基于密码云技术的医保智能基金监管平台应用系统研究

宁伟东，房验茹，杨禹军，王博琦，李佳娜，于靖雯 *
牡丹江医科大学，黑龙江 牡丹江 157011

摘　　要： 随着云计算、大数据、物联网和人工智能等技术的飞速发展，医保基金监管面临着前所未有的挑战与机遇。传统的医保基金监管模式主要依赖于人工抽检和事后核查，存在效率低下、覆盖不全、难以应对复杂违规行为等问题。同时在数字化时代，医疗数据成为重要的战略资源，其安全性直接关系到患者的隐私保护、医疗服务质量的提升以及医疗机构的信誉与社会稳定。因此，构建基于密码云技术的医保智能基金监管平台应用系统，成为提升医保基金监管效能、保障基金安全的重要手段。

关 键 词： 密码云；医保基金；监管平台；信息安全

Research on the Application System of Medical Insurance Intelligent Fund Supervision Platform Based on Password Cloud Technology

Ning Weidong, Fang Yanru, Yang Yujun, Wang Boqi, Li Jiana, Yu Jingwen *
Mudanjiang Medical University, Mudanjiang, Heilongjiang 157011

Abstract: With the rapid development of technologies such as cloud computing, big data, the Internet of Things, and artificial intelligence, the supervision of medical insurance funds is facing unprecedented challenges and opportunities. The traditional regulatory model of medical insurance funds mainly relies on manual sampling and post verification, which has problems such as low efficiency, incomplete coverage, and difficulty in dealing with complex violations. In the digital age, medical data has become an important strategic resource, and its security is directly related to the protection of patients' privacy, the improvement of medical service quality, and the reputation and social stability of medical institutions. Therefore, building an intelligent medical insurance fund supervision platform application system based on cryptographic cloud technology has become an important means to improve the efficiency of medical insurance fund supervision and ensure fund security.

Keywords: password cloud; medical insurance fund; regulatory platform; information safety

引言

随着医疗卫生事业的快速发展，医保基金作为社会保障体系的重要组成部分，其规模不断扩大，涉及面越来越广。同时，随着云计算、大数据、人工智能等技术的兴起，为医保基金监管提供了新的解决方案。其中，密码云技术以其高安全性、高可用性、动态伸缩性等特点，在保障数据安全、提升监管效率方面展现出巨大潜力。因此，将密码云技术应用于医保基金监管领域，构建基于密码云技术的医保智能基金监管平台应用系统，成为当前研究的重要方向。本文通过引入密码云技术，实现医保数据的集中存储、高效处理和安全传输，提升监管效率和准确性，利用智能审核和实时监控功能，实现对医保基金使用的全方位、全天候监管，及时发现并预警违规行为，通过数据加密、密钥管理、安全认证等手段，确保医保数据的安全性和完整性，防止数据泄露和篡改，通过数据分析和决策支持功能分析，为医保政策制定和调整提供科学依据，推动医保政策的精准实施和落地，本研究将密码云技术与医保基金监管相结合，探索新的技术应用模式，推动相关领域的技术创新和发展。

一、密码云技术概述

在构建医保智能基金监管平台的过程中，密码云技术作为一项关键技术，对于确保数据的安全性、完整性及系统的可靠性起着至关重要的作用。以下是对密码云技术的定义、特点及其关键组成的详细阐述[1]。

密码云技术是将密码学原理与云计算技术深度融合的产物，旨在通过云计算平台提供安全、高效的密码服务。它利用云计算的弹性扩展能力、高可用性和灵活性，结合密码学的加密、解密、签名、验证等核心技术，为各类应用提供安全可靠的密码保障。其具

基金项目：
[1]黑龙江省省属高等学校基本科研业务费科研项目 项目编号：2022—KYYWF–0711
[2]黑龙江省大学生创新训练计划项目 项目编号：202410229049
通讯作者：于靖雯，女，汉族，黑龙江省黑河人，临床医学硕士，研究方向：医疗管理、信息技术、临床医学。

