基于区块链技术的计算机数据安全系统设计

刘海军

（内蒙古开放大学，内蒙古 呼和浩特　010011）

摘要：随着信息技术的快速发展，数据安全成为亟待解决的关键问题。基于区块链技术的计算机数据安全系统设计，引入先进的加密算法与权限管理机制，可增强数据的安全性和完整性。系统在功能设计上涵盖了数据加密、验证、权限管理和安全审计四大模块，并在硬件层面配置了高性能处理器、大容量存储设备等关键组件，确保系统的高效稳定运行。经过严格的测试验证，该系统展现了良好的数据保护能力和可靠性。

关键词：区块链技术；数据安全；加密算法；权限管理；安全审计

随着数字化转型的加速推进，信息安全问题日益凸显，传统的中心化数据管理方式在面对数据篡改、泄露等风险时显现出诸多不足。区块链技术凭借其去中心化、透明性高、数据不可篡改等特点，为解决数据安全问题提供了新的解决方案。当前，虽然已有部分基于区块链的数据保护方案，但在实际应用中仍存在性能瓶颈、隐私保护机制不完善等问题，因此，设计一种高效且安全的数据管理系统具有重要的应用价值。

一、需求分析

（一）功能需求

系统须具备数据加密功能，包括对称加密、非对称加密和哈希加密；实现数据验证，涵盖完整性校验、数字签名验证和数据一致性检查；拥有权限管理，包括用户身份认证、访问权限分级和权限动态调整；提供安全审计功能。

（二）性能需求

系统需在短时间内完成加密、解密、数据验证等操作。能支持高并发处理，存储效率高，网络传输延迟低，负载分配均匀性高。确保系统在各种复杂场景下稳定运行，满足高效处理数据和保障数据安全的性能指标。

二、计算机数据安全系统设计

（一）功能设计

1. 数据加密功能

（1）应用对称加密算法。在基于区块链技术的计算机数据安全系统设计中，对称加密算法作为数据加密功能的核心组成部分，已采用高级加密标准（Advanced Encryption Standard，简称 AES）算法实现数据的快速加密与解密。系统利用对称密钥生成机制，能够根据预设的安全级别生成不同长度的密钥，如常见的 128 位、192 位和 256 位密钥。在加密过程中，原始数据通过 AES 算法中的加解密函数，利用特定的密钥进行变换，生成密文数据存储于区块链中。解密时，系统同样依赖相同的密钥恢复原数据。

（2）集成非对称加密技术。在非对称加密技术集成中，本系统选用 RSA 公钥加密算法来实现密钥交换和数字签名功能。生成一对公私钥，即每个用户拥有唯一的一组密钥对，其中私钥由用户本人妥善保存，而公钥则可公开分发。当用户需要发送加密消息时，使用接收方的公钥加密数据，只有持有相应私钥的接收方才能解密。

（3）哈希加密实现。为确保数据的完整性和防止篡改，系统采用 SHA–256 哈希函数来实现哈希加密功能。当数据进入系统时，SHA–256 算法计算出固定长度的哈希值，该哈希值作为数据的指纹记录在区块链中。一旦数据发生变化，再次计算得到的哈希值将与原记录的哈希值不符，从而检测到数据被篡改。为增强哈希值的安全性，系统还结合盐值（salt）技术，在计算哈希值之前向原始数据添加随机数，使得即使输入相同的数据也会产生不同的哈希输出，进一步提高数据的安全性。

2. 数据验证功能

（1）完整性校验机制。在基于区块链技术的计算机数据安全系统中，完整性校验机制主要采用哈希算法实现。具体

作者简介：刘海军，男，内蒙古五原人，硕士研究生，讲师；研究方向：计算机科学与技术、教育理论。

而言，使用 SHA-256 算法为数据生成唯一的哈希值。当数据被存储或传输时，同时存储或传输该哈希值。接收方在接收到数据后，重新计算数据的哈希值，并与接收到的哈希值进行对比。如果两个哈希值一致，则说明数据在传输或存储过程中没有被篡改，完整性得到保证。子功能包括哈希值计算、存储和对比。哈希值计算对数据进行一系列复杂的数学运算得出。

（2）数字签名验证。此系统的数字签名验证功能主要基于非对称加密算法。使用 RSA 算法生成公钥和私钥对。发送方使用自己的私钥对数据进行签名，生成数字签名。接收方使用发送方的公钥对数字签名进行验证。子功能有密钥生成、签名生成和验证。密钥生成过程中，选择两个大素数计算出公钥和私钥。签名生成时，发送方对数据进行哈希运算得到哈希值，然后用私钥对哈希值进行加密生成数字签名。验证时，接收方对收到的数据进行哈希运算，同时用发送方的公钥对数字签名进行解密得到另一个哈希值，对比两个哈希值是否一致，从而确定数据的真实性和完整性。

