教育考试院信息系统安全防护中的数据加密与访问控制研究

文◆甘肃省教育考试院　袁小鹏　张建飞　蒙琴琴　张荞君
兰州乐智教育科技有限责任公司　杨维旺

引言

教育考试院信息系统承担招生考试、成绩管理、信息发布等重要职能，系统中储存着大量考生个人信息、考试数据等敏感信息。随着信息化程度不断提高，系统面临着日益严峻的安全挑战。传统单一防护措施难以满足当前安全需求，亟须构建系统化安全防护体系。数据加密技术结合访问控制机制成为解决问题的关键方案，通过加密算法保障数据安全性，借助访问控制确保授权访问。开展系统安全防护研究对提升教育考试院信息系统安全防护水平具有重要意义。

1 教育考试院信息系统的理论概述

根据教育考试招生业务实际需求，教育考试院信息系统围绕“业务、数据、指挥”三条主线，遵循实现“三库两流一图”的新要求，采取“一级（省级）建设、四级应用”的建设模式，涵盖考试基础数据库建设、考试业务系统、决策指挥系统、综合管理系统、数据交换平台以及技术支撑体系等六大建设任务，实现对教育考试的全局统一指挥、全程分级管理、全域实时监控。

从理论层面来看，系统整体架构遵循分层设计思想，包含基础设施层、数据层、支撑层、业务层、表现层 5 个主要层级。数据层负责存储考生信息、考试题库、成绩数据等关键信息；业务层承担数据处理、逻辑运算、权限控制等功能；表现层则为用户提供操作界面。针对数据存储环节，采取加密技术确保数据机密性；针对数据传输过程，运用安全通信协议保障传输安全；针对用户访问，实施严格的身份认证与授权管理。随着教育考试院业务范围不断扩大，教育考试院信息系统面临着来自内外部多重安全威胁，外部主要表现为黑客攻击、网络窃听、恶意破坏等，内部则存在违规操作、数据泄露等风险。通过系统性地开展数据加密和访问控制的业务研究，提升教育考试院信息系统数据安全防护水平就显得尤为重要。

2 数据加密技术与密钥管理

2.1 数据加密算法选择设计

教育考试院信息系统涉及大量敏感数据，选择加密算法时，需要综合考虑数据量、安全等级、性能开销等多个因素。针对静态存储数据，采用对称加密算法中安全性较高的高级加密标准，密钥长度选择 256 位，分组长度 128 位，加密模式采用密码分组链接模式[1]。加密过程中，明文分组 P 经过加密变换得到密文分组 C，其数学表达如式（1）所示。

$$C = E(K, P) \tag{1}$$

式（1）中，K 为加密密钥，E 为加密变换函数。

在密码分组链接模式下，第 i 个分组的加密过程如式（2）所示。

$$C_i = E(K, P_i \oplus C_i - 1) \tag{2}$$

式（2）中，⊕表示异或运算。对于用户身份认证信息，使用非对称加密算法，密钥长度选择 2048 位，保障认证过程安全性。

【课题项目】甘肃省科技重点研发项目：基于人工智能的高频开关变换器和小型化天线的磁建模及基础产业化应用研究（24YFGA028）；兰州市科学技术局：有限网络带宽约束的核用多智能体系统协同控制研究（2024-3-4）
【作者简介】袁小鹏（1981—），男，江西都昌人，博士研究生，高级教师，研究方向：数字化转型及数智化。

考虑到系统性能需求，设计混合加密方案，即对数据采用对称加密，对会话密钥采用非对称加密。在具体实现中，根据不同数据类型选择合适加密强度。考生个人信息采用全字段加密；考试成绩数据对关键字段进行加密；普通信息采用轻量级加密方案。通过差异化加密策略，在保障安全性基础上提升系统运行效率。系统采用分层分级的密钥分发架构，通过多重认证确保密钥安全传递。

2.2 密钥生命周期管理

密钥生命周期管理贯穿产生、使用、更新、销毁全过程。密钥生成采用硬件随机数发生器，保证随机性，生成记录类型、用途、有效期等属性信息。使用过程严格限制使用次数，超出阈值强制更新，系统自动记录使用情况。更新采用无缝切换策略，确保业务连续性，更新前对原数据重加密保证访问不受影响。系统支持有效期自动管理，临近到期提前预警。

