浅谈计算机信息系统的安全保密技术

薛　靖
苏州江南航天机电工业有限公司　江苏　苏州　215000

摘　要：本文围绕计算机信息系统的安全保密技术展开探讨，首先明确保密性、完整性、可用性三大核心要素，分析各要素的定义、核心需求及相互关联。接着分类阐述关键技术，包括数据加密、访问控制、网络防护、终端安全技术，详解各类技术的应用场景与作用机制。最后从技术更新与适配、人员安全意识培养、安全运维管理三方面提出实施保障措施，为构建全面的信息系统安全保密体系提供思路，助力防范数据泄露、恶意攻击等风险，保障信息系统稳定安全运行。

关键词：计算机信息系统；安全保密技术；核心要素；实施保障

引言：当前计算机信息系统已深度融入企业运营、政务处理、个人生活等领域，系统中存储与传输的敏感数据价值日益凸显，安全保密需求愈发迫切。然而，数据窃取、恶意攻击、人为操作失误等风险持续威胁系统安全，传统防护手段难以应对新型场景下的安全挑战。在此背景下，深入剖析信息系统安全保密的核心要素，梳理关键技术类型，明确实施保障路径，对提升系统抗风险能力、保护敏感数据安全、维护信息系统正常运转具有重要现实意义。

1 计算机信息系统安全保密的核心要素

1.1 保密性

保密性作为信息系统安全保密的基础要素，其定义聚焦限制敏感数据的访问范围，仅允许经过合法授权的主体获取与使用数据。敏感数据涵盖个人隐私信息、企业商业机密、机构核心业务数据等，这些数据一旦被未授权主体接触，可能引发隐私泄露、经济损失或业务混乱等严重后果。核心需求体现在数据全生命周期中，需防止数据在存储阶段被非法侵入终端或服务器窃取，在传输阶段被拦截监听，在使用阶段被违规复制或传播。例如数据存储时需通过加密技术隐藏内容，传输时需建立安全通道隔绝外部窥探，使用时需通过权限控制限定操作范围。保密性与完整性、可用性存在紧密关联[1]。只有先确保数据不被未授权访问，才能为数据完整性提供保护前提，避免未授权主体篡改数据；同时，保密性保障下的授权访问机制，也能减少恶意主体通过非法访问破坏系统的可能，为系统与数据的可用性奠定基础。若保密性缺失，数据完整性与可用性将失去防护根基，整个信息系统的安全保密体系会随之崩塌。

1.2 完整性

完整性的定义明确为确保数据在产生、传输、存储全过程中，内容不被未授权修改、删除或添加。数据产生时需准确记录原始信息，传输过程中需避免内容被篡改，存储阶段需防止数据被恶意修改或意外损坏，以此维持数据的真实性与准确性。核心需求在于避免数据因篡改导致信息失真，这类失真可能影响后续决策制定或引发安全风险。例如企业财务数据被篡改可能导致财务核算错误，医疗健康数据被修改可能影响诊断结果，政务数据被篡改可能破坏公共服务秩序。因此，保障数据完整性是维护信息系统可信度的关键。完整性需与身份认证、访问控制等技术协同发挥作用。身份认证技术可验证访问主体的合法性，避免未授权主体接触数据；访问控制技术可限定授权主体的操作权限，仅允许进行必要的数据操作，从源头减少数据被篡改的可能。数据完整性校验技术如哈希校验，可通过比对数据特征值，及时发现数据是否被篡改，形成完整的防护链条。

1.3 可用性

可用性的定义强调确保授权主体在需要时，能够正常访问信息系统与所需数据，系统不被恶意阻断或因故障无法运行。这一要素关注信息系统的服务连续性，无论面对恶意攻击还是意外故障，都需保障授权主体的正常使用需求。核心需求包括抵御拒绝服务等攻击，避免系统因攻击陷入瘫痪导致数据无法使用；同时需应对硬件故障、软件漏洞、自然灾害等突发情况，通过冗余设计、故障恢复等手段，减少系统中断时间。例如金融交易系统需24小时保持可用，一旦中断将影响资金流转；应急指挥系统需在紧急情况下稳定运行，保障指挥指令顺利传达。实践中需平衡安全性与可用性，避免过度防护影响系统正常运行。例如过于严格的访问控制可能增加授权主体的操作复杂度，频繁的安全验证可能延长数据访问时间。因此，在设计安全保密方案时，需结合系

