

分布式家庭医生服务系统与区块链电子病历*

吴 飞 张 莉 夏伦腾

(1 中南民族大学生物医学工程学院 武汉 430074 2 中南民族大学检测与仪器校级工程中心 武汉 430074)

〔摘要〕 对比传统集中式系统、分布式系统优缺点,指出分布式架构可解决传统架构存在的模块之间耦合度高、开发效率低等问题,设计构建分布式家庭医生服务系统,包括系统功能需求、体系架构、功能架构、分布式服务框架、服务调用流程等,同时在该系统中开发区块链电子病历,该系统及电子病历均通过测试。

〔关键词〕 区块链; 分布式系统; 家庭医生

〔中图分类号〕 R-056 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2020.09.013

Distributed Family Doctor Service System and Blockchain Electronic Medical Records WU Fei, ZHANG Li, XIA Lunteng, 1School of Biomedical Engineering, South - Central University For Nationalities, Wuhan 430074, 2Testing and Instrumentation Engineering Center, South - Central University For Nationalities, Wuhan 430074, China

〔Abstract〕 The paper compares the advantages and disadvantages of traditional centralized system and distributed system, points out that distributed architecture can solve the problems of high coupling between modules and low development efficiency existing in traditional architecture, proposes to design and build the distributed family doctor service system, including functional requirements, architecture, functional architecture, distributed service framework, service invocation process, etc. At the same time, the blockchain Electronic Medical Records (EMR) is developed in the system, and both the system and EMR passes the test.

〔Keywords〕 blockchain; distributed system; family doctor

1 引言

随着“互联网+医疗健康”发展提速,家庭医生签约成为重要一环。政府大力推行家庭医生制以

实现基层首诊、分级治疗目的,可有效缓解大型医院看病难、看病贵问题^[1-2]。现在大多数家庭医生服务系统为传统集中式系统,即由 1 台或多台主计算机组成中心节点集中存储数据,且整个系统所有业务单元集中部署于该中心节点上。集中式系统具较明显缺点:一是中央计算机需要执行所有运算,当终端较多时会导致响应速度变慢。二是如果终端用户有不同需求,需针对每个用户程序和资源进行单独配置,在集中式系统中进行该操作较困难且效率较低、灵活性差^[3]。分布式系统是一个硬件或软件组件分布在不同网络计算机上,通过消息传递进行通信和协调的系统。本研究结合区块链和传统关系型数据库开发新型电子病历独立部署在家庭医生服务系统中。经测试成功部署分布式系统,区块链

〔修回日期〕 2020-07-08

〔作者简介〕 吴飞,硕士研究生;通讯作者:张莉,博士,教授,发表论文 9 篇,国家发明专利 1 项。

〔基金项目〕 国家自然科学基金“基于脑肌电相干性的步行模式识别研究”(项目编号:No.81601586);中央高校基本科研业务费专项基金“一款加样指示跟踪系统的研发与设计”(项目编号:No.CZY18020)。

电子病历核心模块成功通过黑盒测试。

2 系统设计

2.1 功能需求

本系统分为用户端、医生端和管理员端，见图

1。用户端具有用户注册登录、我的医生、体检预约、查看体检报告、健康咨询、查看健康档案和区块链跳转等模块；医生端具有我的病人、医生登录、病人咨询、查看病人档案、预约设置和区块链跳转等模块；管理端具有用户管理、医生管理、体检设置、统计分析和区块链浏览等模块。

