数字化背景下档案管理系统信息安全设计研究

陈雅燕

（中山火炬高技术产业开发区制度创新研究中心（档案馆），广东 中山 528400）

摘 要 在信息科技的迅猛浪潮中，档案管理的数字化转型已成为驱动管理效能飞跃、促进资源高效配置、有力捍卫信息完整性的关键路径。然而，数字化进程虽为档案管理带来了前所未有的便捷性，但随之而来的信息安全挑战亦不容忽视，尤其是如何构筑坚不可摧的防护网，以抵御数据泄露、篡改企图及非法侵入等威胁，已成为亟待解决的紧迫课题。本文旨在通过详尽审视当前面临的多维度安全挑战，构建一套既全面又具前瞻性的信息安全策略框架。

关键词 数字化；档案管理；信息安全

中图分类号：G270.7 **文献标志码**：A **文章编号**：2097-3365(2024)10-0031-03

档案作为历史的见证者、文化的传承者以及决策制定的坚实后盾，其安全性的维护对于任何组织的稳固与成长均具有不可估量的价值。随着数字化时代的迅猛发展，纸质档案正逐步迈向电子化的新纪元，这一变革不仅显著提升了档案管理的效率与灵活性，还拓宽了信息获取的边界。然而，伴随而来的是对信息安全前所未有的挑战。黑客的潜伏攻击、敏感数据的意外泄露，以及系统内部的潜在故障等风险，如同暗流涌动，时刻威胁着档案信息的完整性与保密性。因此，构建一个坚不可摧的档案管理系统，确保其信息安全设计达到行业顶尖水平，已成为当前亟待解决的关键课题。

1 数字化档案管理系统概述

数字化档案管理系统是现代信息管理技术的重要成果，旨在实现档案资源的高效整合、安全存储与便捷利用。该系统通过采用先进的数字化扫描、OCR识别、数据库管理及网络传输技术，将传统纸质档案转化为电子格式，构建起结构化的数字档案库。此举不仅极大地节省了物理存储空间，还显著提升了档案检索速度与准确性，满足了信息时代下快速响应与信息共享的需求。数字化档案管理系统具备严格的权限控制机制，确保档案数据的安全性与保密性，同时支持多用户并发访问与协同工作，促进了档案管理的规范化、标准化与智能化发展。它为企业、政府机构及各类组织提供了强有力的信息支撑，助力其在复杂多变的环境中做出更加精准、高效的决策[1]。

2 数字化档案管理系统面临的安全威胁

首先，数字化档案管理系统面临的主要安全威胁之一是数据泄露风险。在数字化过程中，档案数据被转化为电子形式，并通过网络进行传输和存储。这一过程中，若安全防护措施不到位，将极易遭受黑客攻击、病毒入侵等网络安全事件，导致数据被非法获取或篡改。此外，部分外包服务商在数字化过程中可能未经授权地复制或传播数据，进一步加剧了数据泄露的风险。其次，档案实体在数字化过程中的安全也不容忽视。纸质档案在数字化前需经过拆卷、扫描、校核等多个环节，若管理不善，可能导致档案原件的完整性受损，如邮票、印花税票等票证脱落或被人为盗取。同时，数字化过程中还可能因操作不当导致档案排序错乱，甚至造成档案原件的遗失或损毁。最后，数据存储的安全性也是数字化档案管理系统面临的重要挑战。数据存储方式的选择直接关系到数据的安全与可访问性。目前，许多组织采用光盘、云存储等方式存储数字化档案，但这些方式均存在一定的安全隐患。例如，光盘存储虽成本低廉，但寿命有限，且易受物理损害；云存储则可能面临数据被非法访问或篡改的风险[2]。

3 数字化背景下档案管理系统信息安全设计

3.1 设立稳定的安全防护墙

为了将数字化档案信息的安全防护提升至全新高度，亟需融合前沿技术，精心编织一张牢不可破的网络安全网。首要任务是加固硬件与软件基础设施的安全壁垒，通过增强它们的安全性能，大幅降低潜在的安全风险，为系统稳定运行奠定坚实的物理基础。随后，必须实施严密的访问权限管理机制，精准设定服务器访问权限，并融合网络端口严格管理与先进防火墙技术，实现数据访问安全性的质的飞跃。这一系列举措旨在构建一个多层次、立体化的数据安全防护体系，

确保每一步访问都经过严格筛选与验证。此外，还应引入全方位的安全监控、深度数据分析、严格审计流程以及高效威胁检测机制。这些措施将赋予我们敏锐的洞察力，能够迅速识别并有效抵御外部威胁，显著降低系统与档案信息遭受恶意攻击的风险[3]。