（3）数据一致性检查。数据一致性检查在区块链网络中进行多节点验证来实现。当数据被写入区块链时，多个节点同时记录该数据。在检查数据一致性时，从不同节点读取数据进行对比。如果各个节点的数据一致，则说明数据具有一致性。子功能包括节点数据读取、对比和结果判断。节点数据读取以区块链的分布式存储结构实现。对比功能对从不同节点读取的数据进行逐字节对比。结果判断根据对比结果确定数据是否一致。若不一致，则触发警报或采取相应的纠错措施，确保数据在整个系统中的一致性。

3. 权限管理功能

（1）用户身份认证。在基于区块链技术的计算机数据安全系统中，用户身份认证采用密码学技术与区块链的不可篡改特性相结合的方式。主要子功能包括用户注册、密码验证和身份令牌生成。在用户注册阶段，系统为用户生成一对公钥和私钥，并将公钥与用户信息一起存储在区块链上。密码验证时，用户输入密码，系统使用哈希算法对密码进行处理，然后与存储在区块链上的哈希值进行对比。若一致，则身份认证通过。系统会为通过认证的用户生成一个身份令牌，令牌在后续的操作中用于验证用户身份。

（2）访问权限分级。访问权限分级功能定义不同的权限级别和对应的操作权限来实现。主要子功能包括权限级别定义、权限分配和权限验证。首先，根据数据的敏感程度和用户的角色，定义多个权限级别，如高、中、低。然后，在系统初始化或用户注册时，根据用户的角色和需求为其分配相应的权限级别。在用户访问数据时，系统会根据用户的权限级别和数据的权限要求进行验证。如果用户的权限级别满足数据的权限要求，则允许访问；否则，拒绝访问。

（3）权限动态调整。权限动态调整功能允许系统根据特定的条件和事件自动调整用户的权限。主要子功能包括条件监测、权限调整算法和权限更新。系统持续监测特定的条件，如用户行为、数据的重要性变化等。当条件满足时，触发权限调整算法。该算法根据预设的规则和策略，计算出用户新的权限级别。然后，系统将新的权限信息更新到区块链上，并通知用户。权限更新过程采用区块链的分布式共识机制，确保权限调整的合法性和一致性。例如，如果用户的行为异常，系统可降低其权限级别，以保护数据安全。反之，如果用户表现良好，系统可提高其权限级别，以提供更多的便利。

4. 安全审计功能

（1）操作日志记录。在基于区块链技术的计算机数据安全系统中，操作日志记录功能主要利用分布式账本技术实现。子功能包括事件捕获、日志存储和查询。事件捕获模块实时监测系统中的各种操作事件，如数据访问、修改、删除等，记录事件发生的时间、用户、操作类型等详细信息。日志存储利用区块链的不可篡改特性，将操作日志以交易的形式记录在区块链上，确保日志的真实性和完整性。查询功能允许管理员和授权用户根据特定的条件查询历史操作日志，以便进行审计和故障排查。

（2）异常行为监测。此功能采用机器学习算法和规则引擎相结合的方式。子功能有行为建模、实时监测和警报触发。首先，对正常用户行为进行分析和建模，建立行为基线。使用聚类算法、主成分分析等技术对历史操作数据进行分析，提取正常行为特征。实时监测模块持续监测用户的操作行为，将其与行为基线进行对比。如果发现行为与基线有较大偏差，如频繁访问敏感数据、异常的操作时间分布等，则触发规则引擎进行进一步判断。规则引擎根据预设的规则集，如访问频率阈值、操作时间范围等，确定是否为异常行为。

（3）审计报告生成。审计报告生成功能利用数据分析和可视化技术。子功能包括数据收集、分析和报告生成。数据收集模块从区块链上获取操作日志和其他相关数据。分析模块对收集到的数据进行统计分析、趋势分析等，提取关键信息和指标，如操作频率、用户活跃度、异常行为发生率等。报告生成模块根据预设的模板和格式，将分析结果以可视化的形式呈现为审计报告，如表格、图表等。报告包括系统整体安全状况、用户行为分析、异常行为总结等内容，为管理员提供全面的安全审计视角。

（二）硬件设计

1. 高性能处理器

在基于区块链技术的计算机数据安全系统设计中，选用 Intel Xeon W-3300 系列处理器作为核心计算单元。该系列处理器具备多达 18 个核心，支持超线程技术，能够提供高

达 36 线程的并发处理能力，主频范围从 3.0 GHz 至 4.3 GHz，并支持动态加速技术。Xeon W-3300 系列处理器内置 Intel Turbo Boost Max Technology 3.0，可在需要时自动提升单核或多核的运行频率，以满足密集型计算任务的需求。

2. 大容量存储设备

为满足大规模数据存储与快速访问的需求，系统选用 NVMe SSD 硬盘作为主要存储介质。具体型号为 Samsung PM1733a，该硬盘提供高达 15.36 TB 的存储容量，并支持 PCIe 4.0 x4 接口，能够实现高达 7GB/s 的读取速度和 6GB/s 的写入速度。PM1733a 系列硬盘采用最新的 V-NAND 技术，提高存储密度的同时，也保证数据读写的稳定性。