有高安全性、高可用性、动态伸缩性、易于管理等特点：

高安全性体现在密码云技术采用先进的加密算法和协议，确保数据在传输和存储过程中的机密性、完整性和可用性；高可用性表现为通过云计算的分布式架构和冗余部署，实现密码服务的持续可用和快速恢复；动态伸缩性则是根据业务需求自动调整密码服务资源，满足高并发、大数据量的处理需求；最后是提供统一的密码管理界面和API接口，简化密码服务的部署、配置和运维，便于管理[2]。

二、密码云技术在医保智能基金监管平台系统中的关键技术

（一）对称加密技术

对称加密技术是一种使用相同密钥进行加密和解密的密码技术。在基金监管数据分析系统中，对称加密技术可以用于对大量数据进行快速加密，提高数据的存储和传输效率。常见的对称加密算法有 AES、DES 等。

（二）非对称加密技术

非对称加密技术是一种使用公钥和私钥进行加密和解密的密码技术。在基金监管数据分析系统中，非对称加密技术可以用于数字签名、密钥交换等方面，为数据的完整性和身份认证提供保障。常见的非对称加密算法有 RSA、ECC 等。

（三）哈希函数

哈希函数是一种将任意长度的消息映射为固定长度的哈希值的函数。在基金监管数据分析系统中，哈希函数可以用于数据的完整性校验和数字签名等方面，确保数据的真实性和完整性。常见的哈希函数有 MD5、SHA-1、SHA-56等。

（四）数字证书

数字证书是一种由权威机构颁发的电子文件，用于证明用户的身份和公钥的合法性。在基金监管数据分析系统中，数字证书可以用于用户的身份认证和数字签名等方面，为系统的安全提供保障。数字证书通常由证书主体、证书颁发机构、证书有效期、公钥、数字签名等部分组成。证书主体是指拥有证书的用户或设备；证书颁发机构是指颁发证书的权威机构；证书有效期是指证书的有效时间范围；公钥是用于加密和解密数据的密钥；数字签名是证书颁发机构对证书内容进行签名，以确保证书的真实性和完整性[3]。

（五）身份认证协议

身份认证协议是一种用于验证用户身份的协议。在基金监管数据分析系统中，身份认证协议可以用于用户的登录认证、权限认证等方面，确保只有合法的用户才能访问系统。常见的身份认证协议有 Kerberos、SSL/TLS 等。

三、基于密码云技术的医保智能基金监管平台需求分析

（一）功能需求

1.数据采集和存储

平台需要能够实时采集医保基金相关的数据，并将其存储在密码云中。数据采集包括医保缴费数据、医疗费用数据、个人信息等。数据存储需要保证数据的安全性和完整性，同时支持数据的快速检索和查询。

2.数据分析和挖掘

平台需要具备数据分析和挖掘的能力，能够对医保基金的使用情况、资金流向等进行分析，发现异常情况和风险点。同时，平台还应该支持数据可视化，将分析结果以图表等形式展示，方便监管人员进行决策和管理。

3.风险预警和监测

平台需要具备风险预警和监测的功能，能够根据设定的规则和指标，实时监测医保基金的使用情况，并发现异常行为和风险点。一旦发现异常情况，平台应该能够及时发出预警信息，提醒监管人员采取相应的措施[4]。

