工程与管理科学
Engineering and Management Science
第 8 卷◆第 5 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

基于云计算的企业数据安全治理体系研究

毛敬玉
兰州职业技术学院　730070

DOI:10.32629/ems.v8i5.20224

［摘　要］近年来网络技术的迅猛发展，给人们的生产生活带来了诸多便利，同时也带来了一系列的安全问题，其中最为严重的就是网络非法入侵和黑客攻击，给存储在网络中的数据造成了极大的泄露风险，因此有必要采取有效的措施来解决这一问题。云计算的出现弥补了这一缺陷，安全性高、效率高的优点使其在网络安全、存储安全领域逐渐地得到了广泛的应用。基于此，文章就基于云计算的企业数据安全治理体系展开了相关研究，以供参考。

［关键词］云计算；企业数据；安全治理

引言：

随着企业数字化转型步入深水区，云计算已从最初的资源手段发展为支撑业务创新的基础设施。传统以网络边界防护为主的安全体系存在以下问题：一方面，云服务商与云租户之间的安全责任共担模型在执行层面往往出现认知偏差，部分企业把数据安全保障完全寄托于云平台，忽视了企业内部在身份管理、访问控制、合规遵从等方面的主体责任；另一方面，随着《数据安全法》《个人信息保护法》等法律法规的颁布，数据分类分级、出境评估、最小权限等合规要求在云架构下的落地难度显著增加，企业在云上构建的数据处理流程常常难以满足监管对数据全生命周期的管控要求。因此如何构建一套既能够适配云原生技术架构，又能融合企业管理的数据安全治理体系，已成为当前亟待解决的一项重要课题。

一、云计算环境下企业数据安全风险分析

（一）云计算技术概述

云计算技术的问世，标志着计算机网络技术进入了一个全新的发展时期。从电厂模式、效用计算到网格计算，云计算历经三个阶段的发展，逐步形成了今日较为完善的技术体系。与传统网络计算技术相比，云计算的优势体现在多个方面：其一，云计算技术支持多种软件与终端设备的接入，能为企业提供基础设施即服务、平台即服务、软件即服务等多样化的服务模式；其二，云计算技术具备极强的横向扩展能力与海量数据存储容量，可高效完成对 PB 级乃至 EB 级数据的处理分析；其三，云计算技术运行依赖于一系列标准化协议，可以保证不同系统之间互联互通的可操作性。但是云计算技术的应用也给企业带来了新的安全风险，企业在享受云计算带来的高效率之余，必须对数据安全风险予以足够重视。

（二）企业数据安全面临的主要风险

置身于上述复杂的云架构环境中，企业数据资产正面临着前所未有的风险挑战，这些风险贯穿了数据的采集、传输、存储、使用直至销毁的全生命周期。在多租户共享环境下，虚拟化逃逸与侧信道攻击等底层技术隐患可能导致不同租户间的数据隔离失效，一旦云服务商的底层代码出现漏洞，攻击人员便可能突破逻辑隔离屏障窃取敏感信息。配置错误已成为云数据泄露的首要诱因，由于云控制台权限设置的复杂性，企业极易因疏忽将对象存储桶或数据库设置为公开访问，致使海量数据直接暴露于互联网之下。此外，云端数据的静态存储加密密钥管理难度显著增加，如果密钥与数据同存或缺乏有效的轮转机制，加密防线就会形同虚设。在数据共享环节，特权账号滥用与内部人员威胁被放大，缺乏细粒度访问控制的云环境允许拥有高权限的用户轻易批量导出或篡改数据，形成难以管控的安全盲区。更为严峻的是，数据在跨域传输过程中面临的中间人攻击风险，以及云资源释放后逻辑销毁不彻底导致的残留数据恢复风险，任何单一环节的疏漏都可能引发连锁反应，造成不可估量的经济损失。

（三）云服务模式下的责任划分问题

云安全治理的另一大痛点源于云服务模式下责任共担模型的认知错位，这往往是导致安全真空地带的根本原因。尽管主流云服务商均明确了云平台安全由厂商负责，云上内容安全由用户负责的基本原则，但在实际的 IaaS、PaaS 及 SaaS 不同服务模式中，具体的责任边界往往随着服务层级的加深而发生偏移，许多企业未能准确理解这一界限，误以为上云即意味着将安全责任全盘外包。在基础设施即服务（IaaS）模式下，用户要承担从操作系统到应用数据的全部安全责任，而在平台即服务（PaaS）或软件即服务（SaaS）模式中，云厂商接管了更多底层栈的安全维护，但用户仍需对身份认证、访问策略及数据分类分级负有不可推卸的最终责任。加之云