2.3 数据加密传输过程

数据加密传输采用多层防护策略，构建安全传输通道。传输开始前，双方进行身份互认，建立信任关系[2]。认证通过后，协商生成会话密钥，用于数据加密传输。传输数据按固定大小分块处理，每块数据独立加密。对传输数据块 D_i 进行哈希计算，得到校验值 H_i，计算公式如式（3）所示。

$$H_i = H\left(D_i \| K_i\right) \tag{3}$$

式（3）中，H 为哈希函数，K_i 为当前数据块的校验密钥，$\|$ 表示拼接操作。

接收方通过相同方式计算校验值并比对，验证数据完整性。数据块加密使用会话密钥，减少计算开销。系统记录数据传输过程，实现传输行为追溯。针对互联网传输场景，增加安全隧道加密。实际应用中，校验过程所需时间 t 与数据块大小 n 呈线性关系，如式（4）所示。

$$t = \alpha n + \beta \tag{4}$$

式（4）中，α 为单位数据处理时间，β 为系统基础开销。

传输系统具备断点续传功能，提高传输可靠性。数据接收完成后，自动清除会话密钥，降低泄露风险。传输过程采用动态路由机制，提升传输安全性。系统支持传输性能动态调节，确保传输质量。针对远程传输需求，设计多级加密传输方案。

3 系统访问控制模型构建

3.1 角色属性管理的定义

教育考试院信息系统中角色属性管理采用多维度定义方式。根据工作职责，划分管理员角色、考务人员角色、数据分析人员角色等基本类型。管理员角色负责系统配置、用户管理、安全策略制定；考务人员角色执行考试组织、成绩管理、信息发布工作；数据分析人员角色负责数据统计分析、报表生成。各类角色根据工作区域分为省级、市级、区县级 3 个层次。角色属性包含基本信息属性、权限属性、时效属性、安全属性。基本信息属性记录角色名称、描述；权限属性定义数据访问范围；时效属性控制角色有效期限；安全属性规定访问控制级别。

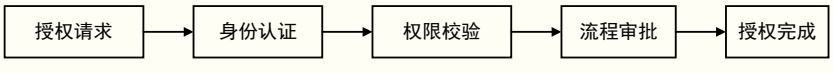

图 1 授权管理机制流程

3.2 访问控制层级组成

教育考试院信息系统访问控制层级从底层到顶层依次包含数据访问层、资源控制层、权限管理层、策略控制层[3]。数据访问层直接与数据库交互，实现数据读写控制；资源控制层管理系统资源访问，采用资源池化管理方式；权限管理层负责角色权限分配、权限校验、权限传递；策略控制层制定访问控制规则，协调各层级工作。层级间通过标准接口通信，保证控制策略顺畅执行。各层级部署安全审计模块，记录访问控制过程。系统设置层级间数据缓存机制，不同层级采用独立加密方案，确保层级安全隔离。

3.3 授权管理机制流程

授权管理机制通过规范化流程实现精确授权控制。授权请求经过身份认证、权限校验、流程审批 3 个环节（见图 1）。身份认证采用多因素认证方式，结合密码、数字证书、生物特征等手段。权限校验包括角色权限验证、时效性检查、安全级别核对。流程审批按预设审批链进行，需经过直接主管、安全管理员、系统管理员逐级审批。紧急授权设置快速审批通道，但权限使用期限严格限制。授权过程全程记录，系统定期扫描已授权账号，对过期权限自动清理。针对敏感操作权限，实施双人授权机制。

3.4 模型层级设计分析

教育考试院信息系统访问控制模型采用分层递进结构。基础

层实现身份识别鉴别功能，采用身份认证矩阵管理用户信息[4]；安全层负责权限分配管理；业务层处理访问请求；扩展层支持临时授权、紧急访问、权限代理等特殊需求。模型各层级通过安全信道传递控制信息，协同配合构建完整的安全防护体系。