统使用场景与数据重要程度，制定合理的防护策略，在保障安全的同时，确保系统与数据的访问效率，满足授权主体的实际使用需求。

2 计算机信息系统安全保密关键技术分类

2.1 数据加密技术

数据加密技术是保障数据安全的核心手段，通过特定算法将原始数据转化为不可直接识别的密文，为数据全生命周期提供保护[2]。存储加密针对本地硬盘、数据库等存储载体中的数据开展处理，无论是个人电脑本地文件还是企业服务器中的业务数据，经加密后即使存储设备丢失或被非法侵入，未掌握密钥的主体也无法解读数据内容，有效避免数据泄露风险。传输加密聚焦网络传输中的数据安全，包括邮件发送、文件传输、即时通信等场景下的数据，通过加密处理让数据在网络通道中以密文形式传输，即便传输过程中被截获，截获方也难以破解获取有效信息，保障数据在跨设备、跨网络传递时的安全性。加密算法选择需结合实际场景需求，对称加密算法采用单一密钥进行加密与解密，运算速度快、效率高，适用于大量数据加密场景，如数据库整体加密、大文件存储加密；非对称加密算法使用公钥与私钥配对工作，公钥可公开传递，私钥由用户单独保管，安全性更高，更适合密钥交换、数字签名等场景，如用户登录认证时的密钥传递。

2.2 访问控制技术

访问控制技术通过多重机制严格管控数据访问权限，确保只有合法主体能按权限操作数据。身份认证是第一道防线，通过密码、生物特征、智能卡等方式验证访问主体身份，密码需满足复杂度要求以提升安全性，生物特征利用独特的个人信息如指纹、人脸等进行识别，智能卡则通过硬件载体存储身份信息，多重认证方式可有效杜绝非法身份进入系统。权限分配遵循“最小权限原则”，根据主体的角色、职责为其分配对应的数据访问与操作权限，例如普通员工仅能访问自身工作相关的数据，无法接触企业核心机密数据，避免权限过度授予导致的数据安全风险，确保每个主体仅能在授权范围内开展操作。访问审计通过记录主体对数据的访问与操作行为，形成详细的审计日志，日志内容包括访问时间、访问主体、操作内容、访问结果等信息，一旦出现数据异常操作或安全事件，可通过审计日志追溯源头，排查风险原因并界定相关责任，为安全事件处理提供依据。

2.3 网络防护技术

网络防护技术构建起系统与外部网络之间的安全防线，抵御各类外部攻击威胁。防火墙技术在系统与外部网络交界处建立防护屏障，依据预设的安全规则对进出网络的数据包进行过滤，允许符合规则的合法网络请求通过，拦截非法请求与恶意连接，阻止未授权主体通过网络访问内部系统，减少外部攻击入口[3]。入侵检测与防御技术实时监测网络流量与系统行为，通过分析网络数据特征、系统操作记录，识别病毒、木马、SQL注入等恶意攻击行为，发现异常时可自动采取阻断措施，如切断攻击连接、屏蔽攻击IP，同时发出告警信号提醒管理人员及时处理，避免攻击对系统造成进一步破坏。虚拟专用网络（VPN）技术为远程访问提供安全保障，当外部人员需要访问内部系统时，通过VPN建立加密传输通道，让数据在公网环境中安全传输，既满足远程办公、异地协作的需求，又确保远程访问过程中的数据安全，防止数据在公网传输时被窃取或篡改。

2.4 终端安全技术

终端设备作为信息系统的重要接入点，其安全防护对整体系统安全至关重要。终端准入控制对接入信息系统的终端如电脑、移动设备进行合规性检查，检查内容包括是否安装杀毒软件、杀毒病毒库是否更新、系统补丁是否完善等，不符合安全要求的终端将被禁止接入系统，避免存在安全漏洞的终端成为攻击入口。终端数据防护借助数据防泄露（DLP）技术，对终端数据的拷贝、外发行为进行限制，可设置禁止通过U盘拷贝敏感数据、限制敏感文件通过邮件外发等规则，实时监控终端数据流转情况，防止敏感数据通过各类途径外泄，保障终端存储数据的安全。终端安全管理通过统一平台对终端的软件安装、系统配置、补丁更新进行管控，管理人员可远程推送必要的软件安装包、统一配置系统安全参数、及时下发系统补丁，避免终端因私自安装不安全软件、系统配置不当、漏洞未修复等问题引发安全风险，提升终端设备整体安全性。

3 计算机信息系统安全保密技术的实施保障

3.1 技术更新与适配

技术更新与适配是确保安全保密技术持续有效的关键。需按季度或半年度定期评估现有安全技术的有效性，结合信息系统应用场景变化，如业务系统升级、用户规模扩大等，分析技术在防护范围、防护强度上是否仍能满足需求。随着云计算、物联网等新型应用场景普及，传统安全技术可能无法覆盖这些场景的特殊风险，因此要及时引入适配新场景的安全保密技术，如针对云计算环境的云数据加密、云访问控制技术，针对物联网设备的轻量级加密、设备身份认证技术，填补新型场景下的安全防护空白[4]。同时需密切关注加密算法、防护

