DOI:10.20033/j.1003-7241.(2026)06-0159-05

基于 RSA 加密算法的企业创新共享互动平台设计

齐景锋, 崔　含, 贾小波, 陈　晨, 李　沛
(陕西陕煤榆北煤业有限公司 榆林信息化运维分公司, 陕西 榆林 719000)

摘　要:随着企业发展体系的完善,企业管理所使用的技术手段也越来越多。企业共享平台可作为信息载体为企业内部提供高效、安全的信息交互服务。但现有平台普遍存在加密强度不足,数据共享机制僵化问题。为了改善企业内部交流的便捷性并解决当前共享平台问题,研究设计了一种企业创新共享互动平台。过程中利用两个随机选取的素数构建欧拉函数,结合高级加密标准算法构建混合加密机制,采用 Miller-Rabin 素数判定算法进行素数整数验证,引入 MapReduce 对数据加密功能模块进行优化。实验结果表明,研究方法在加密效率测试中,当文件大小为 6.0 GB 时的加密耗时为 271 s;在不合理创新共享互动行为拦截成功率分析中,研究方法在移动端中文件大小为 100 MB 时的拦截成功率为 97.7%。说明研究方法具有良好的企业创新共享互动平台运行安全保障能力。研究成果可支撑企业数字化转型中对数据安全与协同效率的双重需求。

关键词:平台设计;MapReduce;Rivest-Shamir-Adleman;加密;共享;创新
中图分类号: TN915.08-34　　**文献标志码**: A　　**文章编号**: 1003-7241(2026)06-0159-05

Design of enterprise innovation sharing interactive platform based on RSA encryption algorithm

Qi Jingfeng, Cui Han, Jia Xiaobo, Chen Chen, Li Pei
(Department of Integrated Management Yulin Information Operation and Maintenance Branch of SHCCIG Yubei Coal Industry Co., Ltd., Yulin 719000, Shaanxi, China)

Abstract: As the enterprise development system becomes more complete, the technical means used in enterprise management also increase. The enterprise sharing platform can serve the internal information of the enterprise as an information carrier, providing efficient and secure information interaction services. However, the existing platforms generally have problems such as insufficient encryption strength and rigid data sharing mechanism. In order to improve the convenience of internal communication within the enterprise and solve the current problems of the sharing platform, a research and design of an enterprise innovative sharing interaction platform is carried out. During the process, an Euler function is constructed using two randomly selected prime numbers, a hybrid encryption mechanism is built by combining the advanced encryption standard algorithm, the Miller-Rabin prime number determination algorithm is used for prime number integer verification, and MapReduce is introduced to optimize the data encryption function module. The experimental results show that in the encryption efficiency test, when the file size is 6.0 GB, the encryption time is 271 s; in the analysis of the interception success rate of unreasonable innovative sharing interaction behaviors, the research method has an interception success rate of 97.7% on the mobile end when the file size is 100 MB. This indicates that the research method has a good security guarantee capability for the operation of the enterprise innovative sharing interaction platform. The research results can support the dual needs of data security and collaborative efficiency in the digital transformation of enterprises.

Keywords: platform design; mapreduce; rivest shamir adleman; encryption; share; innovation

在全球化和信息化的大潮中,企业之间的竞争愈发激烈。企业要想在竞争中立于不败之地,就必须不断创新,提高自身的技术水平和服务质量。然而,创新需要企业不断地学习新知识、掌握新技术、开发新产品,要求企业必须建立一个有效的知识共享和创新互动机制,以便员工之间能够方便地交流思想、分享经验、协作解决问题[1-2]。随着互联网的普及和大数据时代的到来,企业数据的规模和复杂性日益增长,数据安全和隐私保护成为全球关注的焦点。企业不仅要面对内部数据管理的挑战,还要应对来自外部的网络安全威胁。为了保障企业内部网络平台的安全性,传统的解决方案主要依赖于防火墙、入侵检测系统等安全设备。然而随着网络攻击手段的不断升级,这些传统的安全措施已经难以应对复杂的网络安全威胁。数据加密是一种常用的网络安全保护手段。邹益民等[3]结合

收稿日期:2024-10-08;**录用日期**:2024-12-12
基金项目:陕西省煤业科学技术研究项目(2023SMHKJ-B-J-70)
作者简介:齐景锋(1985—)男,高级工程师,研究方向:机电研究、信息化系统建设与维护工作、科研项目建设与管理等。
引用本文:齐景锋, 崔含, 贾小波, 等. 基于 RSA 加密算法的企业创新共享互动平台设计[J]. 自动化技术与应用, 2026,45(6):159-163. (Qi Jingfeng, Cui Han, Jia Xiaobo, et al. Design of enterprise innovation sharing interactive platform based on RSA encryption algorithm[J]. Techniques of Automation and Applications, 2026,45(6):159-163.)