服务商提供的原生安全工具功能繁杂且更新迅速，企业如果缺乏专业的云安全运营团队，便难以有效利用这些工具落实自身应承担的责任部分，最终导致合规基线无法落地，在面对监管审计或安全事件溯源时,因责任界定不清而陷入被动，凸显了强化用户端安全治理能力的紧迫性。

二、基于云计算的数据安全技术

（一）数据加密技术

在云计算中，数据面临着诸多潜在风险，如网络传输过程中的窃取风险以及存储在云端时被未授权访问的风险。对称加密算法，如 AES，具有加密速度快的优点，适用于对大量数据进行加密，其使用相同的密钥进行加密和解密操作，在云存储内部，对于单个用户的数据加密场景下效率较高。但是对称加密的密钥管理较为复杂，密钥的安全分发是一个重要问题。而非对称加密的计算复杂度较高，加密速度相对较慢。加密密钥的生成、存储和分发管理机制也十分重要，安全的密钥管理系统要采用多重身份验证、密钥备份与恢复策略等措施，以确保密钥的安全性。

（二）身份认证与访问控制技术

身份认证和访问控制技术在云计算数据安全存储中起着重要作用，多因素身份认证技术通过结合多种认证方式，如密码、令牌和生物识别，大大提高了用户身份认证的准确性。在云存储环境中，当用户请求访问存储数据时，多因素身份认证能有效防止非法用户的入侵。基于角色的访问控制模型根据用户在组织中的角色分配相应的访问权限，例如，普通员工只能访问与工作相关的部分数据，而管理员则具有更广泛的权限。属性－基于访问控制（ABAC）模型则更加科学，其根据用户、资源和环境等多种属性来确定访问权限。例如，根据数据的敏感度属性和用户的安全级别属性来决定是否允许访问。

（三）数据备份与恢复技术

在云存储中，数据备份策略包括全量备份和增量备份。全量备份是对整个数据集进行备份,虽然备份过程耗时较长，但恢复时较为简单。增量备份则只备份自上次备份以来发生变化的数据，但恢复过程相对复杂，要按照备份的顺序逐步恢复数据。异地备份和多副本存储技术也是保障数据安全的有效方式。异地备份将数据存储在不同地理位置的数据中心，当一个地区发生自然灾害或其他灾难时，其他地区的数据副本仍然可以保证数据的可用性。多副本存储技术则是在同一数据中心或不同数据中心创建多个数据副本，通过冗余存储提高数据的可靠性。在制定灾难恢复计划时，要明确恢复时间目标和恢复点目标。

三、基于云计算的企业数据安全治理体系框架构建

（一）总体设计原则

构建基于云计算的企业数据安全治理体系，必须确立以“零信任”为理念的总体设计原则，该体系坚持以数据为中心的战略导向,确保安全策略紧密跟随数据资产的流动轨迹，实现防护能力在混合云环境中的延伸。面对云原生架构下海量日志与复杂威胁的挑战，设计要深度融合自动化与智能化技术，利用人工智能驱动威胁的实时感知、自动研判及响应闭环，大幅缩短风险处置窗口。同时合规驱动是体系建设的基础，须把《中华人民共和国数据安全法》等法律法规及行业监管要求内化为具体的管理流程。体系架构应把安全能力嵌入 DevSecOps 全流程，通过统一身份认证、细粒度访问控制及全链路加密等机制，构建起可视、可管、可控的弹性防御纵深，最终实现安全与业务发展的协同共生。

（二）治理体系总体架构

1.战略层

战略层是企业云数据安全治理体系的顶层设计，其核心在于把数据安全从单纯的技术支撑职能提升为企业数字化转型的战略资产。在战略层面，企业要先确立“安全与业务共生”的治理理念，即数据安全是驱动业务创新、保障数据要素价值释放的主动引擎。具体而言，战略层需完成三项关键任务：其一，明确数据安全治理的目标，治理目标与企业的业务战略、风险管理偏好及行业合规要求深度对齐；其二，构建权责清晰的决策机制，由企业最高管理层人员共同组成云数据安全治理委员会，负责审定数据安全策略、审批重大资源投入、协调跨部门权责边界，确保治理指令能够穿透组织层级直达业务前端；其三，确立云环境下的安全责任共担原则，清晰界定云服务商、企业安全部门、业务部门与运维部门在数据全生命周期中的职责边界，避免责任真空或权责重叠。

2.管理层

在管理层面上，企业要构建以制度规范、流程管控与考核评价为主体的管理体系。制度规范方面，应以《数据安全法》《个人信息保护法》及行业监管要求为依据，制定覆盖云上数据全生命周期的制度文件体系，包括《云数据分类分级管理规范》《云平台访问控制与权限管理办法》《云数据安全事件应急响应预案》等，形成从通用政策到具体操作指引的完整制度链条。流程管控方面，重点建立数据资产的全流程闭环管理机制。考核评价方面，数据安全治理成效要纳入业

