin, ZHENG Bo-wen, WU Bang-yan. Design and Implementation of Cross-chain Trusted EMR Sharing System Based on Fabric[J]. Computer Science, 2022, 49(6A): 490-495.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210500063

基于 Fabric 的电子病历跨链可信共享系统设计与实现

袁昊男[1]　王瑞锦[1,2]　郑博文[1]　吴邦彦[1]
1 电子科技大学信息与软件工程学院　成都 610054
2 网络与数据安全四川省重点实验室　成都 610054
(yuanhn627@qq.com)

摘　要　电子病历是患者敏感且重要的隐私数据资产,它的可信共享对医疗信息化发展具有重大意义。针对患者病历数据存储不安全、跨域可信共享难、访问周期长等问题,文中整合区块链与边缘计算,设计并实现了基于 Fabric 联盟链的电子病历跨链可信共享系统。系统主要分为患者移动应用、医院 Web 应用及 RFID 电子标签手环,主要包括病历加密与认证、跨链可信共享、远程授权等功能。此外,文中设计了基于生物特征密钥与国密算法的加密与认证机制,以患者为主体控制隐私数据流向,实现个性化隐私保护;在 Hyperledger Fabric 联盟链框架上应用一种主链基于改进的 PBFT 共识算法、从链基于 PoVT 共识算法的主从多链分层跨链模型,实现可靠访问与控制。通过实验与对比分析,证明了本系统在数据安全性与性能上有较大优势。

关键词:电子病历;联盟链;可信共享;边缘计算;生物特征密钥
中图法分类号　TP311

Design and Implementation of Cross-chain Trusted EMR Sharing System Based on Fabric

YUAN Hao-nan[1],WANG Rui-jin[1,2],ZHENG Bo-wen[1] and WU Bang-yan[1]
1 School of Information and Software Engineering,University of Electronic Science and Technology of China,Chengdu 610054,China
2 Network and Data Security Key Laboratory of Sichuan Province,Chengdu 610054,China

Abstract　Electronic medical record(EMR) is a sensitive and important privacy data asset of patients. Its trusted sharing is significant to the development of medical informalization. Aiming at the problems of unsafe data storage,difficult cross-domain trusted sharing and long access period of EMRs,this paper integrates blockchain and edge computing,designs and implements a cross-chain trusted EMR sharing system based on Fabric alliance chain frame. The system is mainly divided into patient mobile application,hospital Web application and RFID tag bracelet,including medical record encryption and authentication,cross-chain trusted sharing,remote authorization and other functions. In addition,this paper designs encryption and authentication mechanism based on biometric key and national commercial cipher algorithm series,to control the flow of privacy data with patients as the main bodyand realize personalized privacy protection. It applies a master-slave multi-chain hierarchical cross-chain model on the Hyperledger Fabric to achieve reliable access and control. Experiments and comparative analysis show that the system has great advantages in data security and performance.

Keywords　Electronic medical record,Alliance chain,Trusted sharing,Edge computing,Biometric key

1　引言

目前,随着医疗信息系统的普及,国内外大部分医院用它实现医院全过程信息化管理,包括对患者电子病历的存储与处理。传统医疗信息系统通常采用 B/S 或 C/S 架构中心化存储数据,信息安全风险大、可共享性差[1]。主要原因有:第一,中心化架构和关系型数据存储不能保证病历数据绝对安全,不同医疗信息系统执行的信息安全等级保护标准不同,存储服务提供商并不充分可信、可靠,系统权限管理机制不严密,角色权限划分不明确,由第三方内部攻击导致的数据泄露层出不穷[2],据 2020 年医疗行业网络安全白皮书[3]数据显示,国内 14 个中心服务器、超 28 万条患者医疗数据暴露于互联网;第二,电子病历存储格式与依赖环境不一致,各医院医疗信息系统互操作性较低,患者数据存储相对分散、由不同主体控制,数据共享难以协调管理,且在跨域共享过程中数据的保密性、完整性、可用性不能保证,可信性存疑;第三,数据

基金项目:国家自然科学基金(61802033,61472064,61602096);四川省区域创新合作项目(2020YFQ0018);四川省科技计划重点研发项目(2021YFG0027,2020YFG0475,2018GZ0087,2019YJ0543);中国博士后科学基金项目(2018M643453);广东省国家重点实验室项目(2017B030314131);网络与数据安全四川省重点实验室开放课题(NDSMS201606)
This work was supported by the National Natural Science Foundation of China(61802033,61472064,61602096),Sichuan Regional Innovation Cooperation Project(2020YFQ0018),Sichuan Science and Technology Program(2021YFG0027,2020YFG0475,2018GZ0087,2019YJ0543),Chinese Postdoctoral Science Foundation(2018M643453),Guangdong Provincial Key Laboratory Project(2017B030314131) and Network and Data Security Key Laboratory of Sichuan Province Open Issue(NDSMS201606).
通信作者:王瑞锦(ruijinwang@uestc.edu.cn)

访问周期长，对病历数据的访问需要通过医疗信息系统进行身份认证、访问权限控制、密钥生成与证书签发等一系列环节，访问量较大时很可能造成网络拥塞，延长数据访问周期，此外，当患者在院外发生危急情况时，很难在短时间内获取历史病历数据，耽误精准急救。

