DOI:10.20033/j.1003-7241.(2025)12-0151-04

基于区块链的人力资源大数据安全存储系统设计

张 露,蔡 琴,王宇峰
(中共国网甘肃省电力公司党校,甘肃 兰州 730000)

摘 要:人力资源大数据存储时存在信息存储不完整问题,导致存储安全性低。因此,设计基于区块链的人力资源大数据安全存储系统。将 Virtex6 FPGA 应用于存储界面,采用 6 口的收发信机作为标准接口;通过监控模块监控用户个人信息,避免 IP 地址泄露;将 RESTfuI 存储芯片与监控模块相连,安全控制大数据存储。使用区块链技术加密大数据,获取区块链报文,并对消息标题加密编程,获取与数据库主机相匹配的信息存储安全系数。在存储体系中引入激励机制,有效调度区块数据,并校验大数据安全存储的完整性。结果可知,该系统安全性系数最高为 0.99,具有安全存储效果。

关键词:区块链;人力资源大数据;数据安全存储;数据完整性;大数据加密
中图分类号:TP315 **文献标志码**:A **文章编号**:1003-7241(2025)12-0151-04

Design of human resource big data secure storage system based on block chain

ZHANG Lu, CAI Qin, WANG Yufeng
(CPC State Grid Gansu Electric Power Company Party School, Lanzhou 730000, China)

Abstract: Incomplete information storage exists in human resources big data storage, resulting in low storage security. Therefore, a human resources big data secure storage system based on blockchain is designed. Virtex6 FPGA is applied to the storage interface, and 6-port transceiver is used as the standard interface. It monitors the user's personal information through the monitoring module to avoid IP address disclosure, connects restfui memory chip with monitoring module to safely control big data storage, uses blockchain technology to encrypt big data, obtains blockchain message, encrypts and programs the message title, and obtains the information storage security factor matching with the database host. An incentive mechanism is introduced into the storage system to effectively schedule block data and verify the integrity of secure storage of big data. The results show that the highest safety factor of the system is 0.99, which has the effect of safe storage.
Keywords: Blockchain; big data of human resources; data ecure storage; data ntegrity; big data encryption

0 引言

近年来,随着人力资源企业的不断出现,互联网人才的竞争也越来越激烈。目前,数据隐私泄露、数据伪造、完整性破坏等诸多问题,已严重影响了人力大数据的质量[1-2]。其中,海量人力数据存储性能的提升成为该领域研究的热点问题。随着云计算技术发展迅速,其核心是将各种数据资源抽象成一种可供使用者自由使用的资源库。然而,由于人员操作失误、系统攻击、软件和硬件故障以及平台供应商的信用不良等问题存在,导致其效果较差。由于云数据可被多个有权限的用户访问,无法提供数据的来源和个人的操作记录[3-4]。在一些特殊的行业中,如工业监控、跟踪等,不能全面地审查系统的动态信息。为此,当前学者们提出了各种各样的存储系统。

文献[5]提出一种基于区块链技术的人力资源大数据加密方法。利用区块链技术中的哈希函数计算人力资源数据的活跃程度,通过与阈值对比消除冗余数据;利用区块链技术将大数据划分为若干数据区块,实现数据分化;利用 RSA 算法生成密钥,通过密钥对经过置乱处理的数据块实施加密,完成基于区块链技术的人力资源大数据加密。但该方法在保障数据安全的同时,可能面临计算资源消耗大、加密解密效率受网络拥堵影响等挑战,需进一步优化。文献[6]提出了一套基于区块链技术的分布式数据安全存储方案,采用分布式节点架构实现数据分片存储,通过改进的共识机制和智能合约提供可信的数据访问控制。方案构建了包含加密存储、数据溯源和故障恢复在内的多层次安全防护体系,针对系统可用性、数据完整性和访问效率进行了优化。但该方案在跨链交互兼容性上仍有不足,且大规模节点部署时共识效率会下降,后续需针对性改进以提升综合性能。

针对上述问题,为了提高人力资源大数据的完成性,提出并设计基于区块链的人力资源大数据安全存储系统,该方法采用了区块链技术,并且结合了激励机制,以此提高大数据完成性的同时,提高存储安全性系数。