4 系统实验结果分析

4.1 系统环境参数设置

实验环境采用分布式架构部署，主服务器配置双路处理器，内存为 64GB，存储采用固态硬盘阵列。网络环境使用千兆以太网互联，实验数据库部署在独立服务器，配置主备双机热备份。客户端测试设备包括台式工作站、笔记本电脑、移动终端等不同型号设备。软件环境中操作系统选择稳定版本，数据库采用分布式集群部署。实验数据集包含百万级用户信息记录、千万级考试数据记录，数据类型覆盖文本、图像、文档等多种格式。测试工具采用专业性能测试软件，支持并发压测、性能监控、数据采集等功能。

4.2 功能实现测试分析

功能测试围绕数据加密传输、访问控制、权限管理 3 个核心模块展开（见表 1）。数据加密传输测试验证了加密算法正确性、传输可靠性，测试数据表明，加密解密准确率达 99.99%，传输成功率达 99.95%。测试过程中模拟断网、网络延迟、数据包丢失等异常情况，系统均能正常恢复工作。访问控制测试验证了角色权限分配、访问策略执行情况，结果显示，权限分配准确率为 100%，越权访问拦截率为 100%。权限管理测试重点关注授权流程执行、紧急授权响应、权限自动清理等功能，测试结果表明，授权流程执行正常，紧急授权响应时间控制在 5s 内，过期权限清理准确率为 100%。功能测试覆盖率达到 98%，关键功能测试用例执行结果符合预期。

表 1 系统功能测试数据对比表

测试指标	优化前	优化后	提升比例
加密解密准确率	98.5%	99.99%	1.49%
传输成功率	97.8%	99.95%	2.15%
权限分配准确率	98.9%	100%	1.1%
越权访问拦截率	99.2%	100%	0.8%

4.3 性能指标测试结果

性能测试重点关注系统响应时间、并发处理能力、资源占用情况（见表 2）。在正常负载下，系统平均响应时间保持在 200ms 以内，其中数据加密平均耗时 50ms，权限验证平均耗时 30ms[5]。并发测试显示，系统能够稳定支持 1000 名用户同时在线操作，极限并发数达到 1500 名用户，超出阈值后系统通过任务排队机制确保平稳运行。资源监控数据表明，处理器使用率峰值达 75%，内存占用率峰值达 65%，存储读写速度维持在 300MB/s。在持续 72h 压力测试中，系统运行稳定，未出现功能异常、数据错误、响应超时等问题。性能指标测试数据证实，系统具备支撑教育考试院日常业务运转能力。

表 2 系统性能测试数据对比表

测试指标	优化前	优化后	提升比例
平均响应时间	350ms	200ms	42.9%
并发用户数	600	1000	66.7%
数据加密耗时	85ms	50ms	41.2%
权限验证耗时	55ms	30ms	45.5%

结语

教育考试院信息系统安全防护方案通过将数据加密技术与访问控制相结合，实现了对敏感数据的保护和精确的授权管理。混合加密方案在保证安全性的基础上兼顾了系统性能，多层级访问控制体系实现了灵活的权限管理。实验结果证实，该系统具备较强的安全防护能力，能够满足实际应用需求。未来，将在现有数据加密和访问控制的基础上，持续完善安全防护机制，为教育考试院信息系统的安全稳定运行奠定坚实基础。

引用

[1] 姜韬.深度学习技术在网络数据加密与解密中的应用研究[J].网络安全和信息化,2024(10):37-39.

[2] 沈锟麒,李中禹.基于随机策略更新的大数据访问控制方案及实验分析[J].中国高新科技,2024(18):41-43.

[3] 李莉,陈介,朱江文.多权威可撤销密文策略属性基加密数据共享方案[J/OL].计算机科学,1-10[2024-11-28].https://link.cnki.net/urlid/50.1075.tp.20241023.0933.004.

[4] 刘炜,李淑培,田钊,等.基于区块链的去中心化多授权机构访问控制方法[J].郑州大学学报(理学版),2025,57(5):46-53.

[5] 马益帆.基于区块链的云存储访问控制机制研究[D].西安:西安工业大学,2024.