区块链技术为电子病历受控、可信、共享提供了安全的分布式框架，其去中心化、不可篡改的特性更符合数据分布式安全存储的趋势[4]，是数据交换的完美解决方案。目前，国内外区块链与智慧医疗相结合的应用研究已经有了较大的发展。如 HealthNautica 公司产品 e-Orders[5] 利用区块链技术提高患者数据的安全，便于医患双方识别和追溯，且无法篡改[6]；BitHealth[7] 运用区块链技术存储医疗数据，并能实现从世界各地任一节点将其恢复；Gem 与飞利浦公司共同开发企业级区块链医疗应用 Gem Health Network[8]，该应用基于区块链技术保护患者隐私，有利于电子病历信息的共享[9]。但以上研究仍存在不足：第一，难适应国内医疗数据的高速率生产与高频率并发共享，不适用于大数据时代环境下复杂富文本信息环境，实现成本较高；第二，未体现以患者为主体的数据流向权限控制，不能实现患者可控个性化隐私保护；第三，未充分利用患者设备算力及整合边缘计算技术，凸显出了单一区块链架构的短板。

随着边缘设备数据处理与算力逐渐增强，边缘计算作为云的扩展被引入互联网应用系统[10]。和云相似，分布式边缘计算及设备通过提供算力、应用服务及存储来实现支持低延迟、异构的服务。将边缘计算及其设备与区块链整合，能够有效提高系统的网络安全性、数据完整性和计算有效性。本文基于区块链去中心化、不可篡改与伪造等特性，结合边缘计算分布式、低时延、高带宽、提供算力与存储服务等特点，依托 Fabric 联盟链框架设计并实现了一个电子病历跨链可信共享系统，提供安全、可信的电子病历跨域共享解决方案，以患者为主体控制隐私数据资产主权与信息流向，体现患者个性化隐私保护，提高医疗效率并降低运营成本，助力数字中国建设。

2 系统总体设计

2.1 系统架构设计

电子病历跨链可信共享系统总体架构设计如图 1 所示。医院节点中心服务器为系统基础业务，如为预约挂号、用户管理等提供支持，与患者端、医院端间采用 B/S 架构通信，客户端向服务器标准 RESTful 接口发起请求，进行 JSON 格式数据交互。服务器采用 SSM（SpringMVC＋Spring＋MyBatis）框架集开发，与存储患者基础信息的本地数据库交互。通过患者移动应用与电子标签急救辅助手环搭建系统边缘计算环境，提供算力与存储功能，通过 RFID 或 NFC 读写数据。主从多链分层跨链区块网络与 IPFS 分布式 P2P 存储网络支持系统核心病历业务。