国密算法设计了一种数据加密传输技术,利用双向身份认证进行数据身份关联,结果显示所提方法具有良好的数据保护效果。Verma 等[4]利用区块链技术和基于属性加密的手段构建了一种安全文档共享模型,使用星际文件系统进行数据加密存储,结果说明所提方法能够有效避开网络攻击。里韦斯特-沙米尔-阿德尔曼算法(Rivest-Shamir-Adleman, RSA)作为一种非对称加密算法,因其安全性高、密钥管理简单而被广泛应用于数据加密和数字签名[5]。在这样的背景下,研究尝试创新性地基于 RSA 技术进行平台加密技术设计,并提出对应的企业创新共享互动平台架构,以期为企业管理提供一定技术参考。

1 创新共享互动平台设计

1.1 RSA 平台加密技术设计

企业创新共享互动平台在设计时,需要整合各种社会资源并建立有效的共享机制,还需要确保信息的透明度和对称性,同时保障数据的安全性和隐私性[6-7]。RSA 算法基于大质数因数分解的困难性,提供了一种安全可靠的数据传输方式[8-9]。研究使用 RSA 算法进行企业创新共享互动平台的加密技术设计。RSA 使用一对公钥和私钥,公钥用于加密,私钥用于解密,适合在不安全的通信环境中建立安全的通信会话。RSA 加密算法在执行时,需要利用两个随机选取的素数构建欧拉函数,如式(1)所示。

$$\varphi(n) = (P - 1) \times (Q - 1) \tag{1}$$

式中,$\varphi(n)$ 代表欧拉函数;P、Q 代表被随机选取的不相等的两个大素数。加密密钥和解密密钥的关系如式(2)所示。

$$D \times E \bmod(\varphi(n)) = 1 \tag{2}$$

式中,D 代表解密密钥;E 代表作为加密密钥的正整数。由两个大素数相乘计算得到公开的数 N,并将作为加密密钥的正整数和公开的数相组合作为用于加密的公钥,将解密密钥和公开的数相组合作为用于解密的私钥。在企业创新共享互动平台的构建中,确保数据的安全性和加密效率是至关重要的。针对大文件的加密需求,单一的加密算法可能无法满足所有要求。RSA 算法以其高安全度而著称,主要得益于其非对称加密特性。然而 RSA 算法在处理大文件时面临性能瓶颈,因为它涉及的模幂运算对于大尺寸数据来说效率较低[10-11]。高级加密标准算法作为一种对称加密算法,具有快速的加密速度和较低的计算资源消耗,适合于对大容量数据进行加密[12-13]。研究构建一种混合 RSA 算法和高级加密标准算法的混合加密机制,使用 RSA 算法加密高级加密标准算法的密钥,然后将该密钥用于加密实际的大文件数据。为了提升平台加密的效率,研究从随机大素数的生成过程出发,通过 Java 语言提供的并行流技术,创建一个包含从 3 到 60 之间所有小素数的列表,记为集合 A。紧接着,从集合 A 中随机挑选出 27 个素数,形成一个新的集合 B,该集合专用于在搜索素数过程中,当遇到非素数时,作为候选的增量元素。研究采用 Miller-Rabin 素数判定算法进行素数整数验证。大素数生成过程如图 1 所示。