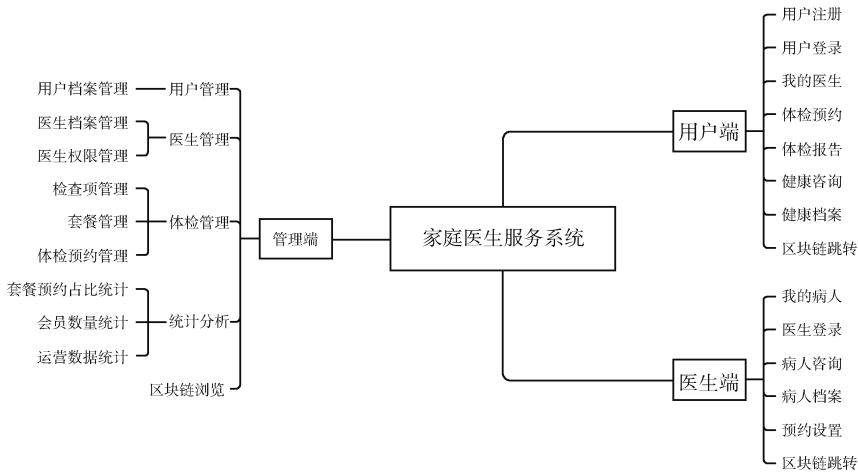


图 1 系统需求

2.2 体系架构

2.2.1 概述 本系统由区块链网络、后端客户端和独立前端 3 部分组成。采用浏览器/服务器 (Browser/Server, B/S) 架构^[4]，整体架构为 3 层设计，主要由 Web 客户端、Web 服务端和数据库 3 部分组成，见图 2。

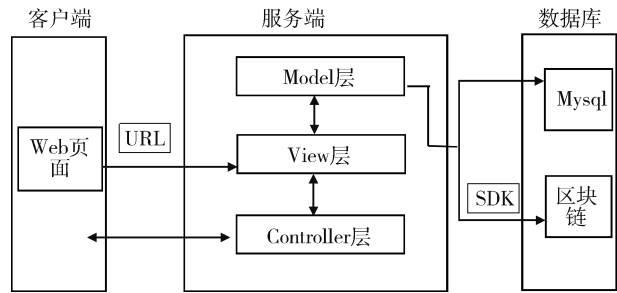


图 2 系统架构

2.2.2 Web 客户端 以 HTML5 页面形式展示在微信公众号上。基于手机浏览器开发，相当于采用传统 B/S 开发模式，将编写的 HTML5 页面根据手机尺寸进行调节，然后将页面内嵌到应用程序中，例如通过微信公众号访问 HTML5 页面。这种开发

方式不需要针对不同手机系统分别进行开发，只需要开发一个版本就能在不同手机上正常访问。

2.2.3 Web 服务端 采用模型、视图、控制器 (Model View Controller, MVC) 框架模式进行编写^[5]。第 1 层的模型层主要负责与数据库交互，用来为视图层和数据持久层准备数据并处理从视图层以及数据持久层接收到的数据。第 2 层的视图层负责显示数据处理结果与状态，从模型层获得数据并展示给用户，相当于提供页面供用户进行人机交互。第 3 层的控制器层用来控制应用程序和处理视图所发出请求。当控制器接收到用户请求后，将用户数据和模型相映射，然后控制器会选择用于响应的视图把模型更新后的数据展示给用户，即所谓的接、调、存、转。

2.2.4 数据库层 分为 Mysql 数据库和区块链两部分。使用 Fabric 搭建区块链网络用来存储用户隐私数据。框架依靠实用拜占庭容错算法 (Practical Byzantine Fault Tolerance, PBFT) 保证各节点数据的一致性，开发人员在使用框架进行开发的过程中可不必关注区块链底层模块构建，提高开发效率。

2.3 功能架构 (图 3)

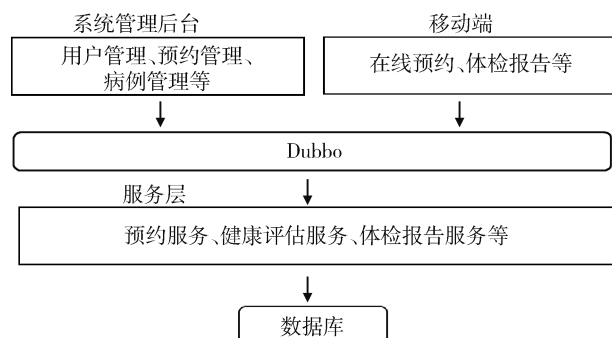


图 3 系统功能架构

Dubbo 是 Alibaba 开源的分布式服务框架，其最大特点是按照分层方式进行架构，使各层之间解耦合。使用 Dubbo 抽取核心业务作为独立服务，逐渐形成稳定服务中心，可用于提高业务复用灵活性，使前端应用更快速响应多变的市场需求。前后端开发人员协议规定交互数据字段，通过 Ajax 和 JSON 则可以实现。前后端分离设计模式可使系统实现高内聚低耦合，提高系统维护性。服务器端采用 SSM 框架设计，为用户端提供健康评估服务、预约服务等接口，用户端通过 POST 方式向服务器端发送请求。