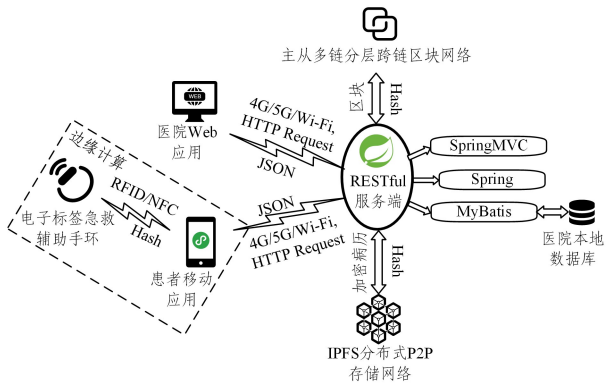


图 1 系统总体架构设计图

Fig. 1 Design diagram of system overall architecture

此外，核心病历业务 5 层架构设计如图 2 所示，分为用户层、应用层、核心业务层、网络层及数据存储层，从不同用户角色及功能需求角度细化系统架构设计。

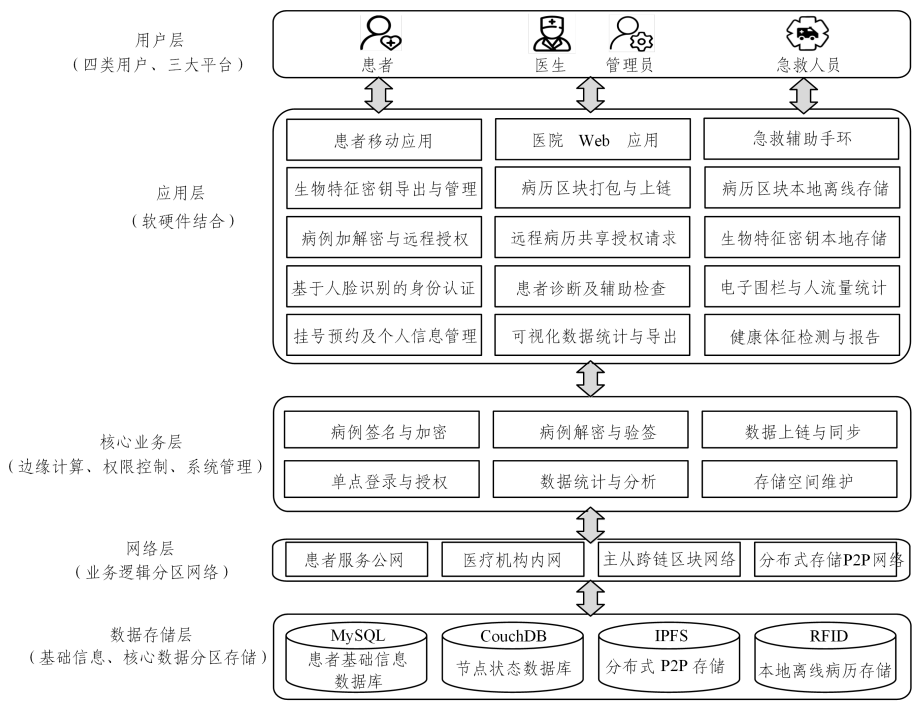


图 2 核心病历业务 5 层架构设计图

Fig. 2 Five-layer architecture design of core medical record business

2.2 系统功能模块设计

经过市场分析与调研以及用户需求分析，设计了如下软件功能结构，共三大应用平台，20 个功能模块，如图 3 所示。

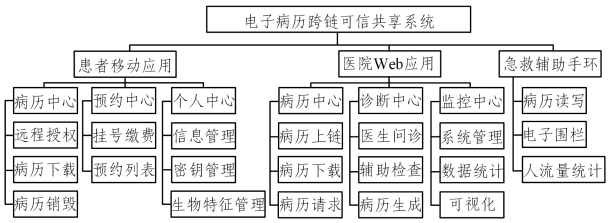


图 3 系统功能模块图

Fig. 3 System function module diagram

(1)患者移动应用端功能模块

1)病历中心：远程授权模块处理医生远程病历查看授权请求；病历下载模块检索历史病历文件并下载、解密、验证签名后供患者查看；病历销毁模块永久删除患者历史病历记录及文件。

2)预约中心：挂号缴费模块供患者查看医生排班表并预约挂号、缴费；预约列表显示患者预约记录。

3)个人中心：信息管理模块提供个人基础信息的增、删、改、查；密钥管理模块管理患者生物特征密钥有效期、加密记录等；生物特征管理模块采集患者生物特征并进行本地离线密钥导出。

(2)医院 Web 应用端功能模块

1)病历中心：病历上链模块由医院节点对系统签名、加密后的病历文件进行上传与上链操作；病历下载模块由医院节点检索历史病历并下载至本地；病历请求模块供医生远程向患者发起病历共享请求授权。

2)诊断中心：医生问诊模块由医生对待诊断患者进行问诊与病历填写；辅助检查模块由医生开具辅助检查申请单；病历生成模块汇总所有诊断记录为病历文档，并进行签名与加密。

3)监控中心：系统管理模块供管理员进行系统管理；数据统计模块支持以多格式文件方式导出系统各类数据；可视化模块提供数据监控大屏。

(3)急救辅助手环模块

1)病历读写：支持将患者基础信息、加密病历索引等信息写入手环并加密。

2)电子围栏：支持设置感应点位电子围栏策略进行活动范围限制。

3)人流量统计：支持通过感应点位统计通过点位的人数。

2.3 系统核心业务流程设计

本系统核心业务为电子病历的签名、加密、上传与上链，以及病历的检索、下载、解密与签名验证，其中基于患者生物特征密钥与国密算法的电子病历加解密认证机制设计如图 4 所示。其中，医院节点在 CA 有效注册后，本地生成医院节点公私钥对$\langle PK_{\text{hos}}, SK_{\text{hos}}\rangle$，将身份信息及公钥 PK_{hos} 提交给 CA，签发数字证书后返回医院节点服务器。患者移动应用客户端需要验证加密病历医院节点数字签名时，向医院节点服务器申请数字证书并确认合法性后得到医院节点公钥 PK_{hos}，进行验证。K_{iris} 为患者生物特征密钥，由患者移动应用客户端本地离线导出。

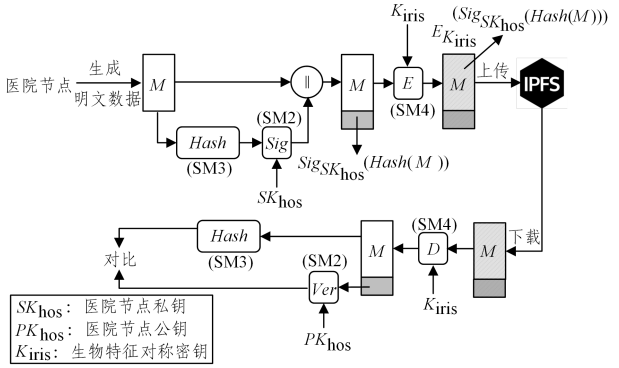


图 4 病历数据加解密与认证机制设计

Fig. 4 Design of medical record data encryption, decryption and authentication mechanism

