

计算机信息管理技术与计算机网络安全应用

韩友凯

潍坊职业学院 山东 潍坊 261000

摘要：数字化时代发展进程中，计算机信息管理与网络安全技术成为信息化系统稳定运行的重要支撑。本文围绕计算机信息管理技术基础体系与核心技术类型展开梳理，系统阐述信息采集、存储、传输、处理等基础技术的运行逻辑，区分结构化与非结构化等多元管理技术的应用特点。进一步搭建网络安全基础技术框架，探索信息管理与网络安全的融合应用路径，落实全流程安全管控。

关键词：信息管理技术；网络安全；数据管控；安全防护；融合应用

引言：数字化转型浪潮下，信息资源的规模与复杂度持续攀升，传统管理手段已难以应对海量数据在采集、存储、传输及处理各环节中暴露的安全隐患。计算机信息管理技术为数据的高效组织与流转提供了系统化方案，而网络安全技术则为信息在开放网络环境中的可信流动构筑了防护屏障。两类技术并非独立运行，而是在实际业务场景中相互交织、彼此支撑。信息管理流程中的每一个节点都可能成为安全攻击的切入点，安全策略的缺失同样会削弱信息管理的效能与可信度。将两者有机结合，已成为提升组织信息治理水平的必然选择。

1 计算机信息管理技术基础体系

1.1 计算机信息采集技术

信息采集是整个管理链条的起点，采集质量直接决定后续处理的可用程度。计算机信息采集依托传感器阵列、条码识别设备、射频识别终端以及网页爬虫等工具完成原始数据的获取。采集过程中需关注数据来源的可靠性与采集频率的合理性，高频采集能够捕捉信息的动态变化特征，低频采集则适用于状态相对稳定的场景^[1]。数据在进入系统之前往往存在格式不统一、噪声干扰、冗余字段等问题，预处理环节通过去重与清洗将原始数据转化为可被系统识别的结构化形式，为存储与传输奠定基础。

1.2 计算机信息存储技术

信息存储解决的是数据在时间维度上的持久化保存问题。关系型数据库通过表与表之间的关联实现结构化数据的有序存放，非关系型数据库则以文档、键值对、图结构等形式适应半结构化与非结构化数据的存储需求。分布式存储将数据分散存放于多个物理节点，借助冗余副本机制保障任意节点故障时数据依然完整可读。存储介质从传统磁盘阵列逐步向固态存储与云端对象存储演进，读写速度与容量密度均获得显著提升。存储架

构的选择需要在访问性能、扩展能力与成本控制之间找到平衡点。

1.3 计算机信息传输技术

信息传输承担着数据在不同节点之间流动的任务。局域网内部依托以太网协议完成设备间的高速数据交换，广域网络则借助TCP与IP协议栈实现跨地域的可靠通信。传输过程中面临带宽瓶颈、延迟抖动与丢包等挑战，数据压缩与流量整形技术能够在有限带宽条件下提升有效吞吐量。加密隧道技术为传输链路提供保密性保障，防止数据在中途被截获或篡改。传输协议的选型直接影响信息到达目的地的完整性与时效性，不同业务场景对延迟容忍度的差异要求传输方案具备灵活适配能力。

1.4 计算机信息整合与处理技术

信息整合与处理是将分散的数据转化为可用知识的关键环节。数据整合通过ETL流程将多源异构数据抽取、转换并加载至统一平台，消除格式差异与语义冲突。数据挖掘与统计分析技术从海量记录中提取隐含规律，支撑管理决策。信息处理还涵盖数据脱敏、格式标准化与字段映射等操作，确保不同系统之间的数据能够无障碍流通。处理过程中计算资源的调度与任务优先级的分配影响整体执行效率，合理的任务编排能够在有限资源条件下最大化处理产出。

2 计算机信息管理核心技术类型

2.1 结构化信息管理技术

结构化信息管理技术围绕具备固定模式与明确字段定义的数据展开，这类数据通常以二维表形式存放于关系型数据库之中。每一条记录遵循统一的字段规范，行与列之间存在清晰的逻辑关联，借助主键与外键建立实体间的映射关系。查询语言通过条件筛选与多表联合操作实现对结构化数据的精确检索，事务机制则保障一组操作要么全部完成，要么全部回滚，避免数据处于不一

致状态。数据仓库技术将来自多个业务系统的结构化记录按照主题维度进行组织,支持多维分析与聚合计算^[2]。这种管理方式适用于财务记录、订单明细、人事档案等字段明确、格式固定的业务场景,技术成熟度高且操作可预测性强。