4.权限管理和审计

平台需要具备权限管理和审计的功能，确保只有授权人员才能访问和操作敏感数据。平台应该支持多级权限设置，以及对操作日志的记录和审计，方便追溯和责任追究。

5.接口对接和数据交换

平台需要与其他医疗信息系统进行接口对接，实现数据的交换和共享。平台应该支持标准化的数据格式和协议，确保数据的一致性和互通性。

（二）技术需求

1.密码云技术

平台需要采用密码云技术，确保数据的安全性和隐私保护。密码云技术可以对数据进行加密和解密，防止数据泄露和篡改[5]。

2.大数据和人工智能

平台需要具备大数据和人工智能的能力，能够处理海量的医保基金数据，并进行智能分析和挖掘。大数据和人工智能可以帮助发现异常情况和风险点，提高监管效率和准确性。

3.数据可视化

平台需要支持数据可视化，将分析结果以图表等形式展示，方便监管人员进行直观的理解和决策。

4.接口技术

平台需要支持与其他医疗信息系统进行接口对接，需要具备接口技术和标准化的数据格式和协议。

四、基于密码云技术的医保智能基金监管平台应用系统实现方案

（一）基于密码云技术的医保智能监控系统

基于密码云技术的医保智能基金监管系统的构建是一个复杂而细致的过程，它涉及到多个技术层面和应用场景的深度融合，旨在通过先进的信息技术手段提高医保基金的管理效率和安全性。从以下四个方面（远程视频查房、就医身份认证监控、医疗设备管理、个人就诊信息共享平台）进行的具体阐述：

1. 远程视频查房系统是医保智能监控系统的重要组成部分，它利用云计算和视频通信技术，允许医保监管人员在不到现场的情况下，对定点医疗机构进行实时或定时的远程查房。这不仅提

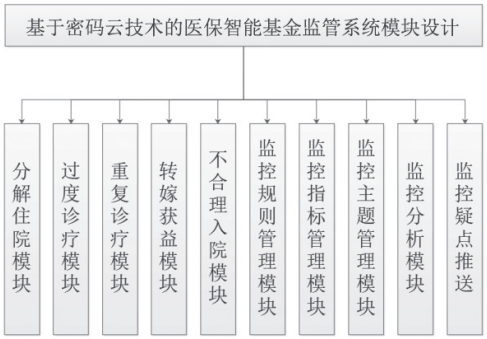
高了查房效率，还降低了行政成本，并有助于及时发现和纠正违规行为。通过搭建稳定的视频通信平台，确保查房过程中的视频流畅和画质清晰。将查房视频存储在云端，支持随时回放查看，以便后续分析和处理。结合密码云技术中的身份认证功能，确保查房人员的身份真实可靠，并防止非授权访问[6]。

2. 就医身份认证监控是防止医保欺诈的重要手段之一。通过密码云技术和生物识别技术，对参保人员的就医身份进行实时验证，确保人证相符，防止冒名就医等欺诈行为。采用指纹识别、面部识别等生物识别技术，对参保人员的身份进行快速准确的验证。将生物识别数据进行加密处理，并通过安全的网络通道传输至医保智能监控系统，确保数据的安全性。建立医保欺诈黑名单数据库，对发现的欺诈行为进行记录和跟踪，并实时更新黑名单信息。

3. 医疗设备管理是医保智能监控系统的重要补充，通过对医疗设备的实时监控和管理，确保医疗设备的正常使用和合规操作，防止因设备问题导致的医保基金浪费和欺诈行为。利用物联网技术，将医疗设备连接到医保智能监控系统中，实现设备的远程监控和管理[7]。

4. 个人就诊信息共享平台是基于云计算和大数据技术构建的，旨在实现参保人员就诊信息的全面共享和高效利用。通过该平台，医保管理部门、定点医疗机构和参保人员可以方便地查询和使用就诊信息，提高医疗服务的效率和质量。利用云计算和大数据技术，将参保人员的就诊信息进行统一存储和管理，实现跨地区、跨机构的信息共享。建立统一的数据标准和互认机制，确保不同医疗机构之间的就诊信息能够无缝对接和共享。在信息共享的过程中，严格遵守隐私保护法律法规，建立严格的权限管理制度，确保个人就诊信息的安全性和隐私性。