3 分布式系统

3.1 优势

3.1.1 高度可靠性 数据分散存储在网络中不同主机上，系统中存在数据冗余，当一台机器发生故障时可使用另一台主机的备份。

3.1.2 均衡负载 每台主机可缓存本地最常用数据，不需要频繁访问服务器，减轻服务器负担，减少网络流量。服务器也可对任务进行分配和优化，突破几种系统中央计算机资源紧张的瓶颈。

3.1.3 满足不同需要 用户可根据需要安装不同操作系统、应用软件以使用不同服务，解决集中式计算机系统受限于中央计算机功能问题。基于以上分析，家庭医生服务系统采用面向服务 (Service - Oriented Architecture, SOA) 分布式架构可解决模块

之间耦合度高、开发效率低、扩展性差、不能灵活进行分布式部署等问题^[4]。

3.2 分布式服务框架

3.2.1 概述 当项目规模较小时使用简化增删改查工作量的数据访问框架——对象关系映射 (Object Relational Mapping, ORM)，达到减少部署节点和缩减成本的目的，但性能扩展困难。当规模逐渐变大单一应用架构无法满足项目需求时，使用 Web 框架 MVC，将应用拆分成数个独立应用，提升效率，但公用模块无法重复利用。当垂直应用越来越多，应用之间交互困难，简单、垂直的应用架构无法满足需求时，可使用分布式服务框架远程过程调用 (Remote Procedure Call, RPC)^[6]。

3.2.2 分布式应用架构 Dubbo 将远程方法调用透明化，只需简单配置，没有任何应用程序接口 (Application Programming Interface, API) 侵入。软负载均衡及其容错机制可在内网替代 F5 等硬件负载均衡器，减少成本和单点。本系统中 Dubbo 采用 Spring 配置方式，透明化接入应用，无 API 侵入，Dubbo 基于 Spring 的 Schema 扩展进行加载^[7]。服务提供方称为生产者 (Provider)，调用远程服务的消费方称为消费者 (Consumer)。用户 Web、商品 Web、订单 Web 都是生产者部署在 A 服务器上，用户服务、商品服务、订单服务则是消费者部署在 B 服务器上，见图 4。消费者可远程调用生产者提供的服务。当服务不断增多时消费者对生产者的调用关系越来越复杂，消费者调用服务时需了解由哪台服务器提供，也就是 IP (Internet Protocol) 地址与服务名称对应关系，需要注册中心实现。本系统使用 Zookeeper 注册中心。Dubbo 服务生产者在 Zookeeper 上创建一个临时节点，暴露自己的 IP 和端口，消费者调用服务时在 Zookeeper 上找到服务生产者，通过 IP 和端口对服务进行调用。如果生产者宕机，Zookeeper 可通过心跳机制检测到宕机机器，将其 IP 和服务名称对应关系从服务提供列表中删除，以免消费者误调用。