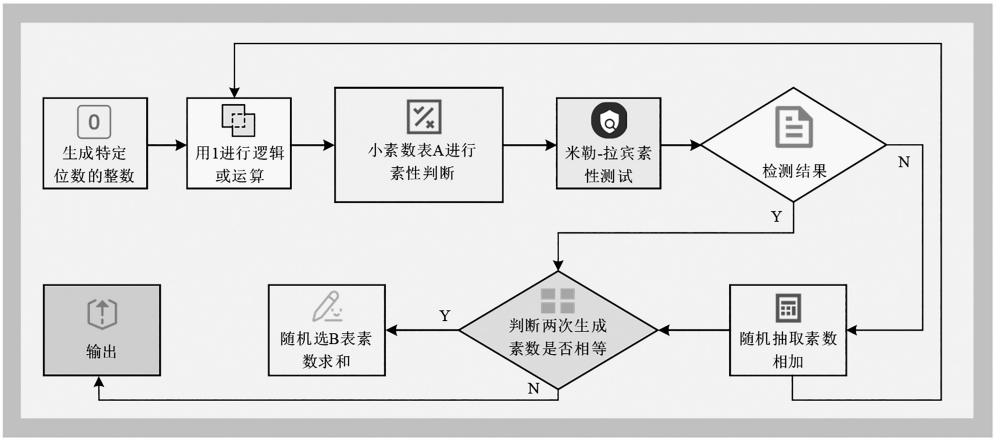


图 1 大素数生成过程

Fig. 1 Process of generating large prime numbers

由图 1 可见,大素数在生成时,首先对大素数位数进行确定,再对整数执行按位或操作,特别是与数字 1 进行按位或操作。确保进行素数判断时所输入的数都为奇数整数。对小素数表进行遍历,并进行取余运算,得到余数非零的数与素数表中的随机数进行相加并再次判断是否是奇数。再将完成验证的整数利用 Miller-Rabin 素数判定算法进行指定轮数验证,通过验证后即视为获得一个大素数。对第二个素数进行生成时避免生成与第一个素数相同的数。使用 RSA 算法生成的公钥对高级加密标准密钥进行加密,以确保其安全性。当用户需要解密文件时,首先利用自己的 RSA 私钥对存储的被加密高级加密标准密钥进行解密,以恢复原始的高级加密标准密钥。最后使用解密得到的高级加密标准密钥对密文进行解密操作,从而获得原始的明文文件。密文和明文的关系如式(3)所示。

$$C = M^e \bmod n \tag{3}$$

式中,C 代表加密后的密文;M 代表明文;e 代表整数公钥;n 代表幂。

1.2 数据加密功能模块设计

在 RSA 平台加密技术的基础上,研究设计企业创新共享互动平台的数据加密功能模块。研究设计数据加密功能

模块包含数据拦截、数据加密、数据解密、数据密匙 4 个主要功能区域。数据加密功能模块运行过程如图 2 所示。

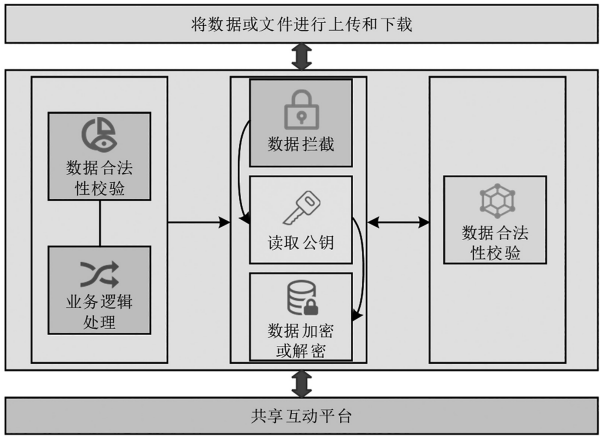


图 2　数据加密功能模块运行过程

Fig. 2　The operation process of the data encryption function module

由图 2 可见,数据加密功能模块在运行时,在共享互动平台的数据管理流程中,数据拦截主要功能是在数据被存储到分布式存储系统之前对其进行安全处理。在数据存储之前,数据拦截模块介入,确保数据在进入存储系统前经过安全检查[14-15]。数据拦截模块与数据加密模块协作,对拦截的数据执行加密操作,生成不可读的数据密文。数据加密、数据解密承担着保护数据安全的重要职责,系统通过数据密钥模块,依据特定的密钥生成算法来创建一个用于加密的密钥。当数据需要被存储时,数据加密模块利用生成的密钥对数据执行加密操作,确保数据在存储介质上是以密文形式存在,从而提高数据的安全性。为了提升企业创新共享互动平台的分布式计算能力,研究引入 MapReduce 对数据加密功能模块进行优化。分片操作的分片大小计算如式(4)所示。

$$s_j=\begin{cases}\left\lceil\left(\dfrac{\text{Length}}{2^{17}}\right)\right\rceil\times 2^{17}\\ \text{Length}-(\text{size}-1)\times\left\lceil\left(\dfrac{\text{Length}}{2^{17}}\right)\right\rceil\times 2^{17}\end{cases}\tag{4}$$