3.2 构建档案加密系统

3.2.1 AES算法加密

鉴于数字化档案蕴含的数据既广泛又复杂，特别是涵盖了普通信息与高度敏感的涉密内容，亟需采用先进的AES加密算法，为档案中的涉密部分量身打造一套周密的安全防护体系，既要确保涉密信息坚不可摧，抵御任何未授权的窥探与访问，又要兼顾加密过程的高效流畅，避免对终端处理速度造成不必要的拖累，维持在合理且高效的工作区间内。在实施层面，要将所有待加密的涉密档案数据进行系统整合，集中存放于一个专为加密设计的数据库中。随后，利用AES算法的强大加密能力，对这批数据进行深度加密处理，以此构建起一道坚不可摧的数据安全防线。

此外，为了实现对不同类型涉密文件更为精细化的管理，规划了差异化的加密隐私区域，并将这些区域无缝整合至一个统一的涉密模块数据库中。以涉密图片数据为例，依据表1所详细列出的加密参数，对数字化图片档案进行了精细的AES加密处理。

表1 图片数据加密格式

中文字符	英文字符	字符类型	主键/非空
尺寸	Size	Text	否/否
名称	Name	Text	否/是
地址	ID	lnteger	是/是
路径	Path	Text	否/否
源目录	Original catalogue	Text	否/是
源名称	Original name	Text	否/是
类型	Style	Text	否/否

在细致运用特定公式对混沌序列进行重构的基础上，采取了以16位比特为单元的精细分割策略，对明文数据集进行了系统化的划分。紧接着，此分块策略无缝对接至AES加密算法的执行流程中，确保数据的每一细微之处都历经高强度的加密洗礼，无遗漏地增强数据的安全性。最终，经过这一系列精密处理的加密密文，被稳妥地安置于采用蜜罐技术加固的系统中，实现了档案数据的高效加密与严密防护，显著提升了数据保护的整体效能与安全性[4]。

3.2.2 蜜罐技术档案加密系统

1. 设计过程。本探究创造性地整合了蜜罐技术与AES加密算法，通过精心模拟真实环境，为涉密数据库构建起全方位的安全屏障，同时，借助尖端工具精准应对潜在安全挑战。在系统设计层面，匠心独运地构建了一个双重职能的控制管理系统：一方面，它严密管理蜜罐环境中的非涉密档案信息，另一方面，利用这些非敏感数据构建了一个坚不可摧的安全控制平台，从而大幅降低蜜罐被恶意渗透的风险。同时，引入了高效的SeBek工具，它在蜜罐系统中隐秘执行数据捕获任务。SeBek凭借其卓越的捕获能力，能够精准追踪攻击者的每一步行动，生成详尽无遗的攻击特征数据集。随后，利用这些数据自动提炼出攻击特征码，为系统的安全防线加固提供了坚实的数据基石。在具体实施层面，遵循了图1所展示的流程图：首先，利用蜜罐系统诱捕攻击信息，并借助SeBek进行隐蔽的数据捕获；随后，将捕获到的攻击特征数据精心整理成特征码；最后，将这些特征码编录成按时间排序并加密的攻击特征信息日志。这一流程不仅增强了日志的安全性，还为未来档案加密策略的持续优化提供了宝贵的实践依据。

2. 加密功能。将AES算法与蜜罐技术相结合，并对数据进行精简后的高效加密。这一过程涵盖了密钥生成、混沌数据生成与打乱，以及数据扩散等关键步骤。采用AES算法生成一个256位的二进制密钥字符串，利用这个256位密钥与档案管理系统中的特定规则（如第n条记录及第m字段的明文值）相结合，动态生成用于加密每条记录或字段的专属密钥。具体的密钥公式如式（1）所示。

