

Research on Real-time Security Monitoring and Auditing Technology of Big Data in Cloud Computing Environment

Miao Kong

Anhui Medical University, Hefei, Anhui, 230032, China

Abstract

With the increasing application of cloud computing and big data in various industries, which also puts forward higher challenges to data security and compliance, the research on real-time security monitoring and auditing technology of big data in cloud computing environment is particularly important. Firstly, the real-time security monitoring of big data in cloud computing environment is explored to reinforce the stable operation and security protection of the business system from the dimensions of system monitoring, security monitoring, business monitoring and resource monitoring. Then it reviews the aspects of data integrity audit, access control audit, log audit, and compliance audit to ensure the integrity and compliance of big data, with a view to providing a strong technical support for the future management and application of big data.

Keywords

cloud computing; big data; real-time security monitoring; auditing techniques

云计算环境中大数据的实时安全监控与审计技术研究

孔淼

安徽医科大学, 中国·安徽 合肥 230032

摘要

随着云计算和大数据在各行各业的应用日益广泛,这也对数据的安全性和合规性提出了更高的挑战,因此,对云计算环境中大数据的实时安全监控与审计技术的研究显得尤为重要。探讨了云计算环境下大数据的实时安全监控,从系统监控、安全监控、业务监控、资源监控等维度,对业务系统的稳定运行和安全防护进行加固。针对数据完整性审计、访问控制审计、日志审计、合规性审计等方面进行评述,以确保大数据的完整性和合规性,以期为未来大数据的管理和应用提供了有力的技术支持。

关键词

云计算; 大数据; 实时安全监控; 审计技术

1 引言

随着信息技术的飞速发展,云计算和大数据技术已成为推动现代社会数字化进程的重要力量,云计算以其高效的资源利用、灵活的扩展性和便捷的服务模式,为企业事业单位提供了前所未有的数据处理能力。同时,大数据技术的应用也使得海量数据的收集、存储、分析和挖掘成为可能,极大地促进了科学研究、商业决策和社会治理的智能化^[1]。由于云计算环境的复杂性和大数据的多样性,数据泄露、非法访问、恶意攻击等安全威胁层出不穷,存在给相关机构带来经济和声誉受损的风险。因此,探讨云计算环境中大数据的实时安全监控与审计技术研究具有重要意义。

2 云计算环境中大数据的实时安全监控研究

2.1 系统监控

在云计算环境中,大数据的实时安全监控确保了大数据服务能够稳定、可靠地运行,而系统监控作为实时安全监控的核心部分,涵盖了设备状态与运行、实时性,以及可视化与智能化等多个方面。系统监控通过持续收集和分析设备的性能指标、健康状态等信息,能够迅速发现设备故障或潜在的性能瓶颈,确保云计算服务的稳定性和高可用性,一旦发现问题,系统监控能够立即触发响应机制,如发送警报通知、执行自动修复等,从而迅速解决问题,减少服务中断时间^[2]。系统监控采用实时数据分析技术,能够即时获取设备的状态信息和运行数据,并在短时间内完成大量数据的处理和分析,这使得系统监控能够迅速发现异常情况并做出响应。此外,系统监控通过可视化界面,管理员可以直观地查看设备的状态信息、性能指标等,从而更加方便地进行管理和维护。同时,基于大数据分析和机器学习技术,系统监控

【作者简介】孔淼(1981-),男,中国安徽合肥人,本科,工程师,从事大数据、信息安全研究。

能够对设备的运行数据进行深度分析,发现潜在的问题和趋势,并给出相应的建议和改进措施,这种智能化分析不仅提高了管理的效率,也进一步增强了云计算环境的安全性和稳定性。通过系统监控的实时性、可视化与智能化特性,可以确保大数据服务的稳定性和高可用性,从而为用户提供更加优质、可靠的服务体验。

2.2 安全监控

随着数据量的不断增长和云计算服务的广泛应用,安全威胁也日益多样化和复杂化,因此,实施有效的安全监控措施对于保护大数据的安全至关重要。

安全监控的核心在于实时分析系统日志、网络流量等关键数据,以便检测和评估系统运行过程中遭遇的各类安全问题,包括但不限于网络攻击、恶意软件入侵、数据泄露等。安全监控通过实时分析,能够迅速捕捉到异常行为或潜在威胁的迹象,从而确保在威胁发生之前或初期阶段就能够得到及时的处理^[3]。在安全监控过程中,安全监控技术运用先进的算法和模型,对数据进行深度分析和挖掘,以发现潜在的安全威胁,一旦检测到异常情况,系统能够立即触发相应的应对措施,这些应对措施可以是自动的,如隔离受感染的设备、阻断恶意流量、关闭部分网络端口等,也可以是手动的,如启动应急响应机制、通知管理员进行人工干预等。此外,实时分析与应对的能力使得安全监控系统能够迅速响应安全威胁,减少潜在损失。