2.2 非结构化信息管理技术

非结构化信息管理技术针对缺乏固定格式的数据类型,包括文本文档、图像、音频、视频以及网页内容等。这类数据无法直接纳入关系型表结构,管理系统采用文档数据库、键值存储或对象存储等方式进行存放。全文检索引擎对文本内容建立倒排索引,使用户能够通过关键词快速定位目标信息。自然语言处理技术从非结构化文本中抽取实体、识别语义关系,将无序内容转化为可被机器理解的结构化表达。图像识别与视频分析技术则赋予系统对多媒体内容进行分类与标注的能力。非结构化数据的体量增长速度远超结构化数据,对存储容量与检索效率提出了更高要求,管理系统需要在保留原始内容完整度与提升可访问性之间寻求平衡。

2.3 动态信息更新与维护技术

动态信息更新与维护技术解决的是数据在生命周期内保持准确性与时效性的问题。信息在产生之后并非一成不变,业务状态的变化、外部环境的波动都会导致数据内容需要修正或补充。增量更新机制仅对发生变化的字段进行修改,避免全量重写带来的资源浪费。版本控制技术为每一次修改保留历史快照,使管理人员能够追溯任意时刻的数据状态。数据一致性维护依赖于定时校验与冲突检测算法,当多个节点对同一条记录进行修改时,系统依据预设规则判定最终取值。过期数据的清理策略与归档机制防止数据库因冗余记录膨胀而性能下降,维护操作的自动化程度直接影响信息管理系统的运行效率。

2.4 分布式信息管理技术

分布式信息管理技术将数据与计算任务分散部署于多个物理节点,通过网络互联形成统一的管理整体。数据分片策略按照一定规则将完整数据集拆分为若干子集,分别存放于不同节点之上,读写请求被路由至对应分片所在的服务器。副本机制为每一份数据维护多个备份,单点故障不会导致信息丢失或服务中断。一致性协议协调各节点之间的数据状态,确保分布环境下的信息准确统一。分布式计算框架将大规模数据处理任务分解为多个子任务并行执行,显著缩短处理耗时。节点间的通信开销与数据迁移成本是这类技术需要重点关注的问题,合理的拓扑设计与负载均衡策略能够有效缓解瓶颈。

3 计算机网络安全基础技术体系

3.1 网络边界防护技术

网络边界防护技术在内部网络与外部网络之间构建起一道安全屏障。防火墙作为边界防护的核心设备,依据预设规则对进出网络的数据包进行逐层检测与过滤,阻断不符合安全策略的通信请求。包过滤技术在网络层与传输层对数据包头信息进行分析,快速丢弃来源不明或目标端口异常的流量^[3]。应用层网关深入解析数据内容,识别并拦截含有恶意代码的网络通信。入侵防御系统部署于网络关键节点,对经过的数据流进行实时特征匹配,将已知攻击行为遏制在网络边界之外。虚拟专用网络技术通过加密隧道将远程通信纳入安全管控范围,使跨公网传输的数据免受窃听与篡改。

3.2 网络数据加密技术

网络数据加密技术通过数学算法将明文转化为密文,使未授权者无法还原原始内容。对称加密算法采用同一把密钥完成加密与解密操作,运算速度快,适合大批量数据的实时保护。非对称加密算法使用公钥与私钥配对,公钥用于加密,私钥用于解密,解决了密钥分发过程中的安全隐患。数字签名技术利用私钥对消息摘要进行加密,接收方通过公钥验证签名真伪,确保消息来源可靠且未被修改。混合加密方案将对称算法与非对称算法结合使用,兼顾了加密效率与密钥交换安全性。传输层安全协议在通信双方之间建立加密通道,保护网页浏览、电子邮件等应用层数据在传输过程中不被截获。

3.3 网络访问控制技术

网络访问控制技术对用户与设备接入网络的权限进行精细化管理。身份认证环节验证用户身份的真实性,密码认证、令牌认证与生物特征认证构成多级验证体系。基于角色的访问控制将权限与岗位职责绑定,用户仅能访问完成工作所需的资源,超出角色范围的操作被系统拒绝。访问控制列表在路由器与交换机上配置过滤规则,限制特定IP地址或端口的通信。网络准入控制在设备接入网络之前检查安全状态,不符合安全要求的终端被隔离至修复区域。单点登录技术将多个应用系统的认证过程统一为一次登录,降低用户频繁输入密码带来的安全风险。

3.4 网络异常行为监测技术

网络异常行为监测技术通过持续采集网络流量与系统日志来发现潜在安全威胁。基于签名的检测方法将网络流量与已知攻击特征库进行比对,命中匹配规则的流量被标记为可疑行为。基于异常的检测方法建立网络流量的正常基线,当实际流量偏离基线超过设定阈值时触

