电子信息系统中的数据安全与加密技术

陈蕴哲

350402*******0011

摘要：电子信息系统中的数据安全与加密技术研究，围绕核心要素、常见安全威胁及成因、主流加密技术类型、保障体系构建及发展趋势展开。明确数据全生命周期安全防护、加密技术与系统场景适配性、数据访问权限控制与审计机制等核心要素，阐述数据泄露途径与诱发因素、非法入侵手段与防御漏洞、数据篡改方式与潜在风险等威胁及成因，分析对称加密、非对称加密、哈希加密等技术类型，探究法律法规与行业标准引导、安全技术与加密机制融合、人员安全意识与操作规范强化等保障体系，展望量子加密产业化、人工智能驱动动态加密、零信任架构加密体系等趋势，为数据安全保障提供思路。

关键词：电子信息系统；数据安全；加密技术

DOI：10.64216/3080-1508.25.07.044

引言

电子信息系统中的隐私保护技术已成为保障数据安全与用户隐私的关键。电子信息系统已成为社会运转的核心基础设施，海量敏感数据在此汇聚流转，其安全防护关乎个人权益、企业生存与国家稳定。当前，网络攻击手段不断翻新，数据泄露、篡改等事件频发，传统安全防护体系渐显乏力。加密技术作为数据安全的“最后一道防线”，在抵御未授权访问、保障数据完整性方面作用关键。深入研究电子信息系统中的数据安全与加密技术，探索适配不同场景的防护策略，对构建多层次安全屏障、维护数据生态秩序具有重要现实意义。

1 电子信息系统数据安全与加密技术的核心要素

1.1 数据全生命周期的安全防护

数据全生命周期的安全防护贯穿数据从产生、传输、存储到销毁的各个阶段，形成闭环式安全管理。数据产生阶段需进行分类分级，根据敏感程度标记保护等级，如个人身份证号、企业商业秘密等敏感数据需采取最高级加密措施。传输过程中通过加密通道（如 SSL/TLS 协议）确保数据不被截获或篡改，同时采用分段加密技术降低单次传输风险。存储阶段结合加密算法对数据进行加密处理，如数据库加密、文件加密等，并定期备份加密数据以防丢失。销毁阶段需采用专业工具彻底清除数据痕迹，避免残留信息被恢复，如对存储介质进行多次覆写或物理销毁。

1.2 加密技术与系统场景的适配性

加密技术与系统场景的适配性要求根据不同电子信息系统的特点选择合适的加密方案，避免“一刀切”式应用。金融交易系统对实时性要求高，需采用高效的对称加密技术（如 AES），在保证安全的同时减少延迟；电子商务平台涉及多方交互，适合使用非对称加密技术（如 RSA）实现身份认证与密钥交换。物联网设备资源受限，应选用轻量级加密算法（如 ChaCha20），降低对设备算力和能耗的影响；云端存储系统数据量大且访问频繁，可采用混合加密模式，用非对称加密保护对称密钥，再用对称加密处理数据，平衡安全性与效率。

1.3 数据访问的权限控制与审计机制

数据访问的权限控制与审计机制是防范内部泄露的关键，通过精细化管理确保“数据可用不可见”。权限控制采用最小权限原则，根据用户角色分配访问范围，如普通员工仅能查看工作所需数据，管理员拥有更高权限但需双人复核。引入多因素认证（如密码+指纹+动态验证码）增强身份验证安全性，防止账号被盗用。审计机制则对所有数据访问行为进行记录，包括访问者身份、时间、操作内容等，形成不可篡改的审计日志。通过日志分析可及时发现异常访问，如非工作时间大量下载数据、越权访问敏感文件等，触发预警并追溯责任。

2 电子信息系统面临的常见数据安全威胁及成因

2.1 数据泄露的主要途径与诱发因素

数据泄露的主要途径包括外部攻击与内部失当操作，诱发因素涉及技术漏洞与管理缺陷。外部途径中，黑客通过钓鱼邮件、恶意软件等获取系统权限，窃取数据库中的敏感数据；公共网络传输时，数据若未加密易被监听截取。内部途径更为隐蔽，员工可能因操作失误将涉密文件发送至外部邮箱，或因利益驱使泄露数据；