2.3 业务监控

业务监控通过实时监控云平台上的业务状态,能够实时获取业务运行的关键指标,如响应时间、吞吐量、错误率等,这些指标直接反映了业务的运行状况,是评估业务性能的重要依据,一旦业务监控系统发现业务运行出现异常,如响应时间延长、错误率升高等,它能够立即发出警报,并触发相应的处理机制。另外,业务监控通过对业务运行数据的深入分析,业务监控系统能够发现业务性能的瓶颈和潜在问题。系统可以提供相应的优化建议,如调整网络配置、优化数据库查询语句、改进代码性能等^[4]。业务监控的另一个重要价值在于提升用户体验。用户是业务服务的最终接受者,对于业务的性能和稳定性有着直接的感受。通过业务监控,业务部门可以及时发现并解决业务运行中的问题,减少业务中断和故障发生的概率,从而提升用户体验。

2.4 资源监控

资源监控的主要任务是对云计算环境中各种资源,如CPU、内存、存储等使用情况和可用性进行实时监控。通过收集和分析这些资源的使用数据,资源监控系统能够提供详细的资源使用报告和趋势分析,帮助信息管理部门了解资源的实际使用情况,以及是否存在资源浪费或资源瓶颈等问题。在实时监控的基础上,资源监控系统还能够及时发现资源不足以及资源被滥用等问题,当系统检测到某个资源的使用量接近或超过其容量限制时,它会立即发出警报,提醒管

理员采取相应的措施,如增加资源容量、优化业务负载等^[5]。同时,资源监控系统还能够监控资源的滥用情况,在这种情况下,系统可以采取限制资源使用、隔离问题用户或应用程序等措施,以确保资源的公平分配和高效利用。除了及时发现和解决问题外,资源监控还能够进行资源的分配和优化。通过分析资源的使用数据和业务负载情况,资源监控系统可以预测未来的资源需求,并提前进行资源的分配和调度。这不仅可以避免资源的过度浪费和瓶颈问题,还可以提高系统的响应速度和可靠性,从而提升用户体验和业务效率。通过实时监控和管理各种资源的使用情况和可用性,资源监控系统能够确保系统的稳定运行和高效资源利用,为单位的发展提供有力的支持。

3 云计算环境中大数据的审计技术研究

3.1 数据完整性审计

在云计算环境中,大数据的审计技术研究对于确保数据的安全性和完整性至关重要。特别是在数据完整性审计方面,对数据源进行验证和跟踪数据变化历史是不可或缺的两个环节。在云计算环境中,大数据来源于多个不同的数据源,包括内部系统、外部合作伙伴以及公共数据集等,为了确保数据的真实性和可靠性,审计系统必须能够对数据源进行严格的验证,这包括确认数据源的身份、检查数据源的授权和访问控制机制,以及验证数据的完整性和一致性等,通过数据源验证,可以确保存储在云平台上的大数据是真实可靠的,为后续的数据分析和应用提供坚实的基础。在云计算环境中,大数据的存储和传输往往是动态和频繁的。因此,审计系统必须能够跟踪数据在云平台上的变化历史,确保数据的完整性和可追溯性,通过记录数据的创建、修改、删除等操作历史,审计系统可以及时发现数据异常和潜在的安全风险,如数据篡改、非法访问等。同时,数据变化跟踪还可以帮助管理员了解数据的使用情况和趋势,为数据管理和优化提供有价值的参考信息。通过数据源验证和数据变化跟踪等技术手段,可以确保存储在云平台上的大数据的真实性和完整性,为机构的数据安全提供坚实的保障。

3.2 访问控制审计

随着数据量的不断增长和云计算服务的广泛应用,如何有效地管理用户权限、监控和记录用户的访问行为,以及及时发现并报告异常行为,成为信息管理部门关注的焦点。审计系统应能够精确地定义和管理用户对大数据的访问权限,意味着系统需要建立严格的权限控制机制,确保只有经过授权的用户才能访问和操作特定的数据资源,通过细粒度的权限设置,系统可以限制用户对数据的访问范围、操作类型和时间等,从而有效防止数据泄露和滥用。审计系统应能够实时监控和记录用户的访问行为,包括记录用户的登录信息、访问时间、访问路径、操作内容等。通过记录这些信息,系统可以追溯用户的操作历史,了解数据的使用情况,

