云计算环境下的大数据安全管理研究

马红岩[1]　何小倩[*2]
1.浙江鹰途软件有限公司　浙江杭州　310000
2.杭州智数科技有限公司　浙江杭州　310000

摘　要：随着信息技术的飞速发展，云计算与大数据技术的深度融合已成为推动社会信息化进程的重要动力。然而，在这一发展趋势下，数据安全问题日益突出，尤其是在云计算环境中，大数据的集中存储和远程访问模式使其更容易受到网络攻击、数据泄露及非法篡改等威胁。因此，如何在保障数据高效流通的同时，确保其安全性，成为当前亟需解决的重要课题。本文围绕云计算环境下的大数据安全管理展开研究，首先阐述云计算与大数据技术的基本原理与融合应用，其次分析面临的主要安全挑战，包括数据隐私保护、访问控制、数据完整性验证等关键问题，最后提出一系列针对性的安全管理对策和技术手段，如加密算法、访问权限分级、可信计算等，以期为提升大数据安全保障能力提供理论支撑与实践指导。

关键词：云计算；大数据；安全管理；数据隐私

进入信息时代以来，数据已成为继土地、资本和劳动力之后的又一核心生产要素，随着云计算、大数据等新兴信息技术的迅猛发展，企业与政府机构纷纷将数据存储、计算与服务转移至云端，以实现更高效的资源整合与智能决策支持。在这一过程中，海量数据在云平台中被快速生成、传输和处理，极大提升了社会运行效率。然而，云计算环境中数据的开放性与共享性，也带来了前所未有的安全管理挑战。尤其在大数据背景下，数据的高维度、多样性和快速变化性，使得传统的安全管理机制难以完全适应。本文正是在这样的背景下展开，旨在通过对云计算与大数据融合技术的系统分析，探讨如何构建科学、可靠的安全管理体系，从而推动数据资源在保障安全的前提下发挥最大价值。

一、云计算与大数据技术概述

（一）云计算技术架构与服务模式

云计算是一种基于互联网的计算服务模式，其核心理念是将分布式计算、虚拟化技术和服务导向架构相结合，为用户提供按需分配、弹性可伸缩的IT资源。云计算的技术架构主要包括基础设施层、平台层（PaaS）和软件层（SaaS）三大服务模式，其中IaaS为用户提供虚拟服务器与存储资源，PaaS为开发者提供开发与运行平台，而SaaS则提供直接面向用户的软件服务。该架构通过虚拟化与资源池化技术实现资源的高效利用与动态调度，大幅降低了IT建设成本，提高了运维效率。在云计算环境下，用户无需拥有和维护物理设备，只需通过互联网即可访问所需的计算服务，这种远程服务模式也对数据安全管理提出了更高的要求。云计算服务安全运维保障要求如表1所示。

表1　云计算服务安全运维保障要求

要求类型	内容
云计算环境与资产运维管理	环境管理、资产管理、介质管理、数据管理
云计算系统安全漏洞检查与风险分析	安全漏洞监测、安全漏洞扫描、安全合规检查、安全风险分析
云计算系统安全设备及策略维护	网络和系统安全管理、恶意代码防范管理、密码管理、设备维护管理、配置管理、变更管理
云计算系统安全监管	云计算系统安全测评、外包运维管理
云计算系统安全监测与应急响应	监控和审计管理、应急预案管理、安全事件处置、备份与恢复管理

（二）大数据的特点与处理技术

大数据指的是规模巨大、结构复杂、变化快速的数据集合，其核心特征可概括为“4V”，包括即体量、速

作者简介：
马红岩（1979.8-）男，汉族，辽宁铁岭人，本科，研究方向为大数据、信息安全。
何小倩（1991.11-）女，汉族，福建南平人，本科，研究方向为软件开发、信息安全。

度、多样性和价值密度低[1]。在实际应用中，大数据不仅包括结构化数据，还包含大量半结构化与非结构化数据，如图片、视频、日志文件等，对数据的存储与处理能力提出了更高要求。为应对这些挑战，目前主要采用分布式计算框架（如Hadoop、Spark）、NoSQL数据库、数据挖掘与机器学习等技术，提升数据处理效率与智能化水平[2]。大数据的广泛应用推动了信息社会的转型，但同时也使数据安全问题更加复杂和多元，亟需在技术与管理层面加强保障[3]。

二、云计算环境下的大数据安全挑战

（一）数据存储安全问题

在云计算环境中，大数据往往以分布式方式存储在多个物理位置分散的数据中心中，这种多节点、高并发的存储架构虽然提高了系统的处理能力和容灾能力，但也带来了严重的数据存储安全问题[4]。首先，数据集中存储于云服务提供商的平台，使得数据所有权与数据控制权分离，用户无法对数据的存储过程进行全面掌控，存在数据被非法访问、窃取或篡改的风险。其次，云存储系统容易成为黑客攻击的目标，一旦攻击成功，可能导致大规模数据泄露。此外，由于不同用户的数据可能被存储在同一物理服务器上，存在“多租户隔离”不严的问题，攻击者可通过技术手段突破虚拟化层而窃取他人数据[5]。云存储中数据备份和恢复机制不完善，也可能在系统故障或攻击事件发生时导致数据永久丢失。