2.3.1 病历签名、加密、上传与上链

医生完成患者诊断后，医院 Web 应用端生成患者明文电子病历。医院节点首先对明文数据采用国密 SM3 算法计算摘要值，之后使用医院节点私钥 SK_{hos} 并采用国密 SM2 算法对摘要值进行签名，得到签名后的摘要值 $Sig_{SK_{\text{hos}}}(Hash(M))$；将明文数据和签名后的摘要值拼接在一起后，使用生物特征对称密钥 K_{iris} 并采用国密 SM4 算法对数据进行对称分组加密，得到完成签名认证及加密后的病历数据 $E_{K\,\text{iris}}(Sig_{SK_{\text{hos}}}(Hash(M)))$。明文病历数据加密及签名算法描述如算法 1 所示。

算法 1 基于国密的明文病历数据签名及加密算法

输入：明文病历数据 emrData、医院节点私钥 SK_{hos}、生物特征对称密钥 K_{iris}

输出：签名及加密后的密文病历数据 emrDataEncrypted

1. 计算明文病历摘要：采用 SM3 摘要算法，计算 emrData 的 Hash 值 emrDataHash；
2. 数字签名：采用 SM2 签名算法，计算对 emrDataHash 的签名值 emrDataHashSig；
3. 拼接：emrDataPlainText=emrData ‖ emrDataHashSig；
4. 对称加密：采用 SM4 加密算法，将明文数据加密为 emrDataEncrypted；
5. 输出 emrDataEncrypted，结束。

明文病历数据签名及加密结束后，将加密病历文件 emrDataEncrypted 上传至 IPFS 分布式 P2P 存储网络，得到唯一与文件内容相关的索引 Hash 值；医院节点将此 Hash 值与便于查询的用户基础信息打包为区块，调用智能合约并启动共识算法上传至主从多链分层跨链网络中。

2.3.2 病历查找、下载、解密与签名验证

当患者本人有查看历史病历需求时，或医生取得患者远程授权后，由医院节点服务器调用智能合约根据关键字在链上查询历史病历记录。查询成功后，根据索引 Hash 值在 IPFS 分布式 P2P 存储网络中下载得到加密病历文件 emrDataEncrypted。用对称密钥 K_{iris} 对病历数据解密，之后验证摘要签名，使用医院节点公钥 PK_{hos}，得到待对比摘要值 H'；将明文病历数据采用国密 SM3 算法计算得到摘要值 H，进入对比验证阶段。若 H 与 H' 完全一致，则通过对比验证，病历数据真实有效，否则失败。密文病历数据解密及验签算法描述如算法 2 所示。

算法 2 基于国密的密文病历数据解密及验签算法

输入：密文病历数据 emrDataEncrypted、医院节点公钥 PK_{hos}、生物特征对称密钥 K_{iris}

输出：明文病历数据 emrData

1. 对称解密：采用 SM4 解密算法，将密文数据解密为 emrDataPlainText；
2. 拆解：取 emrDataPlainText 的后 32 字节为 emrDataHashSig，剩余部分为 emrData；
3. 计算明文病历数据摘要：采用 SM3 摘要算法，计算得出 Hash 值 emrDataHash；
4. 验证签名：采用 SM2 验签算法，输入 emrData，emrDataHashSig，PK_{hos}进行验证；
5. 若第 4 步中验证失败，则输出 null，结束；否则输出 emrData，结束。

此外，当患者在院外发生紧急情况时，急救人员扫描患者急救辅助手环，读取其历史病历 Hash 索引，进而直接下载得到加密病历文件。在不征求患者本人同意的条件下，现场扫描患者虹膜特征导出生物密钥 K_{iris}完成后续步骤，实现精准急救。

3 系统关键技术及实现

3.1 基于生物特征的密钥导出算法

虹膜拥有丰富且独一无二的纹理特征，在各种由生物特征导出的密钥中，虹膜密钥更长，能满足一般对称加密算法对密钥长度(≥56 位)的需求，这一点成为虹膜特征导出生物密钥的独到优势。

在虹膜特征提取生物密钥研究方面，Davida 于 1988 年提出了私有模板方案(Private Template Scheme)[11]，该方案提取典型虹膜特征直接作为密钥，但并没有实验结果，仅停留在理论层面。近期具有代表性的工作是 Hao 的基于纠错码[12]及 Rathgeb 基于语境的虹膜特征密钥生成技术[13]，但以上工作存在以下问题：一是提取的虹膜特征模版存储于云端，存在数据泄露的问题；二是生成的密钥均来自外部，不是来自虹膜特征本身。本系统采用方案为：在虹膜预处理基础上，利用 Haar 小波三层分解提取虹膜特征，采用随机映射函数从虹膜特征中直接提取出 128 位对称加密密钥，用于国密 SM4 对称加密算法，实现患者个性化隐私保护。算法描述如算法 3 所示。