并发现任何潜在的安全风险。同时,这些数据还可以用于生成用户行为分析报告,为决策层提供更深入的数据洞察和决策支持。审计系统应能够识别并报告任何异常或可疑的访问行为,包括未经授权的访问、异常频繁的访问、非工作时间的访问等。通过及时发现这些异常行为,系统可以迅速采取应对措施,如限制用户访问、触发警报通知等,从而防止潜在的安全威胁。通过用户权限管理、实时监控和记录用户访问行为以及异常行为检测等手段,审计系统可以确保只有授权用户才能访问和操作数据,并及时发现和应对潜在的安全风险。

3.3 日志审计

一个高效的日志审计系统不仅能够收集云平台上的各种日志数据,还能进行深入的分析和审计,从而及时发现并解决潜在的安全问题。云平台上的系统日志、应用日志、安全日志等包含了丰富的运行信息和安全事件数据,一个全面的日志审计系统需要能够实时收集这些日志数据,并进行分类、存储和备份,通过收集这些日志数据,机构可以全面了解系统的运行状况和安全状况,为后续的分析 and 审计提供数据支持。在收集到日志数据后,审计系统需要利用先进的分析技术和算法,对日志数据进行深入的分析和挖掘,通过分析,系统可以识别出各种安全事件,如未授权访问、数据泄露、恶意攻击等。同时,系统还可以对日志数据进行关联分析和趋势预测,发现潜在的安全风险和威胁。在识别出安全事件后,日志审计系统需要及时采取相应的应对措施,包括向管理员发送警报通知、启动应急预案、限制用户访问等。通过及时地响应和处理,可以迅速控制安全事件的扩散和影响范围,降低安全风险。通过收集、分析和审计云平台上的日志数据,信息管理部门可以及时发现并解决潜在的安全问题,保障系统的稳定运行和数据的安全可靠。因此,建立一个高效、全面的日志审计系统对于云计算环境的安全管理至关重要。

3.4 合规性审计

随着数据保护法规的日益严格和隐私保护意识的提高,合规性审计成为各类机构不可或缺的一项工作。云平台上的大数据涉及到用户的个人信息、商业机密等敏感数据,因此必须确保这些数据在使用、存储和传输过程中符合相关法规

和规定。审计系统应具备强大的法规遵从性检查功能,能够自动扫描和分析大数据,检查其是否符合数据保护法、隐私法等法规的要求,一旦发现数据存在不合规的情况,审计系统应立即报告并采取相应的措施,如数据脱敏、加密存储等,以确保数据的合规性。审计报告是评估大数据合规性状况的重要依据,也是机构向相关方展示其合规性管理能力的重要手段,审计系统应能够自动生成详细的审计报告,包括审计结果、建议改进措施等,这些报告应包含数据的来源、存储位置、访问权限、使用情况等关键信息,并对数据的合规性状况进行客观评估。通过审计报告,信息管理部门可以清晰地了解自身在大数据合规性管理方面的优势和不足,并据此制定改进计划和措施。通过法规遵从性检查和审计报告生成等功能,审计系统可以帮助信息管理部门确保大数据的合规性,降低合规风险,并提升单位在数据保护方面的形象和信誉。

4 结论

论文深入研究了云计算环境中大数据的实时安全监控与审计技术,有效应对了数据安全和合规性方面的挑战。通过系统、安全、业务和资源的全面监控,确保了大数据的稳定运行和严密防护。同时,数据完整性、访问控制、日志审计和合规性审计等技术的运用,进一步保障了大数据的完整性和合规性。这些研究不仅可以显著提升大数据在云计算环境中的安全性和可靠性,还为大数据的管理和应用提供坚实的技术基础。展望未来,我们将继续深化研究,为大数据的安全与合规保驾护航。

参考文献

- [1] 叶剑虹.大数据分析的制造系统实时安全监控机制平台[D].泉州:华侨大学,2022.
- [2] 陶宏桥.大数据时代下审计风险的影响因素及防范措施研究[J].中国乡镇企业会计,2024(3):166-168.
- [3] 欧雨晴.从传统审计到大数据审计:转型策略与路径探讨[J].现代审计与会计,2024(2):4-6.
- [4] 过艳雯.大数据、云计算技术对审计的影响[J].中国市场,2023(9):187-189.
- [5] 丁晓蓉.大数据审计环境中的审计技术与方法探析[J].财会学习,2023(4):97-99.