式中,s_j 代表分片大小;Length 代表约定文件长度;size 代表系统定义分片大小。为了提升企业创新共享互动平台的安全性,研究向平台中加入安全访问功能,利用接口权限注册模块、请求拦截验证模块、管理员权限模块实现对访问的安全性控制。当系统部署到服务器并启动后,接口权限注册模块将首先被执行,由接口扫描模块自动扫描系统中所有定义的接口。注册后的接口信息,包括接口的唯一标识和访问路径,将被存储至 Redis 缓存中。管理员权限模块用于规范管理员的行为,明确限定了管理员可执行的操作范围,防止其滥用权限。研究构建企业创新共享互动平台存储架构如图 3 所示。

由图 3 可见,企业创新共享互动平台储存架构主要包含了视图层、控制层、系统接口层和共享互动平台层。视图层作为用户与系统交互的前端界面,不仅是用户进行各种操作的起始点,也是用户与系统之间沟通的桥梁。视图层提供了用户与系统直接交互的界面,用户通过视图层上提供的界面元素进行操作。控制层在软件架构中扮演着枢纽的角色,主要负责协调视图层与后台系统之间的交互。当来自视图层的用户请求到达后台系统时,控制层首先对其进行拦截,确保所有的请求都通过这一入口进行管理。控制层内置的拦截器链对拦截到的请求进行预处理,根据路由的结果,定位并调用系统接口层中的具体方法,处理用户的请求。系统接口层作为控制层与云平台层之间的中间件,负责将云平台层的服务和功能以接口的形式提供给控制层。系统接口层将云平台层提供的各种功能进行组织和封装,创建出易于控制层调用的接口。通过标准化的接口,其他系统或第三方平台能够直接与系统接口层交互,实现集成和扩展。共享互动平台层包含基础设施层、业务逻辑层和数据层,实现数据存储、分布式计算。以储存架构为核心,搭建企业创新共享互动平台,确保企业创新共享互动活动的安全性和灵活性。

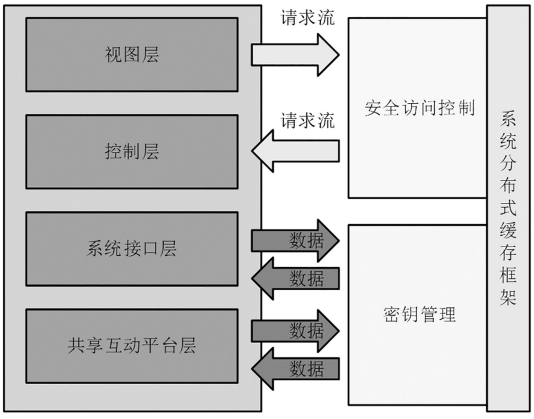


图 3　企业创新共享互动平台存储架构

Fig. 3　Storage architecture of the enterprise innovation sharing interaction platform

2　平台有效性分析

为了对研究设计的企业创新共享互动平台在实际运行中的有效性和应用效果进行分析,研究在 Intel Xeon E2144G 处理器平台上进行有效性分析。将研究方法简称为 RSA 加密法,与高级加密标准算法、平行混合算法进行对比。对方法的加密效率进行测试,如图 4 所示。

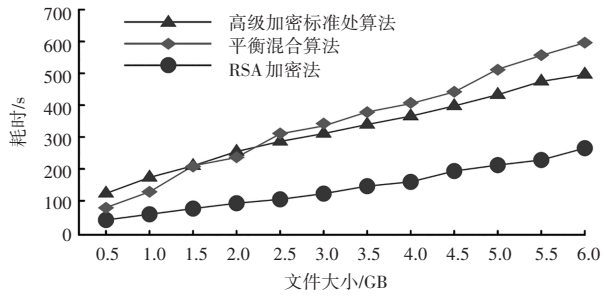


图 4　加密效率测试

Fig. 4　Encryption efficiency test

由图 4 可见,不同方法在进行加密时的耗时都随着文

件增大而上升。高级加密标准算法在运行时,当文件大小为 0.5 GB 时的加密耗时为 122 s;当文件大小为 3.0 GB 时的加密耗时为 30 s;当文件大小为 6.0 GB 时的加密耗时为 497 s。平行混合算法在运行时,当文件大小为 0.5 GB 时的加密耗时为 82 s;当文件大小为 3.0 GB 时的加密耗时为 343 s;当文件大小为 6.0 GB 时的加密耗时为 598 s。RSA 加密法在运行时,当文件大小为 0.5 GB 时的加密耗时为 42 s;当文件大小为 3.0 GB 时的加密耗时为 124 s;当文件大小为 6.0 GB 时的加密耗时为 271 s。说明研究方法在进行加密时的耗时更少,且研究方法在所加密文件大小增大时的耗时增加量也更少。对研究方法的不合理创新共享互动行为拦截成功率进行测试,如图 5 所示。