算法 3 基于虹膜特征的密钥导出算法

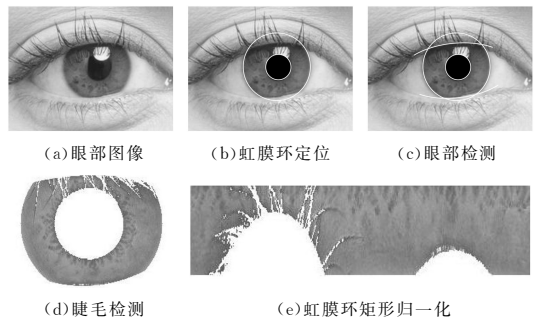
输入：虹膜图像 img

输出：用于国密 SM4 对称加密算法的 128 位密钥

1. 虹膜图像预处理：将 img 进行预处理后得到归一化图像 img_tmp，大小为 100×400；
2. 图像分割：取 img_tmp 图像右上方 40×200 区域 R_4；
3. 二维 Haar 小波三层分解：取结果的 HL_3，LH_3，HH_3 区域，共 375 个小波系数；
4. 特征编码："0～1"阈值化小波系数构成的特征向量 **C** 为二进制码；
5. 密钥导出：通过随机映射函数从 **C** 中提取 128 位对称密码密钥 P；
6. 输出 P，结束。

3.1.1 虹膜图像预处理

虹膜预处理包含虹膜采集、虹膜环定位、眼睑检测、睫毛检测、虹膜环矩形归一化 5 个步骤，其目的是提取有效虹膜区域供特征提取之用。预处理过程如图 5 所示。



(a)眼部图像 (b)虹膜环定位 (c)眼部检测

(d)睫毛检测 (e)虹膜环矩形归一化

图 5 虹膜图像预处理

Fig. 5 Iris image preprocessing

3.1.2 虹膜特征系数提取及编码

虹膜纹理特征主要集中在第三层，对虹膜特征区域进行二维 Haar 小波三层分解，如图 6 所示。

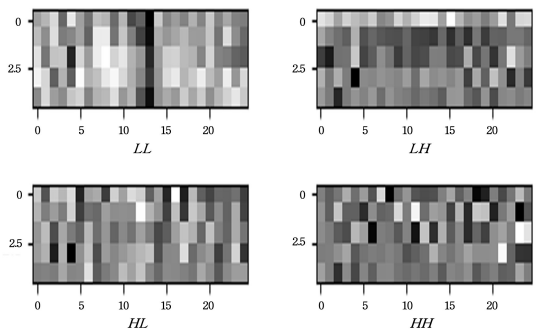


图 6 虹膜图像 Haar 三层小波分解结果

Fig. 6 Results of Haar three-level wavelet decomposition of iris image

虹膜纹理特征的频繁变化导致灰度图像变化的细节信息主要集中在高频系数。若采用低层高频系数为虹膜特征系数，将会导致特征向量空间过大，降低编码效率与密钥导出速度。因此提取第三层高频系数作为虹膜特征向量 ***C***，共有 25×5×3＝375 个小波系数，结果如表 1 所列。

表 1 虹膜特征系数提取结果

Table 1 Results of iris feature coefficient extraction

子图	1	2	3	4	…	22	23	24	25
LH_3	44.625	38.500	18.750	37.000	…	43.000	1.125	39.250	40.625
	20.375	5.875	−1.875	−8.750	…	−8.000	1.375	1.125	−6.000
	…	…	…	…	…	…	…	…	…
	15.125	2.500	−31.875	2.500	…	7.375	9.250	2.500	6.375
HL_3	46.125	−44.250	49.500	33.000	…	−28.750	−30.625	−21.250	−60.875
	30.875	−11.125	11.875	−12.250	…	0.000	−31.875	24.125	−56.750
	…	…	…	…	…	…	…	…	…
	−10.875	−8.250	−12.375	20.750	…	−40.375	−2.500	13.000	12.375
HH_3	2.125	−9.500	−1.250	16.500	…	−16.000	−1.375	21.250	−0.625
	8.625	−8.875	25.125	−8.000	…	0.000	11.125	−40.875	−12.000
	…	…	…	…	…	…	…	…	…
	12.625	1.250	−25.125	5.750	…	−9.125	−7.250	14.250	1.375

为了便于随机映射函数进行处理，设 0 为阈值将特征向量 $\boldsymbol{C}$ 阈值化为二进制码。虹膜特征向量元素 $\boldsymbol{C}(i)$ 的编码规则如式(1)所示：

$$\boldsymbol{C}(i)=\begin{cases}0, & \boldsymbol{C}(i)<0, 1\leqslant i\leqslant 375\\ 1, & \boldsymbol{C}(i)\geqslant 0, 1\leqslant i\leqslant 375\end{cases} \tag{1}$$

将阈值化后的特征向量 $\boldsymbol{C}'$ 通过随机映射函数编码后，得到 128 位对称密码密钥，如图 7 所示。

P	0	0	1	1	1	1	1	1	0	1	0	1	1	0	0
	0	1	0	0	0	0	0	1	1	0	0	1	0	1	0	1
	0	0	1	0	0	1	1	1	0	1	1	0	1	0	1	1
	1	0	1	0	1	1	1	1	0	0	0	1	0	0	1	0
	0	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1
	1	0	0	0	1	0	0	1	1	1	0	1	1	0	1	0
	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	1
	1	0	1	0	1	1	0	0	0	0	1	0	1	1	1	0