发告警。流量分析技术对数据包的大小、频率、方向等维度进行统计,识别出与正常通信模式不一致的数据流动。日志聚合平台将分散在各设备上的审计记录集中存储,便于安全人员进行关联分析与溯源排查。蜜罐技术部署虚假服务吸引攻击者,记录攻击行为与技术手段,为防护策略的调整提供依据。

4 计算机信息管理与网络安全融合应用

4.1 信息全生命周期安全管控应用

信息从产生到消亡的每一个阶段都需要嵌入安全管控措施。采集阶段对数据来源进行可信性验证,防止污染数据进入管理系统。存储阶段依据数据敏感等级划分存储区域,高密级数据采用加密存放与物理隔离手段。使用阶段通过权限策略约束数据的读取与修改范围,操作记录被完整留存以备审计。共享阶段对跨部门流转的数据实施脱敏处理,确保接收方仅获取完成业务所需的最小信息集。销毁阶段采用覆写或消磁方式彻底清除存储介质上的残留数据,避免信息被恢复利用^[4]。各阶段的安全策略相互衔接形成闭环,任何一个环节出现疏漏都可能导致整体防护失效,全生命周期管控的价值在于将安全思维贯穿于数据流转的每一个节点。

4.2 网络环境下信息权限管控应用

网络环境下的权限管控需要适应多用户、多系统、多终端的复杂场景。角色与权限的绑定关系随岗位变动动态调整,人员离职或转岗后原有权限被即时回收。细粒度权限模型将操作权限拆解为读取、写入、删除、导出等独立单元,管理员可按需组合授予。网络环境中设备接入位置的不确定性增加了权限判定的难度,基于网络位置与设备状态的自适应访问策略能够在保障安全的前提下提升使用便捷性。权限变更操作被记录至审计日志,异常权限申请与越权访问行为触发实时告警。权限管控与信息管理系统深度融合使得数据访问行为可追溯、可控制,有效遏制内部人员的非法操作。

4.3 数据传输过程安全防护应用

数据在网络中传输时面临截获、篡改与重放等多重风险,传输过程的安全防护需要从链路层到应用层进行全栈加固。虚拟专用网络技术在公共网络上建立加密通道,使远程节点之间的通信内容对外部不可见。传输层安全协议为应用数据提供端到端的加密保护,握手阶段完成身份验证与密钥协商。数据完整性校验通过哈希算

法对传输内容生成摘要值,接收方比对摘要值判断数据是否被中途篡改。抗重放机制为每一条消息附加时间戳或序列号,防止攻击者截获合法数据包后重复发送。大文件传输场景下采用分片加密与断点续传技术,避免传输中断后需要从头开始。传输安全与信息管理系统协同运作确保数据在流动过程中始终处于可控状态。

4.4 智能化信息安全管理应用

智能化技术为信息安全管理带来了自动化与主动防御能力。机器学习算法从海量安全日志中提取攻击特征,建立动态更新的威胁识别模型,对未知攻击行为具备一定的发现能力。智能分析引擎对网络流量进行实时分类,异常流量被自动标记并触发响应流程,减少人工研判的时间消耗。自动化编排技术将安全策略的下发、设备的配置与事件的处置串联为标准化流程,人工干预仅在关键决策节点介入。智能风险评估系统持续扫描信息管理系统中的脆弱点,按照风险等级排列修复优先级,引导管理员将有限资源投入到最紧迫的安全问题上。智能化管理的推进使安全防护从被动响应转向主动预防,信息管理与网络安全的融合深度得到实质性提升。

结束语

计算机信息管理技术与网络安全的协同应用,使数据在全生命周期内获得了持续性保护。从采集端的可信验证到存储端的分级加密,从传输链路的端到端防护到智能化平台的主动威胁识别,安全逻辑已渗透至信息管理的各个环节。权限管控与审计机制的完善进一步约束了内部操作风险,分布式架构与一致性协议则为大规模数据场景下的安全运行提供了技术保障。两类技术的深度耦合推动信息安全防护从被动响应走向主动预防,为数字化环境下的数据治理奠定了坚实基础。

参考文献

- [1]付青燕.计算机信息管理技术与计算机网络安全应用[J].消费电子,2025(10):167-169.
- [2]王辉.计算机信息管理技术与计算机网络安全应用[J].IT经理世界,2025,28(2):70-72.
- [3]赵洪强.云计算技术在计算机网络安全防御系统中的应用[J].信息系统工程,2025(7):52-55.
- [4]张旭.网络时代计算机网络安全管理技术与应用[J].信息记录材料,2024,25(9):144-146.