离职人员未及时注销账号，导致权限被滥用。技术层面，加密算法过时、密钥管理不善（如密钥明文存储）会增加泄露风险；管理层面，安全培训不足、保密制度松散使员工安全意识薄弱，如使用弱密码、随意接入不明网络，为数据泄露埋下隐患。

2.2 非法入侵的技术手段与防御漏洞

非法入侵的技术手段不断升级，利用电子信息系统的防御漏洞实施攻击。常见手段包括 SQL 注入，通过构造恶意 SQL 语句篡改数据库；缓冲区溢出攻击，向程序输入超长数据覆盖内存，执行恶意代码；DDoS 攻击，通过大量虚假请求耗尽系统资源，使合法用户无法访问。防御漏洞多源于系统更新不及时，未修复已知安全补丁；防火墙配置不当，对异常流量识别不精准；入侵检测系统灵敏度不足，难以发现新型攻击。

2.3 数据篡改的实现方式与潜在风险

数据篡改的实现方式包括对传输中数据的中途拦截修改与对存储数据的非法篡改，可能引发严重后果。传输阶段，黑客通过“中间人攻击”截获加密数据，伪造身份与通信双方分别建立连接，篡改数据后重新加密发送，导致接收方获取错误信息。存储阶段，攻击者突破数据库防护后，直接修改记录内容，如篡改金融系统中的交易金额、医疗系统中的患者病历。潜在风险因数据类型而异，政务系统数据被篡改可能引发社会信任危机；电商平台价格数据被修改会造成经济损失。

3 电子信息系统中主流的加密技术类型

3.1 对称加密技术的应用特点与适用场景

对称加密技术的核心是加密与解密使用相同密钥，具有运算速度快、效率高的特点，适合处理大量数据。其加密过程简单，通过对明文按固定块大小进行分组，使用密钥和算法进行转换，如 AES 算法支持 128 位、192 位、256 位密钥，安全性随密钥长度增加而提升。适用场景包括本地文件加密，如对电脑中的文档、图片进行加密保护；实时通信加密，如即时聊天工具的消息加密，确保对话内容仅双方可见；数据库加密，对存储的大量结构化数据进行加密，防止数据库被盗取后信息泄露。

3.2 非对称加密技术的原理优势与实践方式

非对称加密技术采用公钥与私钥配对使用，公钥可公开分发，私钥由用户自行保管，解决了对称加密的密钥分发难题。其原理基于数学难题（如大整数分解、离散对数），用公钥加密的数据仅能通过对应的私钥解密，反之亦然。优势在于无需传递私钥，安全性更高，且可用于身份认证，通过私钥签名、公钥验证确认发送者身份。实践中，常用于密钥交换，如 HTTPS 协议中，服务器向客户端发送公钥，客户端用公钥加密对称密钥后发送，服务器用私钥解密获取对称密钥，后续通信使用对称加密。

3.3 哈希加密技术的数据校验功能与应用范围

哈希加密技术通过哈希函数将任意长度的输入转换为固定长度的哈希值（摘要），具有不可逆性，即无法从哈希值反推原始数据，主要用于数据完整性校验。其核心功能是检测数据是否被篡改，原始数据哪怕仅修改一个字符，生成的哈希值也会截然不同。应用范围包括文件校验，用户下载文件后，将计算的哈希值与官方提供的哈希值比对，确认文件未被篡改或感染病毒；密码存储，系统不直接存储用户密码，而是存储密码的哈希值，登录时计算输入密码的哈希值与存储值比对，避免密码明文泄露；区块链技术，每个区块包含前一区块的哈希值，形成链式结构，确保区块数据不可篡改。常用的哈希算法有 SHA-256、SHA-3 等，安全性高于已被破解的 MD5、SHA-1。

4 电子信息系统数据安全与加密的保障体系构建

4.1 法律法规与行业标准的规范引导

法律法规与行业标准为电子信息系统的数据安全与加密提供刚性约束和操作指引。国家层面需完善数据安全相关法律，明确数据加密的强制性要求，如对敏感个人信息、关键基础设施数据必须采用加密保护，规定加密技术的最低标准。行业标准应结合领域特点细化规范，金融行业需制定交易数据加密标准，明确加密算法类型与密钥管理要求；医疗行业需规范患者病历的加密存储与传输流程，平衡安全与医疗效率。建立违规惩戒机制，对未落实加密要求导致数据泄露的企业或个人依法追责，提高违法成本。