1 系统总体结构设计

基于区块链的人力资源大数据安全存储系统总体结构,如图 1 所示。

收稿日期:2024-04-07

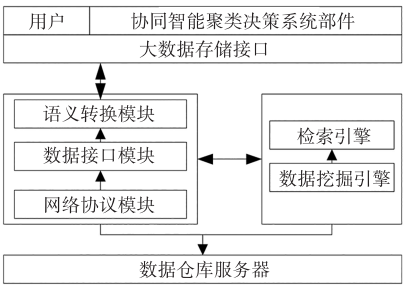


图 1　安全存储系统总体结构

由图 1 可知,本系统主要由大数据存储接口、语义转换模块、网络协议模块和数据挖掘引擎组成。根据数据储存系统基本操作原则,交换各类资料[7]。通过采集系统内部和外部数据,可将数据输入到数据仓库中,并与用户交互。

1.1　存储接口

将 Virtex6 FPGA 应用于存储界面设计中,通过区块链技术实现大规模的大数据读取和写入[8-9]。基于 DES 的加密存储技术,扩展数据缓存内存,采用 6 个收发信机作为标准接口,实现存储接口设计。接收端使用 6 路 TLK2711-SP 收发器与存储器接口相连,将接收端的信息通过数字电路集成芯片传输后,再将采集到的数据存储到内存条中,由 DMA 完成写入和上传操作[10-11]。最后,通过 6 路 TLK2711-SP 收发器将高密度信息安全地存储在内存条中。

1.2　监控模块

用户监控模块是用户数据加密与存储的主要工作部件,由一组数据块监控和一组主机监控组成。客户端是监控模块的最底层。主动监控技术可从网络环境中提取使用者个人信息,并将其标记保存在主机上,被动监控则是通过 geth 节点监控和传输给服务器。主机群无法主动地将消息传送给使用者,只能在被动状态下执行连线指令[12]。由于服务器不会泄露 IP 地址,不会受到任何的攻击。

1.3　检索引擎

检索引擎采用基于区块链的主机技术集成用户的信息。当区块链主机的存储器容量超过额定容量时,该应用程序的驱动程序将中断与存储器主机的数据传输,为用户的数据处理提供更加稳定的数据传输环境[13]。检索引擎结构,如图 2 所示。

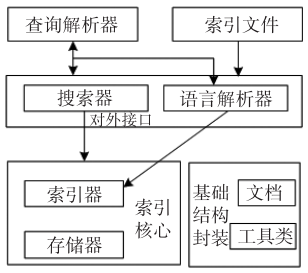


图 2　检索引擎结构

由图 2 可知,该结构包括数据搜索、数据索引构建、数据存储和用户接口。其中,数据搜索主要负责从文件库中搜索与人力资源大数据相关数据;数据索引主要负责从搜索的数据中抽出索引项,并构建索引表;数据存储负责在网络上快速查出相关文档,用户接口负责查询用户信息[14]。

1.4　大数据存储模块

大数据存储模块主要功能是对互联网环境下处理的用户信息,在满足用户对网络环境需求时,将数据和信息传输给其他系统处理设备。为了实现网络应用环境良好平衡,采用 RESTfuI 芯片,该芯片采用区块链主集成,主要作用是与用户的监控模块相连,可以更好地控制用户信息传输[9]。该芯片在大数据存储模块中主要有两个方面优势;一方面,能够为用户提供较为平衡的信息传递环境,另一方面也能适当地减轻网络主机所承受的信息存储压力。利用区块链主机的计算能力,限制和限制网络的密码,既可以避免用户的信息积累,又可以有效地维护相应的信息编码环境。

2　软件设计

2.1　基于区块链的大数据加密处理

区块链报文包括三个部分:消息尾部、消息主体、消息标题。在不同地域环境下,用户信息参数保留了原来“二域值”编码方式。如果已知加密程序的源码,在邻近域号间的进位条件必须被精确定义[15]。消息尾部亦被称作区块链消息后缀,代表使用者信息目的地传送地点,在不同干扰条件下,消息尾部结构也会发生改变;消息主体是区块链信息的主体,代表使用者信息的实际传送步长,在信息加密编程情况下,消息主体结构所占的比重较高,数据库主机存在的数据越多;消息标题也被称为区块链的报文前缀,代表使用者信息的真实储存地点。大数据加密处理受到主机行为影响,存在多样性。