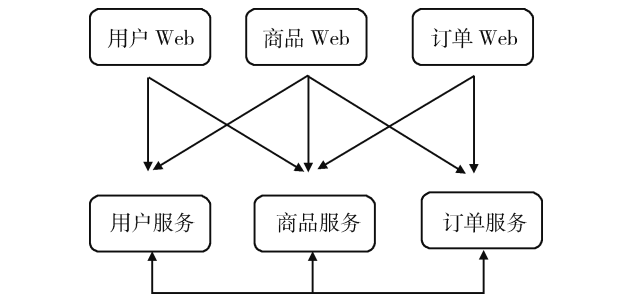


图 4 分布式应用架构

3.3 服务调用流程（图 5）

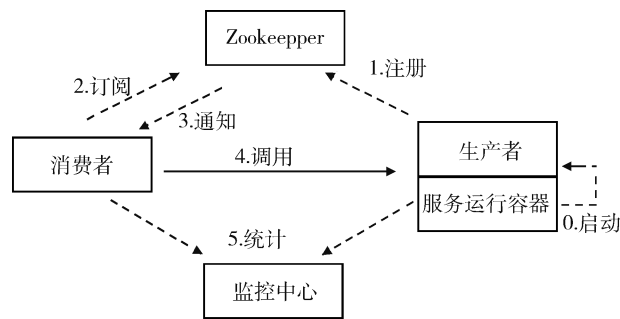


图 5 服务调用流程

本系统中将用户管理 Web、医生管理 Web、病历管理 Web、预约管理 Web、健康咨询管理 Web 作为生产者。当服务运行容器启动时服务生产者随之启动，生产者启动后在注册中心（Zookeeper）进行注册。服务消费者启动时向注册中心订阅所需服务，注册中心为其返回服务生产者地址列表，消费者从中调用所需服务。内存中的调用次数和时间统计后定时发送至监控中心。

3.4 服务调用测试

Dubbo 管控台可对注册到 Zookeeper 注册中心的服务或者服务消费者进行管理。通过管理平台可清晰看到服务生产者的机器 IP 和状态、服务消费者的机器 IP 和应用名等。服务生产者部署在容器 apache - tomcat - 7.0，端口 20880，进入 Dubbo 管控台可看到提供者信息。启动服务消费者，进入 Dubbo 管控台可看到服务消费者信息。生产者成功提供服务，消费者成功调用服务，Dubbo 服务框架搭建成功。

4 区块链电子病历设计

4.1 电子病历数据存储方式

传统在万维网上运行的数据库通常使用客户端 - 服务器架构，权限用户（客户端）可更改存储在中央服务器上的数据。依赖人为管理，如果访问权限出现错误或管理员操作不当数据将有泄露风险。相对于传统关系型数据库，区块链可视为一种去中心化分布式数据库，区块之间通过复杂的密码学算法连接，数据记录在每一个区块上，每一个区块通过计算前一区块的哈希值、新交易区块和随机数得来，保证区块唯一性^[8]。当区块足够多时，如果想篡改其中一个区块的数据，则需要对被篡改区块之后的所有区块重新进行密码学证明，保证区块链不可篡改性。每次数据改动都会通过数字签名合法记录在区块链上^[9]，即数据公开性和可溯源性。基上述优点区块链成为医疗数据存储的重要方式。传统区块链存储方式是将患者所有数据存储到区块链上，将加大系统开支，吞吐量问题难以解决。同时犹豫区块链性能对于患者隐私的保护，医疗数据分享成为难题^[10]。为解决该问题，本系统将传统关系性数据库与区块链结合，将患者个人信息与病历详细信息分开存储^[11]。

4.2 架构设计

4.2.1 电子病历模块 基于区块链的电子病历分为登录、病历生成、诊治信息存储以及查询等模块。电子病历的区块链网络单独存储于整个家庭医生服务系统中，设立单独登录模块，患者通过就诊卡 ID（Identity document）登录，没有注册模块，见图 6。患者第 1 次登录成功后会生成一对公私匙。

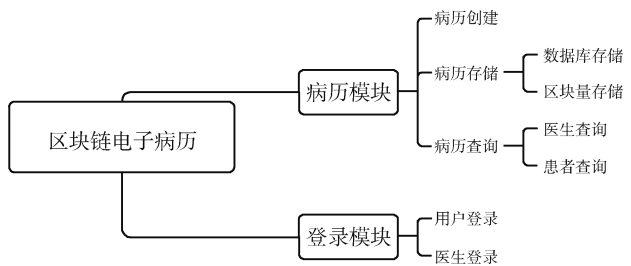


图 6 区块链电子病历模块

4.2.2 病历存储 使用非对称加密公匙加密用户病历上的个人隐私数据^[12], 私匙加密病历上的诊疗信息。将公匙保存到数据库, 私匙储存在患者就诊卡中, 区块链网络根据患者公匙生成的地址创建患者数据, 见图 7。由于已经将病历上的个人信息和诊治信息分离, 且诊治信息数据量大、操作频繁, 所以将诊治信息数据存储到 Mysql 数据库中, 解决数据所有权错权问题并减小区块链网络吞吐量。患者病历上的个人信息涉及个人隐私且操作不频繁。患者的诊治信息单独拥有唯一主键 ID, 系统将患者的个人信息通过对称加密后和数据库中的诊治信息主键 ID 加载到区块链网络中^[13], 组成患者的电子病历数据。区块链中只有患者的诊治信息主键 ID 而不包含个人信息, 既保护了患者的隐私也减少了区块链的吞吐量^[14]。