3. 安全加密芯片

在设计中，采用 Infineon SLE78 系列安全芯片来实现数据加密功能。SLE78 系列芯片支持国际标准的加密算法（如 AES、RSA、ECC），并且内置硬件加速器，能够高效处理加密运算。该芯片符合 ISO 7816、EMV Level 1 标准，并通过 Common Criteria EAL5+ 认证，确保其在金融交易等敏感场景中的安全性。

4. 可靠网络接口

为确保数据在网络传输过程中的安全与高效，系统配置了 Intel Ethernet 700 Series X722-T4 网络接口卡。该网卡支持 10GBASE-T 标准，能够在铜缆上实现高达 10 Gbps 的数据传输速率。X722-T4 网卡具备 Intel Data Direct I/O（DDIO）技术，减少了 CPU 负载，提高数据处理效率。

三、计算机数据安全系统运行测试

（一）搭建测试环境

为确保测试的严谨性和准确性，测试环境的搭建在符合系统设计要求的条件下进行。测试平台使用基于 Intel Xeon W-3370M 处理器（3.0 GHz，18C/36T）的服务器，配备 32GB DDR4 ECC 内存和 Samsung PM1733a NVMe SSD（15.36 TB）。网络环境由 Intel Ethernet 700 Series X722-T4 网卡支持，确保 10 Gbps 的数据传输速率。测试环境中的所有硬件参数与生产环境一致，确保测试结果的可比性与真实性。测试前，对所有硬件设备进行预热和状态检查，保证其处于最佳工作状态。根据系统设计文档，配置软件环境，包括操作系统（Ubuntu 20.04）、区块链软件（Hyperledger Fabric v2.2.0）、加密算法库（OpenSSL 1.1.1f），以及必要的网络服务和安全设置。确保测试平台能够稳定运行并支持所有测试场景。

（二）进行运行测试

1. 功能测试

所有功能测试均在规定的时间内完成，加密 / 解密时间、完整性校验时间、权限验证时间和日志记录时间均达到预期的性能指标。加密 / 解密时间 0.2s 确保 10MB 文件的快速处理，完整性校验时间 0.1s 验证 5MB 文件的完整性，权限验证时间 0.05s 保证了 1000 条访问记录的高效处理，而日志记录时间 0.01s 确保 100 条操作事件的实时记录。系统功能稳定，无异常情况发生，满足设计要求。

表 1　功能测试结果

测试场景	测试指标	指标数据	测试数据	测试结果
数据加密	加密 / 解密时间	0.2s	10MB 文件	通过
数据验证	完整性校验时间	0.1s	5MB 文件	通过
权限管理	权限验证时间	0.05s	1000 条访问记录	通过
安全审计	日志记录时间	0.01s	100 条操作事件	通过

2. 性能测试

性能测试结果表明，系统能够支持高并发处理，1000 个并发用户进行 10000 条访问请求，系统稳定运行，无任何性能瓶颈。存储效率测试中，读写 10GB 数据时，IOPS 达到 150000，远超设计指标。网络传输延迟测试结果为 0.04ms，低于预期的 0.1ms，证明了网络环境的高效性。负载均衡测试中，2000 个并发请求的负载分配均匀性达到 98%，确保了资源的合理分配和系统的高效运行。系统性能卓越，达到设计预期。

表 2　性能测试结果

测试场景	测试指标	指标数据	测试数据	测试结果
并发处理	并发用户数	1000	10000 条访问请求	通过
存储效率	IOPS	150000	读写 10GB 数据	通过
网络传输	延迟	0.04ms	10000 个数据包	通过
负载均衡	负载分配均匀性	98%	2000 个并发请求	通过

四、结语

本研究基于区块链技术设计计算机数据安全系统，集成对称与非对称加密算法、哈希加密，实现高效数据保护；数据验证与权限管理功能确保数据完整性和用户访问安全；安全审计机制有效监测异常，提升系统整体安全性。未来，将深化算法优化，探索更高效能硬件集成，加强系统与人工智能技术融合，以适应不断演进的数据安全需求，推动区块链技术在更广泛领域应用，构建更加安全、可靠的数据保护生态。

参考文献：

[1] 张丽．基于区块链技术的计算机数据安全保护分析 [J]．无线互联科技，2021，18（12）：101-102.
[2] 覃德．基于区块链技术的计算机数据安全保护分析 [J]．长江信息通信，2023，36（6）：42-44.
[3] 祝启云．基于区块链技术的计算机数据安全保护研究 [J]．信息与电脑（理论版），2023，35（23）：206-208.
[4] 李兴福．区块链技术在计算机数据安全中的应用 [J]．集成电路应用，2024，41（4）：81-83.
[5] 刘雪梅．基于区块链技术的计算机机房数据安全防御系统设计 [J]．网络安全和信息化，2024（7）：126-128.