使用区块链技术加密大数据时,将区块链报文表示为

$$Q=\frac{1}{S}\left[\frac{z}{(\alpha-\alpha_0)^2+\lambda^2}\right] \tag{1}$$

式中,z 表示消息体平均值;α 表示消息尾部;α_0 表示消息标题定义条件;λ 表示用户信息特征加密系数;S 表示消息标题的加密编程结果。

对于消息标题的加密编程结果,设 f 表示消息标题的原始长度数值,计算公式为

$$S=\beta\left[\frac{Y_{\max}^{\gamma}-\varepsilon f}{\rho\times\kappa^2}\right] \tag{2}$$

式中,β 表示数字签名的插入作用条件;$Y_{\max}^{\gamma}$ 表示最大信息输出量;ε 表示对称密码变异系数;ρ 表示用户信息特征值;κ 表示与数据库主机相匹配的信息存储安全系数。

在此基础上,进一步提高系统的安全性,设计存储索引智能合约,具体步骤如下。

初始化系统,设置一个可信锚 T,T 选择随机数 s 作为私钥 h_T,并且计算公钥为

$$p_T = sP \tag{3}$$

式中，s 表示随机数；P 表示基点。T 将 s 本地安全存储，并向各个节点发布系统参数，具体为

$$\{p,q,P,p_T,d_0,d_1,d_2\} \tag{4}$$

式中，q 表示由 P 生成的子群的阶为大素数；d_0,d_1,d_2 表示抗碰撞散列函数。

数据索引，将索引域分为 m 个子区，每个子区包含 n 行，确定数据的域关联性用如下公式计算各子区之间的相似度 Y 为

$$I(Y \mid m,n) = 1-(1-Y^n)^m \tag{5}$$

基于此，依据 Y 得到最终的数据索引。

通过上述加密步骤对人力资源大数据存储结果进行加密，能够解决当前大数据存储方法中存在安全性问题，保证了人力资源大数据存储安全。

2.2 大数据存储流程设计

大数据存储流程使用多级访问控制模式，保证相邻实体间能够实时更新信息。基于此，设计基于区块链的大数据存储流程，如图 3 所示。

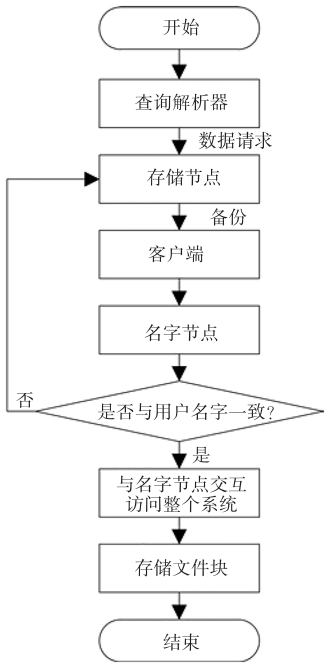


图 3 基于区块链的大数据存储流程

2.3 基于区块链激励机制的安全存储完整性校验

区块链技术主要优点是在存储体系中引入了一种激励机制，该机制具有一定决策权，能够保证各个节点能够调度区块数据。该方法在动态数据存储系统中的应用却有很大的缺陷，在分析局部行为和确保动态数据存储安全、有效前提下，在所有终端拥有被验证的数据时，为了获得最大的利益，需要校验大数据安全存储的完整性。

在人力资源大数据安全存储过程中，设 $E=\{E_1,E_2,\cdots,E_n\}$ 为人力资源大数据集合，由某个终端打包区块组成的验证集合 $R=\{R_1,R_2,\cdots,R_n\}$。对提交区块验证时，获取的验证结果为 T，可满足公式

$$T=\begin{cases}1, & \text{经验证，提交区块合法}\\ -1, & \text{经验证，提交区块不合法}\end{cases} \tag{6}$$

将获取区块验证结果分为如下几种情况。

1）本轮计算尚未结束，针对需要最早校验的数据，应先选择本轮的最佳区块，通过该区块校验数据；

2）本轮计算结束，针对需要校验的某个数据，应先挑选所有需要经过校验的数据，并通过该数据获取最大收益区块；

3）本轮计算结束，在获取最大收益区块后，分析其是否合法，如果合法则证明获取的数据完整。

3 系统测试

所选择硬件环境有客户机、服务器和 100 M 以太网交换机，服务器配置：2.6 GHz CPU，1 GB RAM，80 GB 硬盘，CPU 为 2.66 GHz，RAM 为 512 MB，硬盘为 80 GB。该系统采用了 Windows，2018 操作系统，采用了 Mirosoft Internet Explorer，对系统中某些业务和权限进行测试。

