大数据时代云计算环境下敏感信息泄露风险防控策略

梁　涛
新疆天山职业技术大学　新疆　乌鲁木齐　830017

摘　要：大数据时代云计算环境下，敏感信息泄露风险防控至关重要。本文分析云计算环境下敏感信息泄露风险，包括定义、来源、路径与影响评估。接着构建防控技术体系，涵盖数据加密、访问控制等技术。提出了防控策略，涉及数据安全管理体系、供应链安全管理等。最后阐述实施保障措施、效果验证方法与持续优化机制，旨在为云计算环境下敏感信息泄露风险防控提供全面且可行的方案。

关键词：云计算；大数据；敏感信息泄露；风险防控

引言：在大数据与云计算深度交织的当下，数据量呈爆炸式增长，云计算凭借其资源整合与灵活调配优势，成为数据处理与存储的关键支撑。然而，这种融合也使敏感信息面临前所未有的泄露风险，一旦泄露，将对个人、企业乃至国家造成严重损害。因此，深入剖析云计算环境下敏感信息泄露风险，构建有效的防控策略，成为保障数据安全、推动产业健康发展的迫切需求。

1 云计算环境下敏感信息泄露风险分析

1.1 敏感信息定义

敏感信息是指一旦泄露、非法提供或滥用可能危害国家安全、公共利益，或者侵犯自然人、法人合法权益的信息。在云计算环境中，此类信息涵盖范围广泛，包括个人身份信息如姓名、身份证号、联系方式、生物识别信息等，企业经营信息如核心技术方案、客户资源清单、财务报表、商业合同等，以及政务信息中涉及公共服务、社会管理的未公开数据。与传统环境相比，云计算的分布式存储和多租户特性使敏感信息边界更模糊，需结合云服务类型精准界定[1]。例如，IaaS模式中用户自主管理的操作系统数据与SaaS模式中服务商托管的业务数据，虽存储层级不同，但符合上述危害特征的均属于敏感信息范畴，需纳入重点保护体系。

1.2 泄露风险来源

云计算敏感信息泄露风险来源多样，主要有技术架构缺陷、服务商管理疏漏、外部攻击渗透三类。技术上，云平台虚拟化漏洞、分布式文件系统权限配置不当、API接口无安全校验等，都可能致数据泄露；服务商方面，数据中心物理防护差、运维操作不规范、日志审计缺失及内部人员违规拷贝数据等问题频发；外部攻击中，黑客通过钓鱼、勒索病毒、DDoS攻击等窃取数据。此外，云服务迁移和旧系统退役时若处理不当，也会引发风险，且这些来源相互交织，防控难度大。

1.3 泄露路径与影响评估

敏感信息泄露路径分技术、管理、操作层面。技术路径有云服务器漏洞、传输被截获、存储介质损坏等；管理路径包括安全制度缺失、权限混乱、审计监督失效；操作路径涉及员工误点链接、违规传输、第三方数据共享失控。影响评估要多维展开，个人身份信息泄露会导致多种损失；企业核心商业信息泄露会丧失竞争力、引发客户流失和经济赔偿；政务和关键行业数据泄露危害公共安全和国家安全。量化评估需结合数据量级、敏感等级等测算损失。

2 敏感信息泄露防控技术体系

2.1 数据加密技术

数据加密技术是防控敏感信息泄露的核心手段，贯穿数据全生命周期，包括传输加密、存储加密和使用加密三个关键环节。传输加密采用SSL/TLS协议构建安全传输通道，确保数据在用户端与云服务器之间、云服务各节点之间传输时不被截获解密，针对重要数据可采用双重加密机制提升安全性[2]。存储加密采用透明加密技术对云存储中的敏感数据进行加密处理，密钥由用户自主管理或采用密钥管理系统分级管控，防止存储介质被盗或越权访问导致数据泄露。使用加密通过动态脱敏加密技术，在数据调用过程中对敏感字段进行实时加密，仅授权用户可通过密钥解密查看原始数据，同时支持加密算法动态切换，适配不同云服务场景需求，有效抵御暴力破解等攻击手段。

2.2 访问控制与身份认证

在敏感信息泄露防控技术体系中，访问控制与身份认证是关键防线，能精准限制用户对敏感信息的访问权限，防止非法获取。访问控制通过制定严格的策略，依据用户角色、职责和权限，对云环境中的资源访问进行精细管控。它可设定不同用户对各类数据和系统的操作