工具的技术迭代，老旧加密算法可能因破解技术发展失去保密效果，存在漏洞的防护工具易成为安全突破口。需建立技术跟踪机制，安排专人关注行业期刊、技术论坛等渠道发布的最新技术动态，对达到使用年限、存在安全隐患的技术方案及时替换，例如将强度不足的加密算法更新为符合当前安全标准的算法，将功能落后的防护工具升级为具备实时监测、智能防御能力的新一代工具，避免因技术滞后导致防护失效，确保安全保密技术始终与风险防控需求相匹配。

3.2 人员安全意识培养

人员安全意识培养是降低人为安全风险的核心举措。需每月或每季度开展定期安全培训，培训形式可采用线上课程与线下实操结合的方式，线上课程方便人员灵活学习，线下实操可通过模拟钓鱼邮件点击、密码设置演练等环节强化学习效果。培训内容应结合实际工作场景，普及信息系统安全保密知识，包括识别钓鱼邮件的方法，如通过检查发件人地址、警惕陌生链接与附件；正确设置密码的技巧，如采用复杂组合、定期更换密码；规范数据操作的流程，如敏感数据不随意拷贝、不通过非安全渠道传输等，通过案例讲解、实操演示等方式，让人员直观认识安全风险，掌握防范方法。建立安全保密责任机制同样重要，需明确不同岗位人员的安全职责，如系统管理员负责维护系统安全、数据管理员负责管控数据访问、普通员工负责保护个人操作终端与经手数据，将安全责任落实到具体岗位与个人。通过签订安全保密协议、每季度开展责任考核等方式，进一步强化人员对敏感数据的保护意识，让人员认识到自身行为与信息系统安全的关联性，主动规范操作行为，减少因人员疏忽或违规操作引发的安全风险。

3.3 安全运维管理

安全运维管理是保障安全保密技术持续发挥作用的基础。需制定常态化安全运维流程，明确日常运维工作内容与频率，定期开展系统漏洞扫描，通过专业工具检测系统软件、硬件存在的漏洞，及时安装补丁修复；定期进行数据备份，根据数据重要程度确定备份频率与备份方式，确保数据在丢失或损坏时可快速恢复；定期开展日志审计，分析系统操作日志、访问日志，排查异常操作行为，及时发现潜在安全隐患，将风险消除在萌芽阶段[5]。运维人员需具备专业的安全知识与实操能力，能熟练操作运维工具，准确判断风险类型并采取应对措施。同时需做好运维记录管理，详细记录每次运维工作的内容、时间、结果，形成完整的运维档案，便于后续追溯与复盘。建立应急响应机制不可或缺，针对数据泄露、系统被攻击等突发安全事件，需提前制定应急处置流程，明确事件上报路径、处置步骤与各环节责任分工，如发现数据泄露后，需立即阻断泄露渠道、评估泄露范围、通知相关人员、采取补救措施。同时储备应急处置资源，如组建专业应急团队、准备数据恢复工具，确保突发安全事件发生时能快速响应、高效处置，最大限度降低事件造成的损失，保障信息系统尽快恢复正常运行。

结束语

计算机信息系统安全保密技术是守护数据资产与系统稳定的重要屏障，其核心要素为保密性、完整性、可用性，关键技术涵盖数据加密、访问控制等多维度，实施保障需技术、人员、管理协同发力。随着技术迭代与应用场景拓展，信息系统面临的安全威胁将更复杂，未来需持续优化安全保密技术，适配云环境、物联网等新场景，同时强化人员安全意识与运维管理。唯有不断完善安全保密体系，才能有效抵御风险，为计算机信息系统的安全运行提供坚实保障。

参考文献

[1]李选超.基于计算机信息系统的保密技术及安全管理研究[J].电子元器件与信息技术,2021,5(12):237-238.

[2]瞿勇.计算机信息系统的保密技术及安全管理研究[J].数字通信世界,2021(06):161-162.

[3]周晓辉.计算机信息系统的保密技术及安全管理阐述[J].电子技术与软件工程,2021(05):259-260.

[4]陈利.计算机网络信息安全保密技术探讨[J].长江信息通信,2021,34(06):138-140.

[5]吴红.新环境下的计算机网络信息安全及其防火墙技术应用分析[J].网络安全技术与应用，2022（7）：14-16.