3.1 实验演示系统

搭建实验演示系统，对基于区块链的人力资源大数据安全存储系统的功能进行验证。在演示系统发送端，发送码流数据，并将其传送到信号源的缓存区，即分级复接器。当演示系统接收端接收到码流数据后，经过帧同步提取虚拟信道数据。

3.2 测试用例与结果分析

测试员工列表服务的用例，如图 4 所示。

编号：TC1S001	类型：Web 服务	用例编号：EMP-001
测试目的：有权限的员工才能查看员工表单		
前提条件： 1）用户正确输入地址，进入员工信息服务界面 2）用户能够正确登录		
步骤	输入数据	信息描述
1	* * *	用户点击雇佣清单方法
2	* * *	点击调用按钮

图 4 测试用例 1 演示图

由图 4 可知，对于有权限的员工，系统会返回一个包含 XML 文档的员工表单；对没有权限的员工，系统会返回一个错误的网页。由此也说明网络服务是正确的，系统能够根据用户权限确定是否返回员工表单，返回的员工表格都是等级相同或低于等级的员工表单。

测试一个认可空缺申请的用例，如图 5 所示。

编号：TC2S002	类型：Web 服务	用例编号：EMP-003
测试目的：人事经理对提交的空缺职位申请给予同意		
前提条件： 1）已经有空缺职位，并提交申请 2）用户能够正确输入地址信息，并进入 Web 服务界面		
步骤	输入数据	信息描述
1	* * *	批准空缺申请
2	ID * *	输入空缺职位编号

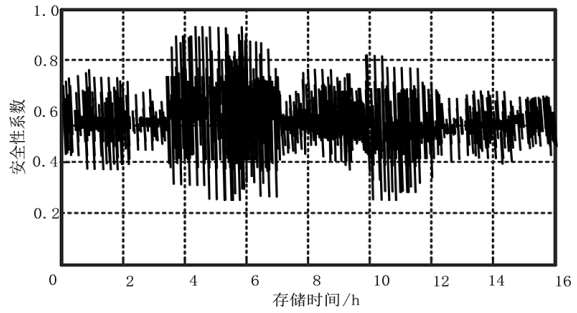
图 5 测试用例 2 演示图

由图 5 可知，在人力资源管理系统中，从菜单中“求职”到“Uacancyapplication”，可找到从“wait”变为

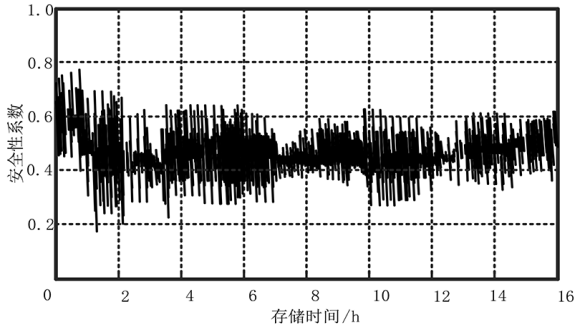
“approve”的申请。由此也说明 Web 服务正确,系统能够根据用户角色决定网络服务可用性。

3.3 存储安全性系数对比分析

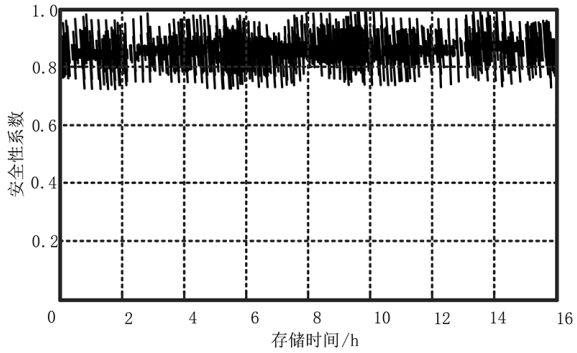
分别使用基于 SAN 架构的数据存储系统、基于 Kubernetes 的数据存储系统和基于区块链的数据存储系统,对比分析数据存储安全性系数,对比结果如图 6 所示。



(a) 基于 SAN 架构的数据存储系统



(b) 基于 Kubernetes 的数据存储系统



(c) 基于区块链的数据存储系统

图 6 三种系统数据存储安全性系数对比分析

由图 6 可知,使用基于 SAN 架构的数据存储系统,数据存储安全性系数忽高忽低,最高为 0.93,最低为 0.26;使用基于 Kubernetes 的数据存储系统,数据存储安全性一直处于较低状态,安全性系数最高为 0.77,最低为 0.17;使用基于区块链的数据存储系统,数据存储安全性一直处于较高状态,安全性系数最高为 0.99,最低为 0.76。