4.2 安全技术与加密机制的融合应用

安全技术与加密机制的融合应用形成多层次防护体系，提升电子信息系统的整体安全性。将加密技术与防火墙结合，对进出网络的数据流进行加密过滤，仅允许加密的合法数据通过；与入侵检测系统联动，当检测到异常访问时，自动提升加密等级并锁定可疑账号。终端安全方面，在操作系统、应用软件中集成加密模块，如硬盘加密、U 盘加密，防止设备丢失后数据泄露；云安全方面，采用同态加密技术，允许对加密数据直接进行计算，既保护数据隐私又不影响云端处理功能。

4.3 人员安全意识与操作规范的强化

人员安全意识与操作规范的强化是减少人为因素导致安全事件的关键。定期开展安全培训，内容包括加密技术原理、常见攻击手段、应急处理流程等，通过案例分析让员工认识到数据泄露的严重后果，如某企业员工因点击钓鱼链接导致客户数据泄露，面临巨额赔偿和声誉损失。制定详细的操作规范，明确数据加密的操作步骤，如敏感文件发送前必须加密，外接设备接入前需进行病毒扫描，密码设置需包含大小写字母、数字和特殊符号且定期更换。建立奖惩制度，对严格遵守规范的员工给予奖励，对违规操作导致安全事件的予以处罚。

5 电子信息系统数据安全与加密技术的发展趋势

5.1 量子加密技术的产业化应用探索

量子加密技术基于量子力学原理，利用光子的量子态进行密钥分发，具有理论上的无条件安全性，是应对量子计算威胁的重要方向。量子计算机的强大算力可能破解现有 RSA、ECC 等非对称加密算法，而量子加密的密钥在传输过程中若被窃听，会因量子态叠加原理导致密钥变化，通信双方可立即察觉，确保密钥绝对安全。当前产业化应用探索集中在量子密钥分发（QKD）网络建设，通过光纤或卫星构建广域量子通信网络，为金融、政务等关键领域提供加密服务。

5.2 人工智能驱动的动态加密防护

人工智能驱动的动态加密防护通过机器学习分析系统行为与威胁模式，实现加密策略的自适应调整，提升防护的智能化水平。人工智能可实时监测电子信息系统的运行状态，如数据访问频率、用户操作习惯、网络流量特征等，建立正常行为基线；当发现异常（如陌生 IP 大量访问敏感数据），自动提升加密等级，如从 128 位 AES 加密升级为 256 位，或临时启用多因素认证。通过分析历史攻击数据，人工智能能预测潜在威胁类型，提前调整加密算法或密钥轮换周期，如针对某类新型 malware 攻击，优先采用抗干扰能力强的加密模式。

5.3 基于零信任架构的加密体系构建

基于零信任架构的加密体系遵循“永不信任，始终验证”原则，打破传统网络的内外网边界，对每个访问请求进行严格加密与验证，适合复杂分布式的电子信息系统。其核心是将加密保护延伸至每个数据节点和访问主体，无论用户位于内网还是外网，访问任何数据都需经过身份认证、权限校验，并对传输和存储的数据全程加密。构建方式包括微服务加密，将系统拆分为多个微服务，每个微服务独立加密并设置访问控制。

6 结论

电子信息系统的数据安全与加密技术需围绕全生命周期防护、场景适配、权限控制等核心要素，应对数据泄露、非法入侵、篡改等威胁。对称加密、非对称加密、哈希加密各有适用场景，通过法律法规引导、技术融合应用、人员意识强化构建保障体系。未来，量子加密、人工智能动态防护、零信任加密体系将推动安全防护升级，为电子信息系统提供更可靠的安全保障，助力数字社会的健康发展。

参考文献

[1]彭访.电子信息系统的数据安全探究[J].中国培训,2017,(02):292.

[2]刘永亮,冯庆云,夏辉福.基于大数据技术的电子信息安全保护策略分析[J].电子技术,2025,54(02):144-145.

[3]廖清阳,宗志亚.云计算下的电力信息系统安全技术探微[J].电子元器件与信息技术,2021,5(02):109-110.

[4]余化龙.智能技术在电子信息产业中的应用[J].电子技术,2025,54(05):389-391.

[5]周志军.云数据管理与电子信息工程系统的集成分析[J].集成电路应用,2024,41(06):316-317.