务部门与安全部门的绩效考核体系，建立关键绩效指标，通过量化评价倒逼治理责任的真正落地。

3.技术层

技术层级构建了以零信任架构为主的技术栈，集成统一身份与访问管理、数据分类分级引擎、密钥管理系统及数据安全态势感知平台等组件。利用机器学习与大数据分析技术，技术层实现了对敏感数据的自动发现、动态脱敏及异常行为实时阻断，确保数据在采集、传输、存储及使用过程中的机密性与完整性。特别是在混合云场景下，技术层通过 API 网关安全加固、微隔离技术及全链路加密手段，有效应对多租户隔离失效与接口攻击风险，为数据资产提供全天候、全方位的智能化防护，使安全能力具备弹性伸缩的特性。

4.执行层

执行层直接面向开发运维团队及一线业务人员，安全控制点无缝嵌入到 CI/CD 流水线中，确保代码上线前即完成漏洞扫描与合规检查。在日常运营中，执行层负责执行具体的访问授权、日志审计、数据备份及灾难恢复演练，保证安全策略在终端与云工作负载间得到执行。面对突发安全事件，执行层依托自动化编排与响应系统，迅速启动应急预案，进行威胁隔离、取证分析及业务恢复，损失降至最低。该层级强调操作的标准化，通过工具化的手段减少人为失误。

四、基于云计算的企业数据安全治理机制

（一）数据分类分级机制

数据分类分级的核心在于构建一套自动化且贴合业务场景的资产识别定级体系，以解决云环境下数据资产的管理难题。该机制利用机器学习与自然语言处理技术，部署智能数据发现引擎，对云上对象存储、数据库及大数据平台中的海量数据进行深度内容识别。系统能自动识别个人身份信息、商业机密、财务数据等敏感字段，结合数据所属的业务域、使用频率及泄露后的影响，依据国家行业标准与企业内部规范，实时赋予数据相应的安全等级标签。基于分类分级结果，治理体系能自动生成差异化的保护策略，把抽象的安全要求转化为具体的技术控制指令，例如对重要商密数据强制实施字段级加密与严格访问审批，对一般公开数据则采取宽松策略，从而实现安全资源的最优配置。

（二）数据全生命周期安全管理机制

在采集阶段，强调源头合规，通过嵌入隐私协议校验与最小化采集原则，从入口端过滤非法或过度收集的数据，利用数字水印技术标记数据来源。进入传输环节，强制推行国密算法或高强度国际加密标准，建立端到端的加密通道，防止数据在跨域、跨云或多可用区流转中遭受中间人攻击或流量劫持。存储阶段聚焦数据安全，实施存储加密与密钥分离管理，引入防篡改技术，同时建立云端数据残留清理标准。销毁阶段，必须建立严格的销毁审批与审计流程，保证数据彻底清除。

（三）安全监测机制

安全监测机制依托大数据分析与人工智能技术，构建统一的数据安全态势感知平台，全面汇聚云厂商原生日志、应用系统日志、网络流量及终端行为数据，形成全局可视的安全视图。系统通过建立用户与实体行为分析模型，深度学习正常业务基线，捕捉异常数据下载、非工作时间访问、高频失败登录及敏感数据违规外传等隐蔽威胁。一旦监测到潜在风险，机制立即触发自动化编排与响应流程，自动执行阻断连接、隔离主机、回收权限或通知管理员等处置动作，平均响应时间压缩至分钟级甚至秒级。

结语：

综上所述，云计算环境下的企业数据安全治理是一项系统性的长期工程。企业必须构建以数据为中心、以零信任为理念的治理体系。通过清晰的战略导向，完善分层架构设计，落地数据分类分级、全生命周期管控、细粒度访问控制及智能安全监测等机制，企业才能有效化解云端风险。

[参考文献]

[1]郝爽.信息化管理下的企业数据安全风险及治理措施[J].通讯世界,2025,32(12):42-44.

[2]林川捷.集团数据治理技术体系的探索与设计——基于分级分类、安全运营与防护技术的框架研究[J].中国新通信,2025,27(22):35-37.

[3]叶中华.国有企业在线培训数据安全治理路径研究[J].现代国企研究,2025,(10):123-127.

[4]万海军,穆小红,何颖珊,等.企业档案数据要素化组织和价值化驱动的治理模式与实践路径探讨[J].档案管理,2025,(04):104-106+111.

[5]马威风,冯波.大数据背景下数据安全治理策略研究与实践[J].办公自动化,2025,30(07):124-128.

作者简介：毛敬玉，女，出生年月：1981.03，汉族，籍贯：甘肃临夏，学历：硕士，职称：副教授，研究方向：计算机网络，云计算。