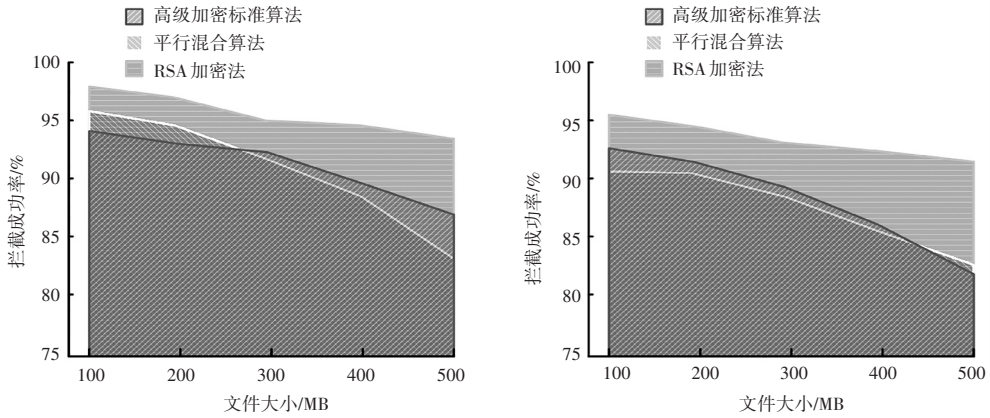
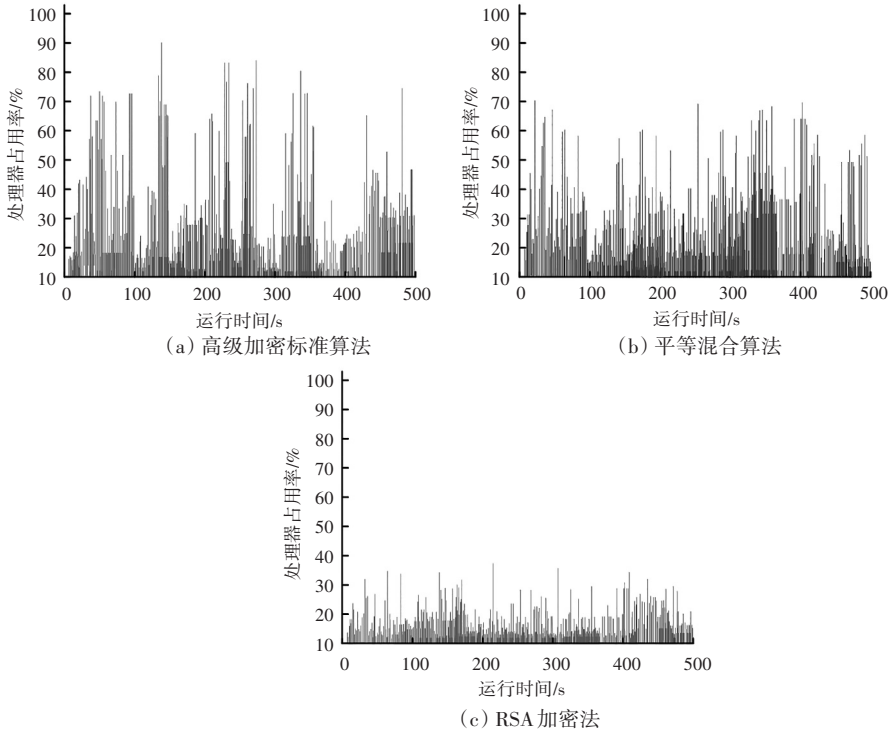


图 5 不合理创新共享互动行为拦截成功率

Fig. 5 Success rate of intercepting unreasonable innovation sharing interaction behaviors