权限，如普通员工仅能查看部分非敏感数据，而管理员则拥有更广泛的管理权限。同时，结合访问时间、地点等条件，进一步增强控制力度，例如限制特定时间段内的访问，或仅允许在公司内部网络访问敏感信息。身份认证是验证用户身份真实性的关键环节。采用多因素认证方式，如密码、短信验证码、指纹识别、面部识别等组合，大幅提升认证安全性。单一密码易被破解，多因素认证则能有效抵御此类风险。持续身份认证技术可在用户访问过程中实时监测其行为，一旦发现异常，如操作习惯改变、访问频率异常等，立即触发二次认证或终止访问，防止账户被盗用后进行非法操作。通过完善的访问控制与身份认证技术，能确保只有合法、授权的用户才能访问敏感信息，从源头降低泄露风险，为云计算环境下的数据安全保驾护航。

2.3 数据脱敏与匿名化

数据脱敏与匿名化是平衡数据使用与安全保护的关键技术，通过对敏感信息进行格式转换或内容处理，实现数据可用不可见。数据脱敏技术分为静态脱敏和动态脱敏，静态脱敏适用于数据离线共享场景，通过替换、删除、掩码等方式处理敏感字段，例如将身份证号后六位替换为星号，处理后的数据可用于开发测试、数据分析等场景；动态脱敏适用于数据在线访问场景，根据用户身份权限和访问场景实时调整数据展示形式，同一数据对管理员展示完整信息，对普通用户展示脱敏后信息。匿名化技术通过删除个人标识信息、模糊化属性信息等方式，使处理后的数据无法关联到具体个人，常用方法包括k-匿名、l-多样性、t-接近性等，确保数据在用于大数据分析时不泄露个人隐私，同时保留数据统计价值。

2.4 安全监测与应急响应

安全监测与应急响应技术构建起敏感信息泄露的动态防护屏障，实现风险早发现、早处置。安全监测采用多维度监测机制，通过部署云安全态势感知平台，实时采集云服务器日志、网络流量数据、用户操作行为等信息，运用机器学习算法分析异常行为特征，例如识别多次失败的登录尝试、异常的数据批量传输、违规的端口访问等风险事件，及时触发预警。应急响应建立标准化流程，包括预警核实、风险隔离、漏洞修复、数据恢复四个环节，当监测到泄露风险时，立即核实风险等级，通过关闭异常账户、切断违规传输链路等方式隔离风险源，利用漏洞补丁修复技术缺陷，借助数据备份系统恢复受损数据。建立应急响应演练机制，定期模拟不同泄露场景，提升技术团队应急处置能力，缩短风险处置时间。

3 大数据时代云计算环境下敏感信息泄露风险防控策略

3.1 数据安全管理体系建设

数据安全管理体系建设需构建“制度-流程-责任”三位一体的架构，适配大数据与云计算融合场景需求。制度层面，制定数据分类分级标准，依据数据敏感等级和重要程度划分为绝密、机密、秘密、公开四个等级，针对不同等级明确存储期限、传输方式和访问权限；建立数据全生命周期管理制度，覆盖数据采集、存储、使用、共享、销毁各环节，规范数据处理流程。流程层面，搭建数据安全管理平台，实现数据分类分级自动化、权限申请审批流程化、操作行为审计全程化；建立跨部门协同机制，明确IT部门、业务部门、安全部门的职责分工，确保数据安全管理落地执行。责任层面，落实数据安全主体责任，明确管理层、技术人员、操作人员的安全职责，建立责任追究机制，对违规操作导致数据泄露的行为严肃追责。

3.2 供应链安全管理

云计算环境下供应链安全管理需覆盖云服务商、软硬件供应商、第三方合作机构等全链条，防范供应链各环节的安全风险。对云服务商的管理方面，建立严格的服务商准入机制，从资质认证、安全技术能力、应急处置能力、服务质量等维度进行评估，选择符合安全要求的服务商；签订详细的服务级别协议和数据安全协议，明确数据存储位置、安全防护责任、泄露赔偿条款等内容，定期开展服务商安全审计[3]。对软硬件供应商的管理方面，建立供应商安全评估体系，对服务器、数据库、安全设备等硬件产品进行安全检测，对操作系统、中间件、应用软件等软件产品进行漏洞扫描和源代码审计，杜绝存在安全缺陷的产品进入供应链。对第三方合作机构的管理方面，严格审核合作机构的安全资质，规范数据共享范围和方式，对共享数据进行脱敏处理，定期开展合作机构安全检查，确保供应链各环节安全可控。

3.3 人员培训与安全意识提升

人员是敏感信息泄露防控的关键因素，人员培训与安全意识提升需构建常态化、分层化的培训体系。培训内容应结合云计算和大数据场景特点，涵盖数据安全法律法规、企业数据安全制度、敏感信息识别方法、常见泄露风险防范技巧、钓鱼攻击识别与应对、应急处置流程等内容，同时增加实际案例分析，提升培训针对性。培训方式采用线上线下相结合的模式，线上通过安全学习平台提供课程视频、在线测试等资源，方便员工自主学习；线下开展专题讲座、实操演练、安全知识竞赛等

