国密证书动态信任评估系统

师　凯　杨清淞　余埔铭　叶清清　谢云跃　蒋　凯　邓　琴　包致婷通讯作者

重庆工程学院　重庆　400056

摘　要：在于解决传统PKI证书管理中数据孤岛、信任单点依赖等问题，系统利用区块链技术实现证书全生命周期数据的分布式存证与不可篡改追溯，结合国密SM2/SM3/SM4算法保障数据隐私与通信安全。通过智能合约自动执行证书状态验证与动态信任评分，AI模型实时分析链上证书行为数据，触发阈值预警与自动化吊销。创新融合联盟链共识机制与国密密码体系，构建去中心化、抗攻击的证书信任网络，适用于政务、金融等高安全场景，助力构建国产化、高度可信的证书系统。

关键词：区块链；PKI证书管理；国密算法；智能合约；AI模型

引　言：

在当前数字化进程加速的背景下，传统PKI证书管理体系因中心化架构逐渐暴露出数据孤岛和单点信任依赖等局限性，难以满足政务、金融等高安全场景对可信认证的迫切需求[1]。本文提出的区块链与AI融合的国密证书动态信任评估系统，通过分布式账本技术实现证书全生命周期数据的不可篡改存证，结合国密SM系列算法构建自主可控的密码安全体系，有效规避了传统CA机构集中式管理的潜在风险。系统引入AI驱动的动态行为分析模型，能够实时监测证书使用异常并触发自动化预警机制，将静态证书验证升级为持续演进的信任评估流程。这种技术协同不仅提升了证书管理的透明性与抗攻击能力，还为不同场景提供了国产化、高可信的密码基础设施支撑，对企业进行安全身份认证有重要实践意义[2]。

一、需求分析

经济可行性分析：建设本系统所需要的服务器、存储设备以及其他硬件，市场上的高性价比选择多种多样，软件方面选用的PyQt5、MySQL8.0等都是开源软件，不需要支付高昂的软件授权费用。开发过程中使用的GmSSL国密算法库也是开源的，降低了开发成本，具有较好的经济可行性。技术可行性分析：国密算法有着清晰明确的标准与规范，GmSSL库也给出了对应的实现方式，方便在系统里进行集成。PyQt5被运用到客户端开发中，可迅速搭建起功能多样丰富的图形用户界面，MySQL8.0拥有强大的数据存储以及管理能力，可契合系统对于数据存储以及查询的需求。在政策方面，国家积极推动国密算法的应用，颁布了一系列法律法规以及政策给予支持，鼓励企业与机构使用国产密码技术来保障信息安全，本系统有良好的社会可行性。

基于政务、金融等高安全场景对证书管理的刚性需求，该系统需构建一个集区块链存证、国密算法加密与AI动态评估于一体的可信基础设施。安全性需求：结合IPFS存储SM4加密的证书明文数据，确保操作可追溯且难以篡改[3]；引入AI动态信任模型，基于滑动窗口统计规则对证书使用行为（如单日下载次数、验证成功率）进行实时分析，当异常阈值连续触发时自动预警或吊销证书，形成智能决策闭环。使用SM2完成数字签名与密钥交换，SM3哈希算法保障数据完整性，SM4对称加密保护通信隐私，并通过SQL注

图1　系统总体设计

入防护、密码加密存储测试等安全验证，确保在对抗攻击环境中保持稳定运行[4]。

二、系统设计

系统在基础通信层面沿用asyncio.start_server搭建高性能TCP服务，运用异步非阻塞I/O模型高效处理海量并发连接，每个连接均由handle_client协程独立管理，不仅负责请求解析、路由分发及响应返回，还新增了异步日志投递机制，将实时通信数据推送至AI分析队列。CryptoUtils模块在整合SM2、SM3、SM4等国密算法的基础上进行了扩展，除承担密钥生成与常规加解密外，还集成了Fabric SDK适配接口与IPFS交互逻辑，负责对区块链交易进行SM2签名以及将证书密文上传至分布式存储网络。DatabaseManager升级为混合存储管理器，在利用连接池维护MySQL中用户凭证与元数据的同时，通过智能合约接口与Hyperledger Fabric区块链网络交互，实现数据的“链上链下双重锚定”，既保留了关系型数据库的高效查询，又保障了核心数据的不可篡改性。SessionManager凭借SM4动态会话密钥维持加密通信隧道，结合AI模型的实时反馈，能够在检测到异常流量行为时动态缩短会话有效期或强制阻断连接。系统采用装饰器模式实现的日志系统不再局限于UI回调展示，而是作为AI动态信任评估模块的数据采集探针，实时捕获异常堆栈与操作行为，构建了一个分工清晰、云边端链协同工作的增强型C/S分层架构。