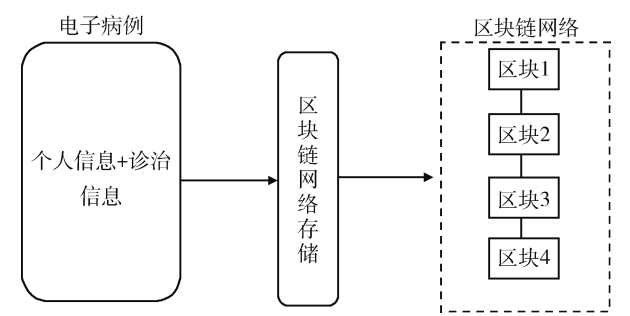


图 7 区块链网络病历存储

4.2.3 病历查询 分为患者查询和医生查询。由于诊治信息数据保存在 Mysql 数据库中, 医生查询时可直接搜索公开的诊治信息。患者就诊时可使用就诊卡 ID 进入查询系统查询病历信息。系统使用私匙进行解密后通过诊治信息的主键 ID 查询数据库中具体数据, 整理后返回给患者, 见图 8。

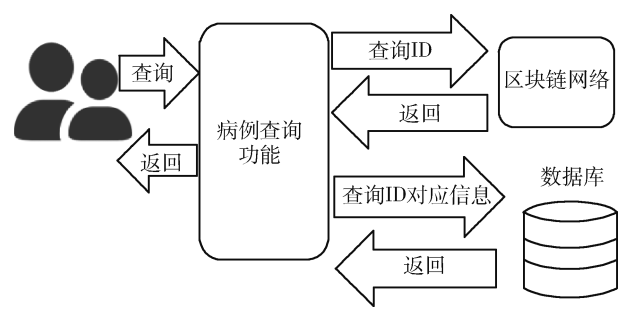


图 8 患者查询病历

4.2.4 病历生成 医生根据患者主诉请求填写病历信息, 完成后提交给服务器, 校验成功后将数据上传, 提取患者信息同时创建诊治信息数据摘要, 使用患者私匙进行签名, 向区块链发送更新患者病历的请求, 链代码解析请求并且更新患者数据^[15], 将病历表上的诊治信息主键 ID 和数据摘要信息更新到电子病历中。

4.3 核心功能测试

对区块链电子病历的核心功能分成 3 部分进行测试, 即用户登录、病历生成和病历查询测试, 每部分再分为数个测试单元, 采用黑盒测试方法。测试结果, 见表 1。针对将病历数据全部储存到区块链的传统方式, 通过区块链与传统关系型数据库的有效结合, 达到减小区块链网络吞吐量的目的, 同时使诊治信息数据与患者个人隐私分开, 解决了所有权错位问题, 可更好地分享医疗数据。

表 1 核心功能测试结果

测试功能	测试单元	结果
用户登录测试	1. 1 点击登录按钮可以跳转到登录页面	成功
	1. 2 输入就诊卡 ID 可以登录	
病历生成测试	2. 1 点击创建病历, 可以跳转到创建病历页面	成功
	2. 2 填写病历表单后, 可以提交	
	2. 3 提交病历后, 区块链网络和数据库更新数据	
病历查询测试	3. 1 输入就诊卡 ID 可以查询到病历	成功
	3. 2 医生输入关键词可以搜索到数据库诊治信息数据	

5 结语

该分布式家庭医生服务系统分别开发了用户端、医生端和管理端, 既有传统家庭医生服务系统的签约医生、预约体检、健康咨询、健康档案等功能, 同时部署区块链电子病历。针对传统集中式家庭医生服务系统低耦合性、灵活性差等缺点, 该系统采用分布式系统架构, 将核心模块分别部署在不同服务器上, 解决应用耦合性高的问题, 提高系统