4 结束语

针对人力资源大数据存在安全风险的问题,提出基于区块链的人力资源大数据安全存储系统,通过区块链技术能够辅助网络主机对用户信息进行安全加密处理。由于采用监控模块和驱动模块等硬件结构,使数据的加密和编程操作变得简单。验证分析可知,本文系统的数据存储安全性系数达到了 0.99,分别高出对比系统 0.06 和 0.22,最低安全系数比文献系统分别高出 0.50 和 0.59,由此可知,该系统有效提高了人力资源系统的安全性,并且系统可以从菜单中“求职”到“Uacancyapplication”,找到从“wait”变为“approve”的申请,其能够根据用户角色决定网络服务可用性,因此,该系统具备可行性和有效性。

参考文献

[1] 余克南. 大数据背景下计算机隐私信息安全研究[J]. 信息与电脑, 2025, 37(15):87-89.

[2] 徐艳艳. 大数据背景下网络空间安全防御的研究应用[J]. 中国宽带, 2025, 21(10):55-57.

[3] 李磊, 周正, 陈家璘, 等. 基于云计算的电力智能信息数据网架构研究[J]. 自动化技术与应用, 2024, 43(6):176-180.

[4] 谭靓洁, 李永飞, 吴琼. 基于区块链的煤矿安监云数据安全访问模型研究[J]. 工矿自动化, 2022, 48(5):93-99.

[5] 宫永红, 孙苗苗. 基于区块链技术的人力资源大数据加密方法研究[J]. 自动化技术与应用, 2024, 43(7):125-128.

[6] 秦榕霞, 苏俊琦, 韦萌萌. 基于区块链技术的分布式数据安全存储方案[J]. 信息记录材料, 2025, 26(7):161-163.

[7] 张照明. 基于云计算的分布式数据安全存储方法[J]. 信息记录材料, 2023, 24(3):227- 229.

[8] 张利华, 曹宇, 张赣哲, 等. 基于区块链的微电网数据安全存储与删除验证方案[J]. 计算机工程与设计, 2023, 44(4):967-976.

[9] 刘超, 梁雪青, 袁兴佳, 等. 基于 IPFS 和区块链技术的可信数据安全存储和共享系统[J]. 微型电脑应用, 2024, 40(10):143-147.

[10] 吴元杰. 基于大数据的网络数据安全存储检索系统的设计[J]. 软件, 2024, 45(5): 95-97.

[11] 刘超, 梁雪青, 袁兴佳, 等. 基于 IPFS 和区块链技术的可信数据安全存储和共享系统[J]. 微型电脑应用, 2024, 40(10):143-147.

[12] 高志琨, 孙琴, 张海超. 基于双层分片区块链的信息安全动态防护方法[J]. 电子设计工程, 2025,33(14):94-97.

[13] 张维俊. 基于对称密钥加密算法的无线网络通信数据安全传输方法[J]. 通信电源技术, 2024, 41(8):173-175.

[14] 王永军, 王金帅, 王辉, 等. 基于变分自编码器和差分隐私的轨迹数据发布方案[J]. 小型微型计算机系统, 2024, 45(9): 2261-2268.

[15] 于运涛, 张大松, 姜洪朝, 等. 基于区块链的网络安全系统关键数据存储处理系统设计[J]. 电子技术应用, 2023, 49(4):78-82.

作者简介:张 露(1970—),女,硕士,高级讲师,工程师,研究方向:党建研究、干部培训。

(上接第 39 页)

[8] 高萌,吕向群,谢俊磊,等. 基于 GO 法和 Bayes 的制导弹药控制系统可靠性评估[J]. 兵工自动化,2021,40(1):60-62.

[9] 唐莉,程世娟,张晓洁,等. 多源异构数据贝叶斯变权融合可靠性评估模型[J]. 重庆理工大学学报(自然科学),2023, 37(2):272-277.

[10] 韦金芬,宋保维,毛昭勇. 多阶段实验数据融合的 Bayes 可靠性评定模型[J]. 计算机工程,2012,38(9):265-267.

作者简介:苏筱婷(1996—),女,硕士,工程师,研究方向:光学目标仿真技术。