三、过程论述

证书签发模块：客户端首先负责构建可信的申请数据包，涉及模板ID、主题名称以及公钥等必要参数，验证请求数据的完整性和有效性。系统会检查该用户是否拥有使用指定证书模板的权限，利用SM3杂凑算法依据主题名称、时间戳以及公钥生成唯一的证书序列号。与传统流程不同的是，客户端在提交申请时，会同步采集当前的设备指纹与网络环境特征（作为AI风险评估的初始基线数据），连同证书申请信息一并提交至服务器。服务器接收后，将证书申请信息保存到数据库中，状态设置为“pending”。服务端主要由handle_certificate_application和handle_certificate_approval两个核心函数构成，实现了“智能风控前置”与“区块链存证确权”的双重保障。handle_certificate_application负责处理证书申请的初始化流程，如接收用户提交的主题名称、公钥、模板ID及行为特征数据，首先验证参数的有效性与用户权限。另外在生成唯一序列号之前，系统调用AI规则引擎对申请者的历史行为及当前请求特征进行实时匹配（例如检测是否存在批量异常申请或黑名单设备），计算初始风险预期。若风险过高，直接驳回；若通过，则将申请信息存入MySQL数据库，状态设为“pending”，并为AI模型建立该证书的初始行为基线档案。handle_certificate_approval则负责处理证书的签发、加密存证与上链流程，是实现数据不可篡改的核心环节。即管理员审核通过后，系统依据模板设置有效期，使用CA私钥基于SM2算法对证书内容进行数字签名，生成正式证书（X.509格式）。随后，为了保护隐私与数据安全，系统立即调用SM4算法对证书明文文件进行加密，并将加密后的密文上传至IPFS分布式存储网络，获取唯一的内容寻址哈希（CID）。系统计算证书原文的SM3哈希值作为唯一数字指纹，通过Fabric SDK调用智能合约（Chaincode）。合约将 证书Hash、IPFS CID、序列号、初始AI风险评分及有效期打包成交易，经共识节点确认后写入区块链账本，实现证书状态的“链上确权”。最后，函数将MySQL数据库中的证书状态更新为“Valid”，并记录关联的区块链交易ID（TxID），完成链上链下数据的最终一致性同步。

证书管理模块：该模块对证书整个生命周期进行深度管控，融合了AI动态风控与区块链分布式账本技术，以此保障证书的实时有效性以及全流程的不可篡改可追溯性。当出现证书私钥泄露、用户身份信息变更或AI模型监测到异常使用行为（如异地突发高频访问）等情形时，证书吊销流程将通过“人工-智能”双轨机制触发。证书吊销通过revoke_certificate函数实现，该函数逻辑已被重构为多层级操作：首先，当管理员手动确认或AI决策模块自动判定风险超标时，函数被调用；其次，系统不仅会在本地MySQL数据库中将证书状态更新为“revoked”并发布更新后的CRL，它会通过Fabric SDK同步调用区块链智能合约，发起一笔状态变更交易。该交易经过共识排序后，将链上对应的证书资产状态永久修改为“REVOKED”或“FROZEN”，确保吊销操作一旦执行便无法被恶意回滚或篡改。此外，系统实现了增强型的证书下载功能，下载请求均通过SM4解密密文后交付用户，且所有的下载与验证行为都会作为特征数据实时输入至AI评估模型中，用于持续的信任度计算。整个管理过程的操作记录不再仅依赖本地日志，而是生成了包含TxID的双重审计记录，从而实现了证书生命周期管理达到可追溯性与安全审计要求。

证书验证模块：通过handle_certificate_verification函数实现。首先验证请求中的证书序列号格式与长度的有效性，然后系统会立即启动AI行为感知逻辑，将当前验证请求的来源IP、时间频次、地理位置等元数据实时推送至风险评估模型的输入层，用于更新该证书的动态信用评分。接着，系统执行“双重状态校验”机制：一方面从本地数据库查询证书的名称、公钥及有效期