（二）基于密码云技术的医保智能基金监管系统模块设计



分解住院模块实时收集医疗机构的住院患者情况，分析医疗行为，识别潜在的违规行为，应用算法或数据模型来自动监测异常模式。对住院间隔过短和住院频次过高的诊疗行为进行监管，系统会应用算法或数据模型来自动监测异常模式[8]。过度诊疗模块识别包括不符合诊疗规范、无依据或理由的检查治疗和用药，如套餐式检查、无阳性结果的多次大型仪器检查等。此类行为不仅浪费医疗资源，还加重患者负担，并可能导致医保基金损失。重复诊疗模块对诊疗项目进行监管，一般情况下医药机构在一定周期内对同一对象，开具相同诊疗项目的诊疗次数会有规定次数（排除特殊病种和特殊诊疗项目：如糖尿病血糖检查），超过规定次数的系统会自动筛选出来，暴露成疑点，规范医药机构的相关医疗行为。转嫁获益模块识别让患者到院外药店或机构自费购买贵重药品或耗材；通过不同账务系统，部分费用以自费形式结算；隐形自费，即将可报销费用转嫁给患者；以及异地手工报销中的费用隐藏等，针对以上事件提高识别违规行为的准确性和效率。不合理入院模块杜绝医疗机构将无需住院治疗或在一般门诊即可治疗的患者收治住院，通过实施监管和数据分析对只检查无治疗、无检查只有药物治疗、仅有物理治疗无药物治疗、降低标准入院、虚假入院等行为。监控规则管理模块依据法律法规、药学知识等基于密码云技术制定知识库和规则库大模型，规则的阈值的修改可以可以随着模拟测验、核对病例、监管经验不断完善等确保规则的有效性和精准度。监控指标管理模块遵循遵循结果导向、过程管理、全面客观、科学精准的原则，针对医保基金使用、支付和拨付的全流程，全面、客观、动态地反映医疗机构、医保、参保患者三方在医疗和 DRG 支付过程中的实际情况，通过多项监控指标的组合，实现对某类违规行为的多维分析。基于密码云技术对监控主题下的数据进行深度挖掘和分析，及时发现异常情况和潜在风险[9]。系统将一个或多个监控规则组合或监控指标组合纳入到监控主题，并根据本地违规特征，为规则或指标分配不同的权重，从而提高监管分析疑点推送的精准度。利用多维度数据分析、实时监控、全流程管理、风险模型构建等手段建设监控分析模块。系统筛查出疑点后，利用大模型进行分析判断，通过密码云技术分别对接不同权限接口进行统一办理[10]。

五、结论

密码云技术在医保智能基金监管系统中具有重要的应用价值。通过采用密码云技术技术，可以有效地保障医保智能基金监管数据分析系统中数据的保密性、完整性、真实性和可用性，提高基金监管的安全性和有效性。然而，密码云技术在应用过程中也面临着一些挑战，需要通过优化密码算法和实现、加强密钥管理、推动密码标准统一、遵守法律法规等措施来加以解决。随着密码技术的不断发展和完善，相信密码云技术在医保智能基金监管系统中的应用将会越来越广泛，为医疗行业的稳定发展提供更加可靠的安全保障。

参考文献

[1]大数据平台下智能监控体系助推徐州市按病种收付费的实践［J］. 黄广振；包婷；高泽方；李芬；覃朝晖. 中国医疗保险，2022(01).

[2]过度医疗行为认定及医保监管指标研究［J］. 郑树忠；龚忆莼；耿韬；黄蛟灵. 中国医疗保险，2022(12).

[3]基于身份加密的 Ad hoc网络安全模式［J］周慧华. 湖北民族学院学报（自然科学版），2005,(03).

[4]荣春萌. 基于联盟链的边缘计算节点身份认证机制研究［D］. 重庆邮电大学，2022.

[5]张林东，赵勇，王翔宇. 商用密码技术标准在云计算场景下的应用实践［J］. 信息技术与标准化，2024(z1):34-40.

[6]何重阳，刘晓浩，陈刘忠，等. 量子密码技术现状及云安全应用展望［J］. 网络安全技术与应用，2023(9):27-28.

[7]叶寒. 云计算密码应用技术体系的合规性分析［J］. 信息安全与通信保密，2012(11):144-146.

[8]邓一星，蔡沂，王文翰. 云计算技术下大规模用户密码安全认证算法［J］. 计算机仿真，2022,39(2):141-144.

[9]霍炜，王小云，韩文报. 密码运行安全体系与关键技术研究［J］. 密码学报，2024,11(3):485-503

[10]何智，赵海英，雷波. 面向数据中心安全的密码保障体系研究［J］. 信息安全与通信保密，2024(1):48-59.