（二）数据传输与访问安全

在云计算环境中，大数据在采集、处理、传输和共享的各个环节都可能面临安全威胁，尤其是在数据传输和访问过程中更容易遭受攻击。首先，数据在云端与用户设备之间传输过程中，若未采用安全的通信协议或加密机制，容易被中间人攻击、监听或篡改，从而导致数据泄露或内容被恶意修改。其次，由于云平台存在大量用户同时访问系统的情况，如果访问权限管理不严，可能出现未授权访问、越权操作等问题，严重影响数据的完整性与保密性。此外，不同用户对同一数据集的访问需求不同，而云平台若未建立精细化的访问控制机制，容易导致数据过度暴露或资源滥用。同时，一些攻击者还可能通过构造恶意请求，借助应用程序漏洞获取敏感数据或进行拒绝服务攻击（DDoS），造成服务中断。

（三）用户隐私保护难题

在云计算与大数据融合的背景下，用户的行为数据、位置信息、交易记录、浏览历史等被广泛采集和分析，虽然为个性化服务提供了支持，但也引发了严重的隐私保护问题。首先，大数据分析往往需要整合多个数据源，容易造成用户隐私的“再识别”风险，即便是经过脱敏处理的数据，也可能通过多源信息的交叉比对还原出用户真实身份。其次，云服务平台在提供数据处理能力的同时，掌握了大量用户敏感信息，若服务提供商管理不当或内部员工恶意操作，可能导致隐私数据外泄。此外，当前在隐私保护法律法规、标准体系方面仍存在一定滞后，一些企业为获取商业利益甚至主动泄露用户信息。再者，用户在云端对自身数据缺乏有效的控制权和知情权，难以明确数据被如何使用、分享或保存。

三、大数据安全管理策略与技术手段

云计算平台的安全保障应从信息系统、物理与环境、网络通信、设备计算、应用数据等多层面入手，通过全面部署网络安全技术并整合多种安全手段，能够构建多重网络安全机制，有利于实现平台整体安全可控，从而保障云计算环境的稳定与可信。云计算平台安全防范机制如表2所示。

表2　云计算平台安全防范机制

保护对象类型	安全措施内容
物理和环境安全	物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护
网络和通信安全	网络架构、通信传输、边界防护、访问控制、入侵防范、恶意代码防范、安全审计、集中管控
设备和计算安全	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、镜像和快照保护
应用和数据安全	身份鉴别、访问控制、安全审计、软件容错、资源控制、接口安全、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护

（一）加密与脱敏技术

在云计算环境中，大数据在存储、传输和处理过程中面临诸多安全威胁，加密与脱敏技术作为核心的数据保护手段，能够有效保障数据的机密性与隐私性。加密技术主要通过对数据进行编码处理，使其在未授权访问时无法读取，常见的加密算法包括对称加密（如AES）和非对称加密（如RSA）。在实际应用中，数据传输阶段可采用SSL/TLS协议进行加密，保障数据在网络中传输的安全性；数据存储阶段则可采用磁盘加密、数据库加密等方式。脱敏技术则是在不影响数据结构和可用性的

前提下，对敏感数据进行模糊化处理，如掩码、替换、加扰等方法，广泛应用于数据分析和共享场景，确保敏感信息（如身份证号、银行卡号、用户联系方式等）不被泄露。

（二）访问控制与身份认证机制

访问控制与身份认证机制是保障云计算环境下大数据安全的关键环节，直接关系到数据资源的合理授权与使用。访问控制主要解决“谁能访问哪些数据、在什么条件下访问”的问题，常见模型包括基于角色的访问控制（RBAC）、基于属性的访问控制（ABAC）等。RBAC通过为用户分配角色，再赋予角色相应权限，适用于组织结构清晰的企业环境；而ABAC则基于用户属性、环境属性和资源属性动态判断访问权限，更加灵活，适应复杂的云环境。身份认证机制则用于确保访问者身份的真实性，目前主流方式包括口令认证、双因素认证、生物识别认证和基于PKI的数字证书认证等。在云平台中，推荐使用多因素认证结合单点登录（SSO）机制，提升用户体验同时增强安全性。

（三）安全审计与日志管理

在大数据系统中，安全审计与日志管理是实现可追溯、安全监控和合规审查的重要手段。安全审计通过对系统操作、用户行为、权限变更等进行记录和分析，能够及时发现异常行为、潜在风险和违规操作，是应对内部威胁和外部攻击的重要保障。而日志管理则包括日志采集、存储、分析和响应等多个环节，通常涵盖访问日志、操作日志、系统日志和应用日志等类型。为提高日志数据的处理效率，云环境中常采用分布式日志系统（如ELK Stack）进行实时日志分析与可视化展示，有助于安全运维人员及时发现问题并做出响应。

结语

综上所述，在云计算环境下，大数据安全管理已成为信息技术发展过程中的重要课题，本文通过对云计算架构特点、大数据安全风险及其成因进行分析，探讨了访问控制、数据加密、隐私保护、身份认证等安全管理策略，在技术、管理与制度多方协同下，从而能够有效提升云计算环境下的大数据安全水平。

参考文献

[1]韦明剑.基于云计算环境下的大数据安全与隐私保护分析[J].电脑爱好者（普及版）（电子刊），2020（11）：807-808.

[2]顾潇腾.大数据云计算环境下的数据安全探讨[J].数字通信世界，2024（8）：223-225.

[3]黄晔华.大数据云计算环境下的数据安全问题与防护研究[J].数字通信世界，2024（11）：32-34.

[4]王格.大数据云计算环境下的数据安全探析[J].通信电源技术，2022，39（6）：167-169.

[5]邓湘勤，丁朋鹏.大数据云计算环境下的数据安全分析[J].网络安全技术与应用，2023（8）：59-60.