图 7 生物特征密钥提取结果

Fig. 7 Results of biometric key extraction

3.2 主从多链分层跨链模型

跨链共识算法可以提高区块链的吞吐量和可扩展性，增强交易处理能力。本系统构建了一个主链基于改进 PBFT 共识算法[14]、从链基于 PoVT 共识算法的主从多链分层跨链模型。该模型使用基于公证人机制的跨链技术，从链负责打包病历数据区块与校验，主链负责对从链上传区块进行排序、共识与上链。模型结构如图 8 所示。

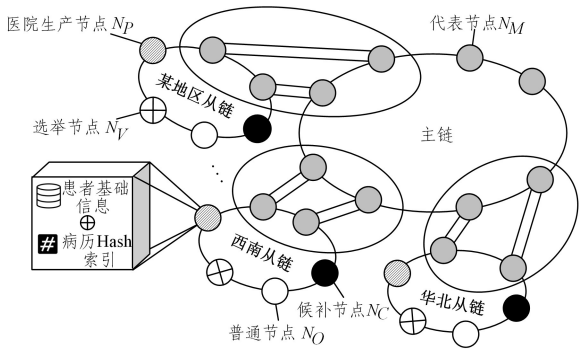


图 8 主从多链分层跨链模型结构

Fig. 8 Structure of master-slave multi-chain hierarchical cross-chain model

3.2.1 从链共识

从链采用一种基于投票机制和信用机制的 PoVT 共识机制。该共识机制通过引入投票机制来选择出块节点，保证了参与共识的节点可靠性，同时降低了节点权益对记账权分配的影响，从而增大对系统发起权益粉碎攻击、双花攻击、私自挖矿攻击等的难度。从链在一个时间片内完成数据区块打包与上链，在一个周期结束后，从链中的代表节点将本周期内所有数据区块上传至主链网络。从链节点分为 5 类角色：普通节点、选举节点、生产节点、候补节点、代表节点。普通节点不参与任何共识，负责同步最新数据区块至本地；选举节点对数据区块进行校验并投票；生产节点将病历数据及患者基础信息打包为区块；候补节点负责在生产节点或选举节点无法提供服务时，递补成为该角色继续行使使命；代表节点负责将其所在主体每一周期内已被确认的数据区块上传至主链网络中。从生产节点、选举节点、候补节点中选取部分节点组成一个共识节点集合 N，集合 N 中节点允许同时拥有主链节点和从链节点的双重身份。集合 N 形成后，通过 PoVT 共识算法决定每一个时隙中产生区块的生产节点编号，同时通过运行梅森旋转算法生成一个伪随机数作为组成主链的代表节点的编号，将数据区块上传至主链网络。

3.2.2 主链共识

主链采用一种改进的 PBFT 共识机制。该共识机制在 PBFT 共识机制的基础上，检查点协议取消了定时检查清除证书步骤，节点同步过程采用向其他节点索要区块并校验的方式完成同步；视图切换协议在结合区块生成协议的基础上，采用超时机制进行视图切换。改进后的 PBFT 共识不需要节点间的 3 段相互通信，减少了通信消耗。

代表节点将自己所在从链中已确认的区块数据上传至主链网络中，随后参与主链改进的 PBFT 共识，在共识完成后，各代表节点将主链区块保存至本地网络中。每一个代表节点保存的主链区块中都包含来自不同从链的区块数据，供其所在的从链的其余节点查询，从而完成不同从链间的数据跨链。

4 系统分析及测试

4.1 系统分析

4.1.1 安全性分析

(1)数据安全性：系统将用户基础低敏感数据与重要敏感数据采用不同方式处理并存储。其中基础低敏感数据存储于医院本地数据库中，如用户密码等字段进行“哈希加盐”处理后存储。重要敏感的病历数据采取一系列基于生物特征与国密算法的加密与认证机制来处理，其中最关键的对称加密密钥由患者本人虹膜的图像导出，国密算法安全性背书，难以破解，病历数据安全可靠。此外，边缘计算设备中 RFID 电子标签采用 NTag213 芯片，开启了密码保护模式，其采用 128 位 ECC 加密，当密码试错 50 次后，电子标签将会永久锁死，安全性较高。

(2)系统运行安全性：系统核心网络架构均采用分布式与 P2P 结构设计，通过所有节点共同维护，可在一定程度上避免单点攻击；主从多链分层跨链网络中主链改进的 PBFT 共识算法支持 $3f+1$ 节点容错，可较好地保证系统稳定性。

4.1.2 效率分析

使用 SimPy 模拟器对系统核心区块链网络与边缘计算业务运行流程进行建模，选择标准 PBFT 共识算法以及 H-PBFT 算法进行对比。

首先比较在系统节点数为 20，50，100 这 3 种情况下的吞吐量与时延。从图 9 和图 10 可以看出，采用标准 PBFT 共识算法的系统性能随着节点数的增多而下降，采用 H-PBFT 共识算法的系统性能有所改善。本系统将边缘计算技术与区块链系统结合，采用主从多链分层跨链模型，实验结果表明本系统指标最优，在吞吐量与时延上都有较大优势。其次，对比 CPU 占用率随时间的变化，结果如图 11 所示。从结果中可以看出，随着时间推移，采用标准 PBFT 共识算法的系统 CPU 占用率持续升高，并长期保持在 98%左右；H-PBFT 算法 CPU 占用率变化趋势与之相似，长期保持在 82%左右；本系统 CPU 占用率有较大改善，可以保持在 20%以下。

