 DOI: https://doi.org/10.12349/iser.v7i6.10799

Utilizing the Information Technology Environment to Enhance the Security of Digital Publishing

Xiao Liu

Information Technology Department of Dazhong Newspaper Group, Jinan, Shandong, 250014, China

Abstract

In the context of the comprehensive promotion of digital transformation, the digital publishing industry exhibits a development trend characterized by diverse content forms, extensive dissemination channels, and continuous growth in user scale. At the same time, it faces security risks such as data leakage, illegal access, and malicious attacks. The informatization and innovation industry, supported by core technologies such as self-controlled chips, operating systems, databases, and middleware, provides key technical paths and underlying guarantees for the construction of digital publishing security systems. Relying on national cryptographic algorithms, identity authentication, data encryption, access control, etc., it can enhance the security protection level of digital publishing in terms of copyright protection, content transmission, identity authentication, system operation, and data storage. In practice, the integration of informatization and innovation with digital publishing still faces practical challenges such as technical adaptation, security iteration, ecosystem improvement, and architecture design. In the future, it is necessary to strengthen technological research and development, improve standards and norms, enhance security awareness, and build an independent and controllable, safe and efficient digital publishing security system to promote the high-quality development of the industry.

Keywords

information innovation environment; digital publishing; security architecture; national cryptographic algorithm; identity authentication; data security

利用信创环境提高数字出版安全性

刘潇

大众报业集团信息技术部，中国 · 山东 济南 250014

摘　要

在数字化转型全面推进的背景下，数字出版产业呈现内容形态多元、传播渠道广泛、用户规模持续增长的发展态势，同时面临数据泄露、非法访问、恶意攻击等安全风险。信创产业以自主可控芯片、操作系统、数据库、中间件等核心技术为支撑，为数字出版安全体系建设提供关键技术路径与底层保障。依托国密算法、身份认证、数据加密、访问控制等安全能力，可从版权保护、内容传输、身份认证、系统运行、数据存储等维度提升数字出版安全防护水平。实践中，信创与数字出版融合仍面临技术适配、安全迭代、生态完善、架构设计等现实挑战。未来需强化技术研发、健全标准规范、提升安全意识，构建自主可控、安全高效的数字出版安全体系，推动行业高质量发展。

关键词

信创环境；数字出版；安全架构；国密算法；身份认证；数据安全

1 引言

当前，数字技术深度融入文化生产、传播与消费全流程，数字出版向智能化、融合化、场景化加速演进，内容呈现从单一文字拓展至图文、音视频、融媒体等多元形态，传播覆盖客户端、网站、小程序、新媒体平台等全渠道。数字阅读、有声出版、知识付费、在线资讯等业态快速普及，成为文化产业高质量发展的重要引擎。与此同时，数字出版数据体量持续扩大、业务链路不断延伸，安全风险随之凸显，用户隐私泄露、版权内容窃取、越权操作、系统入侵、DDoS 攻击等事件频发，对平台稳定运行、内容版权保护、用户权益保障及行业公信力构成严重威胁。

信创产业作为国家信息技术自主创新的核心支撑，在核心软硬件突破、生态体系完善、安全能力升级等方面取得显著进展，为解决数字出版安全痛点提供国产化解决方案。本文立足信创环境技术特征与数字出版安全需求，分析信创技术在数据加密、传输安全、身份认证、系统防护、数据管理等场景的应用价值，梳理实践中的关键挑战，提出优化路径，为数字出版安全体系建设提供参考。

【作者简介】刘潇（1980–），女，回族，中国山东济南人，本科，初级，从事媒体融合、信息技术研究。

2 数字出版安全核心需求与风险挑战

数字出版以数字内容生产、加工、存储、分发、运营为核心，涉及用户数据、版权内容、业务数据、支付信息等敏感资源，其安全需求贯穿全业务链条，主要体现在数据安全、访问安全、系统安全、版权安全四个维度，当前面临的风险集中表现为以下方面。

2.1 数据泄露风险突出

数字出版平台沉淀了海量的用户身份标识信息、个性化阅读行为轨迹、交易付费记录，以及平台自身的原创版权内容资产，这些敏感数据的商业价值很高，一直是网络攻击者和数据黑产的重点瞄准对象。

从内部来看，部分企业的人员权限管控存在疏漏，操作流程不够规范，甚至存在违规导出数据的情况；从外部来看，黑客的钓鱼入侵、木马植入、系统漏洞利用等恶意行为层出不穷，这些问题都有可能引发大规模的数据泄露事件，不光会侵害用户的个人隐私，更会直接威胁到企业的核心资产安全。