$$k_{nm}=\{x_0, y_0, R, H\} \tag{1}$$

其中，将蜜罐系统分别设定为xo，yo的初始值，将干扰系统运行的数据设定为H，公式中的R则代表为蜜罐系统的数据控制参数，利用该公式获取档案解密的结果：

$$F'_{nm}=f_{k_{nm}}(F_{nm}) \tag{2}$$

在式（2）中，数字化档案的明文设定为F_{nm}，密文设定为F'_{nm}，将加密函数设定为$f_{k_{nm}}$，最终加密密文的结果可通过公式（2）得出。

3.3 应用信息安全保障技术

3.3.1 防火墙技术

“防火墙”这一术语，其精髓在于其隐喻的生动性，实则融合了计算机硬件与软件的精湛技术，被巧妙地

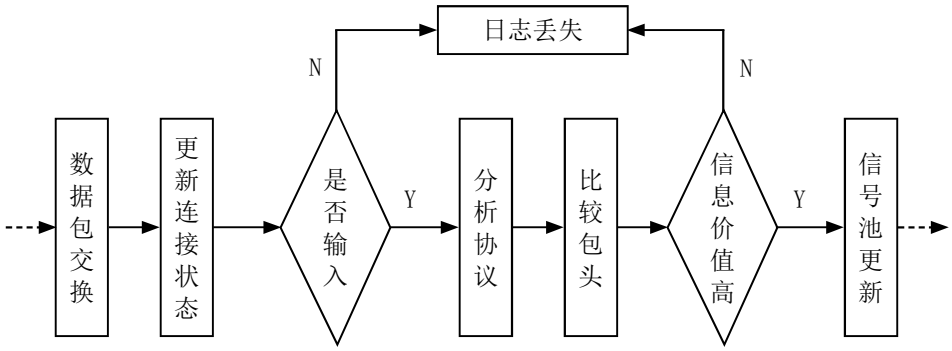

图 1 攻击码特征获取流程图

部署于网络入口处的服务器上。此安全屏障的主要职责是守护宝贵的私有网络资源，通过其强大的防护能力，有效地抵挡来自外部用户的非法窥探与潜在的网络攻击，从而确保所有信息资产的安全与完整，免受侵害[5]。

3.3.2 身份认证与访问的控制

实施高效且可靠的身份认证机制是保障访问权限合法性的基石。在用户账户设立与权限分配的过程中，应优先采用先进的身份验证技术，确保每位用户的身份准确无误，从而有效阻断非法访问的入口。通过精心部署网络访问控制系统，并设定细粒度的访问控制策略，可以实现对用户访问内部档案资源的精确管理，这不仅提升了系统的灵活性与可控性，还极大地降低了敏感数据泄露的风险。此外，需构建一个健全的访问日志审计体系，实时捕捉并分析网络中的各项活动，形成详尽无遗的审计记录，为安全事件的调查与响应提供强有力的支持。

3.3.3 数据备份

档案管理员肩负着定期实施数据备份的重任，有效抵御病毒、木马侵袭及黑客渗透等潜在风险对珍贵档案信息的侵扰与破坏。另外，倡导引入先进的容灾策略，该策略精髓在于将全部档案数据实施全面复制，并巧妙分散存储至多个办公室、跨越不同地域乃至分支机构的计算机系统之中，确保了其安全性与保密性的无懈可击，同时也显著降低了因自然灾害、人为失误或技术故障等不可预见因素引发的数据丢失与损毁风险[6]。

3.3.4 防范系统漏洞

鉴于计算机软件与操作系统在复杂的逻辑设计与精细的编码环节中，难以完全避免瑕疵的存在，这些潜在的漏洞往往成为黑客窥伺的门户，极大地增加了档案信息泄露的安全风险。因此，构建并运行高效的漏洞扫描系统显得尤为迫切和重要。该系统具备智能化检测能力，能够深入剖析本地及远程系统架构，精准识别潜藏的安全漏洞。一旦发现任何安全隐患的蛛丝马迹，系统便能即时触发响应机制，迅速部署针对性的补丁修复方案，从而在威胁实际发生之前就有效筑起一道坚实的防线[7]。

4 结束语

在数字化浪潮的推动下，档案管理系统的信息安全设计成为一项既复杂又至关重要的任务。为了筑牢信息安全防线，我们需严格遵循保密性、完整性、可用性及可控性的核心设计原则。通过实施一系列强化措施，如精细化访问控制机制、高强度的数据加密技术、严密的防火墙与入侵检测系统、全面的安全审计流程、定期的数据备份与恢复策略，以及持续的员工安全教育与培训，我们能够显著提升档案管理系统的安全防护能力。

参考文献：

[1] 滕晓军 . 数字化档案管理系统在医院档案管理中的应用研究 [J]. 黑龙江档案 ,2024(02):261-263.
[2] 张剑阳 . 人工智能驱动的档案数字化管理系统设计 [J]. 产业科技创新 ,2024,06(01):89-92.
[3] 彭柳 , 张淼 , 高杰欣 . 基于区块链技术的电子档案安全存储与可信验证方案 [J]. 中南民族大学学报 : 自然科学版 ,2022,41(06):728-733.
[4] 陈春燕 . 医院内网在线档案云存储隐私信息加密技术研究 [J]. 自动化技术与应用 ,2022,41(06):51-54,61.
[5] 王延红 . 基于云存储技术的电子档案信息库系统设计 [J]. 自动化技术与应用 ,2022,41(11):171-174,183.
[6] 蒋伟红 . 区块链技术对高校档案管理的影响与对策 [J]. 智库时代 ,2022(26):5-8.
[7] 王晓琴 . 基于加密全息数字水印技术的电子档案管存系统设计 [J]. 现代电子技术 ,2021,44(08):81-84.