由图 5 可见,不同方法的不合理创新共享互动行为拦截成功率都随着文件增大而下降。图 5(a)显示,在移动端中,高级加密标准算法在文件大小为 100 MB 时的拦截成功率为 94.3%;在文件大小为 500 MB 时的拦截成功率为 86.7%。平行混合算法在文件大小为 500 MB 时的拦截成功率为 82.8%。RSA 加密法在文件大小为 100 MB 时的拦截成功率为 97.7%;在文件大小为 500 MB 时的拦截成功率为 93.5%。图 5(b)显示,在网页中,高级加密标准算法在文件大小为 100 MB 时的拦截成功率为 92.6%;在文件大小为 500 MB 时的拦截成功率为 81.7%。平行混合算法在文件大小为 100 MB 时的拦截成功率为 90.5%;在文件大小为 500 MB 时的拦截成功率为 82.6%。RSA 加密法在文件大小为 100 MB 时的拦截成功率为 95.4%;在文件大小为 500 MB 时的拦截成功率为 91.3%。说明研究设计的企业创新共享互动平台能够保证更安全地在线互动,为企业创新共享互动提供更高的交流质量。对研究方法运行时造成的硬件负担进行分析,如图 6 所示。



(a) 高级加密标准算法 (b) 平等混合算法

(c) RSA 加密法

图 6 硬件负担分析

Fig. 6 Hardware burden analysis

由图 6 可见,不同方法在运行时对于硬件造成的负担状况不同。图 6(a)显示,高级加密标准算法在为期 500 s 的运行中,最高处理器占用率达到 89%。期间有 5%的计算处理器占用率达到 70%以上,有 40%的计算处理器占用率达到 30%以上,90%的计算处理器占用率达到 15%以上。图 6(b)可见,平行混合算法在为期 500 s 的运行中,最高处理器占用率达到 71%。期间有 5%的计算处理器占用率达到 50%以上,有 30%的计算处理器占用率达到 30%以上,95%的计算处理器占用率达到 15%以上。由图 6(c)可见,RSA 加密法在为期 500 s 的运行中,最高处理器占用率达到 39%。期间有 5%的计算处理器占用率达到 25%以上,有 10%的计算处理器占用率达到 20%以上,95%的计算处理器占用率达到 12%以上。说明研究方法在运行时对于硬件设备的性能需求更低,具有更好的适用性。

3 结论

研究设计了一种基于 RSA 技术的企业创新共享互动平台,以实现更轻松的企业内部学习。过程中使用 RSA 算法进行企业创新共享互动平台的加密技术设计,使用 RSA 算法加密高级加密标准算法的密钥,对第二个素数进行生成时避免生成与第一个素数相同的数,利用自己的 RSA 私钥对存储的加密高级加密标准密钥进行解密,明确限定了管理员可执行的操作范围,搭建了企业创新共享互动平台储存架构。实验结果表明,研究方法在加密效率测试中,当文件大小为 0.5 GB 时的加密耗时为 42 s;在进行不合理创新共享互动行为拦截成功率分析时,在网页中当文件大小为 500 MB 时的拦截成功率为 91.3%;进行硬件负担分析时,研究方法在运行期间仅有 5%的计算处理器占用率达到 25%以上。说明研究方法能够有效实现平台安全保护,能够更好地保障企业创新共享互动顺利进行。但研究未考虑特定网络攻击造成的系统风险,后续将结合特定网络攻击进行研究,以改善方法并扩大适用范围。