2.2 非法访问与越权操作频发

过去很长一段时间里，许多平台都只用单一的账号密码做登录认证，这个模式的短板现在看来太明显了。密码设简单了很容易被暴力猜解，设复杂了用户记不住，而且不少用户习惯一个密码用到底，很容易被撞库攻击 —— 就是把别的平台泄露的密码拿来试，一撞一个准，还有的用户不小心就把登录凭证给泄露了，这些都会破坏业务流程，进而影响平台的正常运行。

2.3 网络攻击与系统故障频发

从近年的行业实践来看，网络威胁的迭代速度正在持续加快，各类新型攻击手段层出不穷，DDoS、CC 这类资源型攻击，还有 SQL 注入、网页篡改这类应用层攻击，复杂度都在不断提升。尤其是在重大新闻发布、热点事件报道的关键节点，这类攻击的频率明显上升，前几年行业内就出现过相关案例：一次 DDoS 攻击通过大量虚假请求挤占服务器带宽与计算资源，导致平台服务中断了近 4 小时，直接影响了重大新闻的正常推送。此外，部分沿用国外软硬件架构的平台，还面临漏洞响应不及时的问题，最终导致系统的运行稳定性缺乏保障。

2.4 版权保护与内容管控难度大

数字内容不像实体产品那样有形，复制成本低，能在各类平台间迅速传播，而且修改后几乎不留痕迹。正因如此，行业内盗版、未经许可的转载、恶意篡改原创内容等现象反复出现，一直难以根除。

以上风险不利于数字出版行业健康持续发展，要构建自主可控、防护全面、响应及时的安全出版体系，这也是行业的必然选择。

3 信创环境对数字出版安全的支撑作用

在信创环境下，核心技术都是自主可控的。从芯片、操作系统，到数据库、中间件，再到安全组件，整个链条已经换成国产方案。这样一来，不管是底层的硬件还是上层的应用，都能形成闭环的安全能力，可以满足数字出版中各种安全方面的要求。从实际落地情况看，这套体系确实给数字出版安全带来了比较全面的提升。

3.1 基于国密算法的底层安全加固

先说安全底层。一个关键做法是用国密算法替换掉原先的国外加密算法。国密算法不仅自己可控、安全性高，也完全符合合规要求。它能覆盖数据加密、数字签名、身份鉴别、完整性校验等几乎所有核心安全场景。下面具体说三种算法：

SM4 对称加密：采用分组加密方式，加解密速度快，安全性也不错。实际使用中，它能处理大量数字内容——不论是文本、图片还是音视频。在存储和传输过程中用 SM4 加密，可以保证这些资源在整个生命周期里不被窃取或篡改。

SM2 非对称加密：属于公钥密码体制，支持数字签名、密钥交换和身份认证，可以替代传统的 RSA、ECC 算法。用了 SM2，就能对用户身份进行可信验证，操作行为也无法抵赖。像登录认证、版权交易、内容审核这类业务场景，用 SM2 都很合适。

SM3 杂凑算法：生成 256 位固定长度的摘要，抗碰撞能力比 MD5、SHA-1 这些过时算法强得多。它可以用于用户密码的哈希存储，也能做文件完整性校验和数据溯源，防止内容数据被非法修改

3.2 全链路加密保障传播过程的安全

再来看内容传播安全。把国产加密芯片和国密算法整合起来，再对 SSL/TLS 通信协议做一些适配优化，就能搭建端到端的加密传输通道。这样一来，用户终端和服务端之间的通信全程都是加密的。包括版权内容、用户隐私、支付数据这些敏感信息，在传输过程中会得到比较严密的保护，可以有效避免监听、窃取、篡改、劫持等风险。换句话讲，内容分发的安全性就真正变得可控了。

3.3 多因素认证从源头防范访问风险

基于信创技术，可搭建多因素认证体系，融合静态密码、动态口令、短信验证，以及国产生物识别（指纹、人脸）等多种验证手段，构建多层次的身份验证机制。同时可配套异常检测能力，结合登录地点、设备指纹、操作行为等维度，实时拦截可疑登录、自动触发风险预警，配合动态凭证更新，从源头防范账号被盗、越权访问、非法操作的风险。

3.4 国产操作系统提升底层系统安全

原有国外操作系统可替换为国产系统，这类系统基于 Linux 内核深度定制，实际应用中的统信 UOS、麒麟 OS 等

主流产品，具备核心代码可控、安全机制完善、漏洞响应快速等特点。系统内置数据加密、强制访问控制、安全审计、进程防护等原生安全功能，大幅降低恶意入侵、病毒感染、数据泄露的风险。数字出版领域的采编、排版、发布等业务系统，均可迁移至国产操作系统，实现底层运行安全的全面提升。