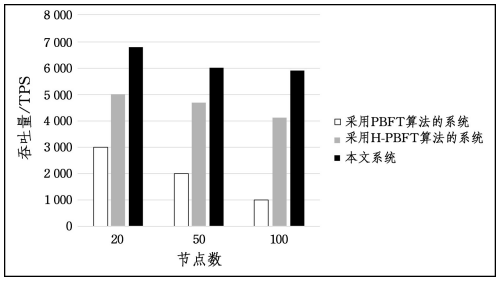


图 9 系统吞吐量对比

Fig. 9 Comparison of system throughput

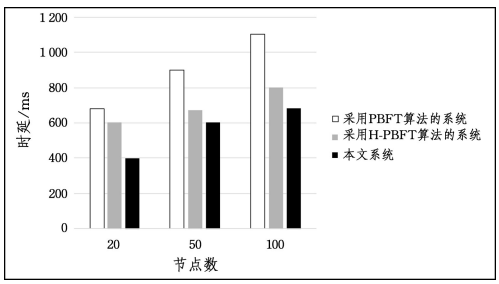


图 10 系统时延对比

Fig. 10 Comparison of system delay

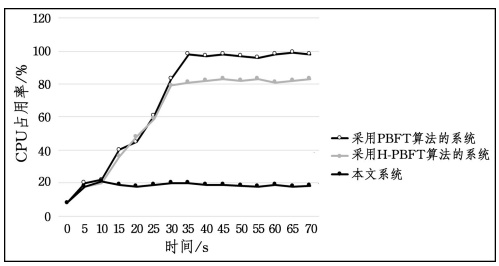


图 11 系统 CPU 占用率对比

Fig. 11 Comparison of CPU utilization

4.1.3 同类系统对比

从共识算法、链结构、系统效率（吞吐量、时延、CPU 占用率）、数据共享性、是否整合边缘计算 5 个方面对主流同类电子病历数据共享系统进行了分析对比，结果如表 2 所列。可以看出，参与比较的电子病历数据共享系统均基于区块链开发，如 MedRec 基于以太坊、MDSM 与本文系统基于联盟链。此外，本文系统将区块链与边缘计算有机整合，借助患者边缘计算设备算力与存储快速导出密钥，在本地进行病历加解密、认证与存储，降低系统时延。同时，本系统采用的主从多链分层跨链模型增强了区块网络容错性，减轻了主链压力，提高了系统效率。

表 2 同类系统对比

Table 2 Comparison of similar systems

系统	共识算法	链结构	系统效率	数据共享性	是否整合边缘计算
MedRec[15]	PoW	单链	较低	较弱	否
MeDShare[16]	—	单链	适中	适中	否
MDSM[17]	DPoS	单链	适中	较强	否
EMRSBC[18]	PBFT	双链	较高	中	否
本文系统	PoVT，PBFT	多链	高	强	是

4.2 系统测试

患者移动应用、医院 Web 应用实现结果分别如图 12、图 13 所示。根据用例规约设计测试方案，系统通过了功能性测试与非功能性测试。

图 12 患者移动应用病历中心页面

Fig. 12 Core page of patient mobile application medical record

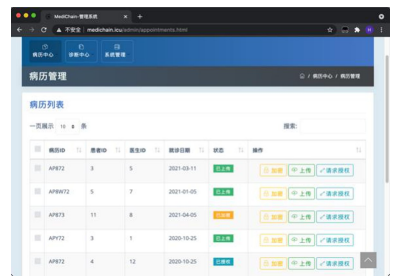


图 13 医院 Web 应用病历管理页面

Fig. 13 Management page of hospital Web application medical record

结束语 本文整合区块链与边缘计算技术，设计并实现了电子病历跨链可信共享系统，以患者生物特征导出密钥，实现个性化隐私保护，有较强的安全性与实用性，提供了强大的去中心化网络和丰富的边缘计算及存储资源。当然，本系统仍有较多不足，在区块链与边缘计算技术结合的探索中，仍面临一系列重大挑战，如将部分计算及存储转移到边缘计算及设备后导致的强伸缩性、安全性及保密性挑战，以及边缘计算节点增多带来的自组织困难等问题，有待进一步深入研究。

参 考 文 献

[1] JIANG J X. Application Research of Medical System Based on Blockchain[D]. Anshan: University of Science and Technology Liaoning, 2020.

[2] DENNIS R, OWENSON G, AZIZ B. A temporal blockchain: A formal analysis[C]// 2016 International Conference on Collaboration Technologies and Systems (CTS). Orlando, FL, USA: IEEE, 2016: 430-437.

[3] CCID. White Paper on Network Security of Medical Industry 2020[EB/OL]. [2020-12-15]. http://www.wfnetworks.cn/news1/shownews.php?id=416.