活动，增强培训互动性。分层培训方面，针对管理层开展战略层面的安全培训，提升安全决策能力；针对技术人员开展专业技能培训，提升安全技术防护和应急处置能力；针对普通员工开展基础安全培训，提升安全意识和规范操作能力。建立培训效果评估机制，通过在线测试、实操考核、行为审计等方式评估培训效果，将评估结果与员工绩效挂钩，对表现优秀的员工给予奖励，对考核不合格的员工进行补训，确保培训达到预期效果。

4 防控策略实施保障与效果验证

4.1 实施保障措施

防控策略实施保障需从组织、技术、资源三个维度构建支撑体系，确保防控措施落地执行。组织保障方面，成立数据安全专项工作小组，由企业高层担任组长，统筹协调各部门资源，制定防控策略实施计划和时间表，明确各阶段工作任务和责任人，定期召开工作推进会，解决实施过程中存在的问题。技术保障方面，加大安全技术投入，升级云安全防护设备，部署数据加密、访问控制、安全监测等技术系统，构建技术防护体系；建立技术研发机制，针对云计算和大数据场景出现的新型风险，研发适配的安全技术和工具，提升风险防控技术水平。资源保障方面，合理配置安全预算，确保安全技术采购、人员培训、审计评估等工作有充足资金支持；建立安全人才培养和引进机制，通过内部培训、外部招聘等方式组建专业的安全人才队伍，同时与高校、科研机构合作，引进先进的安全技术和理念，为防控策略实施提供全方位保障。

4.2 效果验证方法

防控策略效果验证需采用定量与定性相结合的方法，全面评估防控措施的有效性。定量评估方面，建立关键指标评估体系，包括敏感信息泄露事件发生率、漏洞修复及时率、安全监测预警准确率、应急处置完成时间、员工安全知识考核通过率等指标，通过数据统计分析，量化评估防控策略实施效果；开展渗透测试和漏洞扫描，组织专业安全团队模拟黑客攻击，检测云平台和数据系统的安全防护能力，发现潜在安全漏洞。定性评估方面，组织行业专家、安全顾问对防控体系进行评审，从制度完善性、技术先进性、管理规范性等维度评估防控策略的合理性；开展用户满意度调查，收集业务部门、员工对防控措施的反馈意见，评估防控措施的可行性和适用性。通过定量与定性评估相结合，全面掌握防控策略实施效果，为后续优化提供依据。

4.3 持续优化机制

敏感信息泄露风险处于动态变化中，需建立持续优化机制，确保防控策略适配风险变化。建立风险动态监测机制，定期开展风险评估，结合云计算技术发展、大数据应用场景拓展、外部攻击手段升级等因素，识别新型风险点，更新风险清单和防控重点[4]。建立策略迭代更新机制，根据风险评估结果和效果验证反馈，及时修订数据安全制度、优化技术防护方案、调整管理流程，例如针对新型勒索病毒攻击，升级加密技术和监测规则；针对员工操作习惯变化，优化培训内容和方式。建立行业交流合作机制，参与行业安全论坛、技术研讨会，与同行分享防控经验，学习先进的防控技术和理念；跟踪国际国内数据安全法律法规更新，确保防控策略符合合规要求。通过持续优化，使防控体系始终保持有效，应对各类敏感信息泄露风险。

结束语

大数据与云计算深度融合，敏感信息泄露风险防控形势严峻。本文从风险分析、技术体系构建、防控策略制定到实施保障与效果验证，形成一套完整防控方案。然而，风险动态变化，防控需持续优化。未来，应紧跟技术发展与法规更新，不断调整完善防控体系，强化人员安全意识，提升技术防护能力，以有效应对各类风险，保障敏感信息安全，推动大数据云计算产业健康发展。

参考文献

[1]曾海峰.大数据时代计算机网络安全技术的优化策略[J].网络空间安全，2024，15(4):232-235.

[2]向丽,何花,宋春.电力企业敏感信息数据防泄密技术研究[J].网络安全技术与应用,2021,(12):110-112.

[3]孙典,徐亚峰,黄成鑫,陶希同.分布式网络敏感信息泄露预警系统[J].电脑知识与技术,2021,17(25):102-105.

[4]侯桂明,杨文泽,杨天华.互联网环境下档案业务监督服务的安全保密管理[J].兰台内外,2024(16):7-9.