参考文献

[1]宋涛, 李秀华, 李辉, 等. 大数据时代下车联网安全加密认证技术研究综述[J]. 计算机科学, 2022, 49(4):340-353.
[2]高丽萍, 季仕承, 郝玉忠. 基于云端辅助的国ˆ土资源数字化档案信息自动加密方法[J]. 自动化技术与应用, 2024, 43(2):85- 88.
[3]邹益民, 庞瑞卿, 冯汝康. 基于国密算法与移动 CA 的移动办公平台数据安全体系研究[J]. 内蒙古大学学报(自然科学版), 2022, 53(3):325-329.
[4]Verma G, Kanrar S. Secure document sharing model based on blockchain technology and attribute-based encryption[J]. Multimedia Tools and Applications, 2024, 83(6): 16377-16394.
[5]庞宇, 魏东, 王俊超. 基于混沌浮点运算的医学图像加密方法与 FPGA 实现[J]. 电子技术应用, 2023, 49(1):135-140.
[6]刘嵩, 张建强, 邱达, 等. 一种三阶分段线性混沌系统及其在图像加密中的应用[J]. 华中师范大学学报:自然科学版, 2023, 57(2):213-222.
[7]牛淑芬, 戈鹏, 宋蜜, 等. 移动社交网络中基于属性加密的隐私保护方案[J]. 电子与信息学报, 2023, 45(3):847-855.
[8]王新, 冯英, 杜炜, 等. 互联网传输中医院就诊数据安全加密方法研究[J]. 自动化技术与应用, 2024, 43(6):74-77.
[9]任永珍. 基于物联网技术的饲料企业供应链信息服务平台构建[J]. 饲料研究, 2022, 45(6):131-134.
[10]郭海洲, 褚全红, 龚思扬, 等. 基于区块链技术的柴油机电控系统数据共享平台研究[J]. 现代电子技术, 2022, 45(19):173-177.
[11]王浩田, 鄂海红, 王勇, 等. 一种云原生数据智能服务生产平台设计与实现[J]. 计算机技术与发展, 2023, 33(10):15-21.
[12]王瑞萍, 鲍喜, 张海超, 等. 人工智能审计流程的设计及平台构建[J]. 微型电脑应用, 2022, 38(1):62-65.
[13]曹萌, 余孙婕, 曾辉, 等. 基于区块链的医疗数据分级访问控制与共享系统[J]. 计算机应用, 2023, 43(5):1518-1526.
[14]Wang W, Sun J, Wang G, et al. Fisher-Yates scrambling algorithm combined with S-box color image encryption technology based on 3D-SCCM chaotic system[J]. Multimedia Tools and Applications, 2023, 82(29): 45233-45258.
[15]张志勇, 宋斌, 梁腾翔, 等. 基于纵向联邦学习的社交网络跨平台恶意用户检测方法[J]. 小型微型计算机系统, 2022, 43(7):1541-1546.

(上接第 153 页)

[2]翟社平, 白喜芳, 童彤. 基于区块链的电子病历共享模型研究[J]. 小型微型计算机系统, 2023, 44(12):2765-2772.
[3]张建伟, 刘瑾, 杨海马, 等. 基于多特征信息融合自注意机制的中文命名实体识别方法[J]. 武汉大学学报(理学版), 2024, 70(3):281-292.
[4]雷松泽, 刘博, 王瑜菲, 等. 结合多特征嵌入和多网络融合的中文医疗命名实体识别[J]. 电子与信息学报, 2023, 45(8):3032-3039.
[5]王玉珏. 基于对抗神经网络的医院科研数据混合加密系统设计[J]. 自动化技术与应用, 2023, 42(10):85-87.
[6]Fugkeaw S, Wirz L, Hak L. Secure and lightweight blockchain-enabled access control for fog-assisted iot cloud based electronic medical records sharing[J]. IEEE Access, 2023, 40(11):62998-63012.
[7]张智源, 孙水华, 徐诗傲, 等. 基于 BERT 和多窗口门控 CNN 的电机领域命名实体识别[J]. 计算机应用研究, 2023, 40(1):107-114.
[8]Munjal K, Bhatia R. A systematic review of homomorphic encryption and its contributions in healthcare industry[J]. Complex&Intelligent Systems, 2023, 9(4): 3759-3786.
[9]叶靖祺, 时玉梅, 邵蓉珺. 区块链技术支持下的医院财务数据交换系统安全性技术研究[J]. 自动化技术与应用, 2025, 44(9):143-148.
[10]李子彬, 王理丽, 王子乐, 等. 基于多元感知信息融合的电抗器故障声纹诊断研究[J]. 环境技术, 2024(2):121-126.
[11]张小艳, 段正宇. 基于句级别 GAN 的跨语言零资源命名实体识别模型[J]. 计算机应用, 2023, 43(8):2406-2411.
[12]陈娜, 孙艳秋, 燕燕. 结合注意力机制的 BERT-BiGRU-CRF 中文电子病历命名实体识别[J]. 小型微型计算机系统, 2023, 44(8):1680-1685.
[13]翟社平, 白喜芳, 童彤. 基于区块链的电子病历共享模型研究[J]. 小型微型计算机系统, 2023, 44(12):2765-2772.
[14]朱西平, 赖宇, 龙文涛, 等. 基于区块链的电子病历共享与可验证方案[J]. 科学技术与工程, 2023, 23(14):6113-6122.
[15]巫朝霞, 唐靖蕾, 苗志伟. 云环境下支持多授权机构的医疗数据安全共享方案[J]. 计算机应用研究, 2023, 40(12):3800-3804.