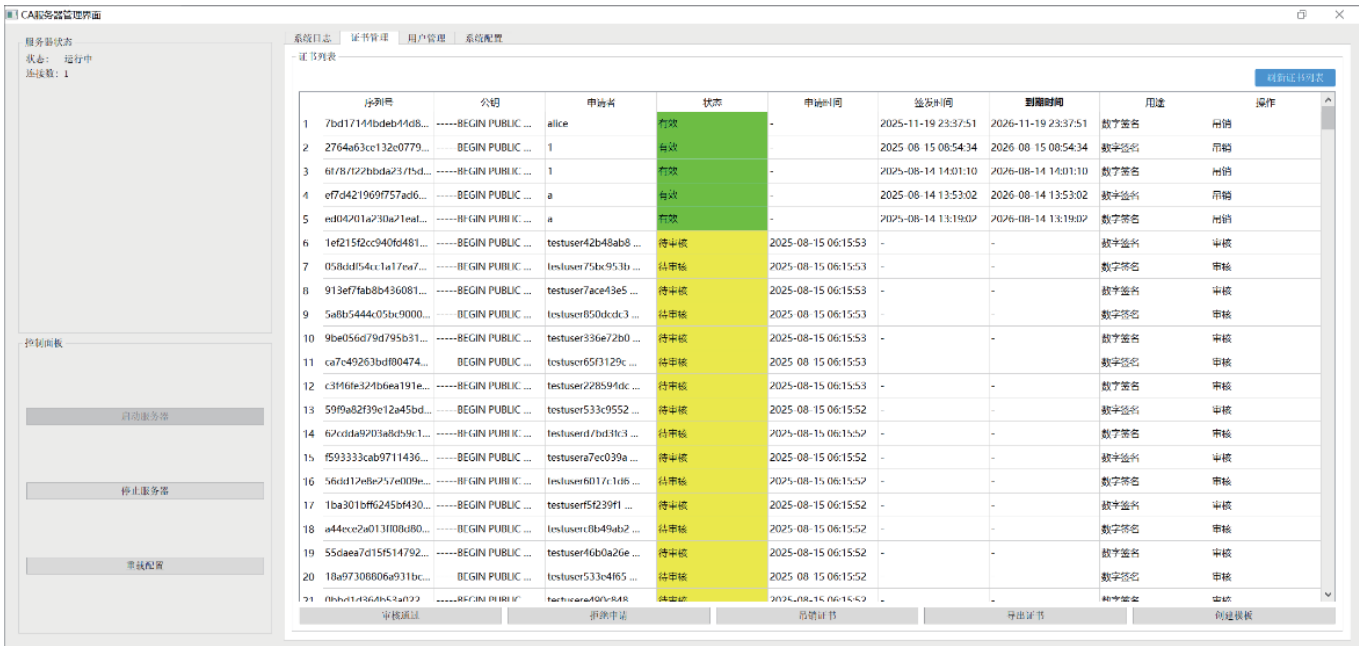

图2　系统主界面图

等基础信息；另一方面，利用Fabric SDK向区块链发起查询请求，检索链上账本中该证书哈希对应的实时状态（Valid/Frozen/Revoked）。这种机制确保了即便本地数据库被攻击篡改，验证结果依然能依据区块链的不可篡改性做出正确判断。随后，函数将当前时间与证书过期时间进行比对，并结合AI实时反馈的风险等级进行综合判定，若证书处于有效期内但AI判定当前行为风险极高（如短时异地登录），系统将即时触发临时冻结策略。最后，系统重建证书关键数据，使用SM2公钥验证数字签名。最终返回的验证结果不仅包含证书是否有效、主题信息及有效期，还附带了基于区块链确权的最新状态以及AI评估的动态风险提示，实现了从“验签名”到“验行为”的安全跨越。（见图2）

四、总结

本文聚焦于基于区块链、AI和国密算法对证书动态信任评估的CA认证中心展开深入研究，采用SM2完成证书签名、SM3生成哈希、SM4加密通信链路，并利用AI驱动实时分析达成证书全生命周期的管理，制定严谨的密钥生成、存储、备份策略以及使用授权和审计机制。每个功能模块都经过精心的设计与优化，可契合不同主体多样化的认证需求，凭借定制安全策略与认证流程，像是多因素身份认证、严格的证书审核流程等，全方位保障数字社会安全活动顺利开展，为各行业数字化转型提供安全可靠的认证服务。

参考文献：

[1]郭亚州.基于国密算法的CA认证应用研究[D].华北电力大学(北京),2023.

[2]卢秋如.国密算法应用研究综述[J].软件,2023,44(01):123-125.

[3]李付国.区块链技术在档案数据管理中的应用[J].信息记录材料,2025,26(03):141-143.

[4]梁丹池,李敏盛.基于PKI体系的数据加密系统架构[J].视听,2022,(12):182-185.

项目支持：2025年重庆工程学院大学生创新创业训练计划项目（AI赋能的国密证书动态信任评估系统 CXCY2025024）

作者简介：师凯（2004.8.18-）男，汉族，重庆人，本科在读，专业为信息安全。