可靠性和开发效率, 面对用户需求变化系统后期更易扩展。区块链与传统数据库的结合, 一方面保护患者隐私, 另一方面减少区块链网络压力, 同时解决医疗数据所有权错权问题。经测试分布式系统被成功部署, 区块链电子病历核心功能成功通过黑盒测试。该系统的开发为医疗机构、医生和用户提供联系平台, 为“互联网+医疗健康”增添动力, 为家庭医生制的推行奠定基础。

参考文献

1. 黄武全, 范晓晔, 翟佳焱, 等. 家庭医生团队下家庭医生助理的服务模式研究 [J]. 中国全科医学, 2020, 23 (25): 3146-3153.
2. 钟三字, 范亲敏. 家庭医生签约长效机制的落实路径——以分级诊疗为视角 [J]. 福建医科大学学报 (社会科学版), 2018, 19 (3): 10-15, 65.
3. 孟广雨, 于洁潇, 杨挺. 基于随机网络演算的分布式能源调控系统时延上界计算 [J]. 电工技术学报, 2020, 35 (11): 2360-2371.
4. 张慎武. 基于 SSM 框架集的省级档案科技管理平台的设计和实现 [J]. 数字技术与应用, 2018, 36 (4): 173-174, 176.
5. 王思洁. 基于 SSM 框架的零食在线销售系统的设计与实现 [J]. 南方农机, 2020, 51 (9): 223.
6. 苏畅. 对内存分布式列式数据库查询及优化探析 [J]. 时代农机, 2018, 45 (8): 139-140.
7. 罗松飞, 王梓成. 基于分布式集群的无人值守监控系统研究 [J]. 科技咨询, 2019, 17 (33): 13-16.
8. 田林. 基于区块链的电子病历存证系统的设计与实现 [D]. 济南: 山东师范大学, 2019.
9. 张圣垚. 基于区块链的电子病历系统的设计与实现 [D]. 哈尔滨: 哈尔滨工业大学, 2018.
10. 李博文. 基于区块链技术的医疗数据存储 [D]. 西安: 西安电子科技大学, 2018.
11. 栾新. 积极推进区块链的智能合约建设 [N]. 学习时报, 2019-12-27 (007).
12. 黄穗, 陈丽炜, 范冰冰. 基于 CP-ABE 和区块链的数据安全共享方法 [J]. 计算机系统应用, 2019, 28 (11): 79-86.
13. 黄敬英, 范勤勤. 区块链技术在医联体建设中的应用探讨 [J]. 医学信息学杂志, 2019, 40 (10): 30-34.
14. Donna Ellen Frederick. Blockchain, Libraries and the Data Deluge [J]. Library Hi Tech News, 2019, 36 (10): 1-7.
15. Esmaeilzadeh Pouyan, Mirzaei Tala. The Potential of Blockchain Technology for Health Information Exchange: experimental study from patients' perspectives [J]. Journal of Medical Internet Research, 2019, 21 (6): e14184.
6. 鲁春燕, 孙娟. 浅析 C/S 模式和 B/S 模式的优缺点 [J]. 福建电脑, 2008, 24 (6): 87.
7. Yajing L, Guie T. Design and Implement of University Laboratory Equipment Network Management Platform Based on C/S and B/S Model [C]. Saint Joseph: International Conference on Industrial Control & Electronics Engineering, 2012.
8. Loney K. Oracle Database 10g The Complete Reference [M]. New York: McGraw-Hill, 2004.
9. 朱二华. 基于 Vue.js 的 Web 前端应用研究 [J]. 科技与创新, 2017 (20): 119-121.
10. Crawford W, Kaplan J. J2EE Design Patterns [M]. Boston: O'Reilly Media Inc, 2003.
11. 蒋玉峰, 吕晓猛. 基于 MVC 架构的 Blackboard 平台运行数据分析系统研究 [J]. 常熟理工学院学报, 2014 (4): 87-91.
12. 高红岩. Struts 实用开发指南: 基于 MVC + MyEclipse 的 Java Web 应用开发 [M]. 北京: 科学出版社, 2007.
13. 王晓华. Web Service 接口描述语言 WSDL [J]. 中文信息, 2003 (10): 26-30.
14. Newcomer E. Understanding Web Services: XML, WSDL, SOAP, and UDDI [M]. Boston: Addison-Wesley, 2002.

(上接第 63 页)