[4] VUKOLI M. Rethinking permissioned blockchains[C]// Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. Abu Dhabi, United Arab Emirates: ACM, 2017: 3-7.

（下转第 638 页）

[20] CHENG P, CHEN Z. Multidimensional compressive sensing based analog CSI feedback for massive MIMO-OFDM systems [C]// Vehicular Technology Conference. IEEE, 2014: 1-6.
[21] JANG Y, KONG G, JUNG M, et al. Deep Autoencoder based CSI Feedback with Feedback Errors and Feedback Delay in FDD Massive MIMO Systems [J]. IEEE Wireless Communications Letters, 2019, 8(3): 833-836.
[22] KUO P, KUNG H, TING P. Compressive sensing based channel feedback protocols for spatially-correlated massive antenna arrays[C]// Proc. IEEE Int. Conf. Wireless Commun. Netw. (WCNC). 2012: 492-497.
[23] GUERREIRO J, DINIS R, MONTEZUMA P. Analytical Performance Evaluation of Precoding Techniques for Nonlinear Massive MIMO Systems With Channel Estimation Errors [J]. IEEE Transactions on Communications, 2018, 66(4): 1440-1451.
[24] HUYNH V T D, NOELS N, STEENDAM H. BER evaluation of OFDM systems with joint effect of TI-ADC circuits gain mismatch and channel estimation error [J]. IEEE Transactions on Communications, 2019, 67(5): 3612-3623.
[25] WANG C, AU E K, MURCH R D, et al. On the performance of the MIMO zero-forcing receiver in the presence of channel estimation error [J]. IEEE Transactions on Wireless Communications, 2007, 6(3): 805-810.
[26] MARZETTA T L. BLAST training: estimating channel characteristics for high-capacity space-time wireless [C]// Proceedings of the Annual Allerton Conference on Communication Control and Computing. 1999: 958-966.
[27] HASSIBI B, HOCHWALD B M. How much training is needed in multiple-antenna wireless links? [J]. IEEE Trans. Inf. Theory, 2003, 49(4): 951-963.
[28] WEN C, SHIH W, JIN S. Deep Learning for Massive MIMO CSI Feedback [J]. IEEE Wireless Communications Letters, 2018, 7(5): 748-751.

QING Chao-jin, born in 1978, Ph.D, associate professor, is a member of IEEE. His main research interests include wireless network and communication, AI empowers the innovative theory and application research of wireless and mobile communication physical layer.

DU Yan-hong, born in 1996, postgraduate. Her main research interests include AI empowers wireless communication physical layer and CSI feedback.

(上接第 495 页)

[5] SHRIER D, WU W, PENTLAND A. Blockchain & infrastructure (identity, data security) [J]. Massachusetts Institute of Technology-Connection Science, 2016, 1(3): 8-11.
[6] XIANG F, ZHANG B L, FAN B N. Application of blockchain technology in foreign medical and health field[J]. Chinese Journal of Medical Library and Information Science, 2018, 27(8): 31-37.
[7] BAXENDALE G. Can blockchain revolutionise EPRs? [J]. ITNow, 2016, 58(1): 38-39.
[8] DHILLON V, METCALF D, HOOPER M. The Hyperledger Project[EB/OL]. [2018-07-20]. http://www.gemhealth.net/.
[9] QIN B, CHEN L C H, WU Q H, et al. Bitcoin and Digital Fiat Currency[J]. Journal of Cryptologic Research, 2017, 4(2): 176-186.
[10] SATYANARAYANAN M. The emergence of edge computing [J]. Computer, 2017, 50(1): 30-39.
[11] DAVIDA G I, FRANKEL Y, MATT B J. On Enabling Secure Applications Through Off-Line Biometric Identification [C]// Security and Privacy-1998 IEEE Symposium on Security and Privacy. Oakland, CA, USA, IEEE, 1998: 148-157.
[12] HAO F, ANDERSON R, DAUGMAN J. Combining cryptography with biometrics effectively[J]. IEEE Transactions on Computers, 2006, 55(9): 1081-1088.
[13] RATHGEB C, UHL A. Context—based biometric key generation for iris[J]. Computer Vision, 2011, 5(6): 389-397.
[14] HUANG Q B, AN Q W, SU H Q. Study and Realization of an Improved PBFT Algorithm as An Ethereum Consensus Mechanism[J]. Computer Applications and Software, 2017, 34(10): 288-293.
[15] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: Using Blockchain for Medical Data Access and Permission Management[C]// 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 2016: 25-30.
[16] 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.
[17] XUE T F, FU Q C, WANG C, et al. A Medical Data Sharing Model via Blockchain[J]. Acta Automatica Sinica, 2017, 43(9): 1555-1562.
[18] ZHANG L H, LAN F, JIANG P P, et al. A secure medical record storage and sharing scheme based on dual-blockchain[J]. Computer Engineering & Science, 2019, 41(9): 61-67.

YUAN Hao-nan, born in 2000, undergraduate, is a member of China Computer Federation. His main research interests include blockchain, information security and software engineering.

WANG Rui-jin, born in 1980, Ph.D, associate professor, master supervisor, is a member of China Computer Federation. His main research interests include information security, privacy protection and blockchain.