3.5 用国产数据库保护关键数据的安全存储

在数据库这一层，可以用国产产品替换掉国外数据库。像人大金仓这类国产数据库，在实际项目中已经用起来了。它们自主可控，安全性高，运行也稳定，而且能兼容原有的业务系统。具体来说，支持细粒度的权限控制、数据透明加密，还有操作全程审计，以及自动备份和快速恢复。有了这些能力，可以有效防止 SQL 注入、暴力破解、数据被窃取等风险。这样一来，用户数据、版权内容、业务日志等关键信息，在整个生命周期里都能得到较好的安全保障。

3.6 信创中间件让业务流程更稳定

中间件也可以换成国产的。比如，用 TongWeb 代替原来常用的 Tomcat，给 Web 应用提供稳定又安全的支撑；再比如，在内容发布、消息推送、数据同步等场景中，RocketMQ 能很好地发挥作用，还能保证分布式事务的一致性。这些国产中间件对出版业务适配得不错，能明显提升系统的可靠性和抗风险能力，从而确保数字出版各个环节都能稳定运行。

4 信创背景下数字出版安全的改进思路

4.1 加强技术攻关与适配工作

结合数字出版自身的业务特点，针对国产芯片、操作系统、数据库和中间件，开展具体场景下的适配研发，推动全栈国产化方案的真正落地。同时，统一接口标准和适配规范，减少不同组件之间的集成难度。再通过全流程的兼容性测试和性能调优，进一步提高系统的运行稳定性和安全防护能力。

4.2 打造闭环的安全运营体系

建立一套覆盖漏洞监测、快速修复、威胁预警和应急响应的闭环安全运营机制。通过与国家级威胁情报平台对接，可以有效提升安全事件的处理效率。与此同时，推进安全检测工具、审计平台、防护组件等产品的国产化替换，确保安全能力始终掌握在自己手中。

4.3 完善行业生态和标准体系

推动信创厂商和数字出版企业之间开展深度的产学研合作，一起开发适合出版行业的专用安全工具和解决方案。在此基础上，制定行业层面的信创安全建设标准、评估办法和实施指南，明确技术要求、部署流程和合规条款，引导整个行业朝着规范化方向走。

4.4 优化全局安全架构设计

以零信任安全理念为核心，搭建“身份可信、设备可信、链路可信、应用可信”的四维安全架构。对数据从采集、存储、传输、使用到销毁的整个生命周期，实现全程加密保护。同时，把国密算法、多因素认证、数据脱敏、权限管理、版权溯源、攻击防护等能力整合起来，形成一套覆盖全场景、全链路、全要素的一体化安全防护体系。

4.5 提升人员安全意识与能力

常态化开展信创安全培训、业务操作规范培训以及应急演练，强化从业人员的安全防护意识；同时建立权限分级管理、操作审计、责任追溯的配套制度，从制度层面防范内部安全风险。

5 结语

信创产业与数字出版深度融合，是保障文化数据安全、提升内容传播能力、推动行业高质量发展的战略方向。信创环境从底层技术到上层应用为数字出版提供自主可控、安全高效的支撑体系，有效应对数据泄露、非法访问、恶意攻击、版权侵权等风险。面对技术适配、生态完善、架构设计等挑战，需坚持技术创新、标准引领、生态共建、安全优先，持续优化安全架构、完善防护能力、提升运营水平，构建自主可控、持续演进的数字出版安全体系，为数字文化繁荣发展提供坚实保障。

参考文献

[1] 向宴颉 黄晓芳 向科峰 郑继楠.一种基于国密算法的区块链无证书加密机制[J] 计算机科学 2024,51(08),440-440

[2] 蔡秋霞.基于密码技术的智能制造网络安全保障体系研究[J] 电脑知识与技术 2024,20(24),10-13

[3] 袁颐赖 彩明.运营商级DDoS统一防护系统建设分析[J] 中国新通信 2019,21(14),61-62

[4] 王宏 赵雨昕.无连接场景下基于国密算法的身份认证方法[J] 计算机与现代化 2025(01), 120-126

[5] 刘沛 秦蔚蓉 李帅 闫炎 黄昊.国产操作系统、数据库及安全产品发展情况综述[J] 中国数字医学 2024,19(04) 1-9

[6] 李恒.基于高性能国密算法的数据库透明加密技术研究[J] 中 国新通信2024,26(18),24-28

[7] 杨子叶.中波台安播信息系统数据库国产化替代研究[J] 广播与电视技术2024,51 (11),64-68

[8] 钱褚佳.广播电视国产化软硬件办公系统适配浅析[J] 电视技术 2022,46(10),177-181