 DOI: https://doi.org/10.26549/bdai.v4i3.13878

Discussion on Network Security Audit Techniques for Big Data Environments

Chunchun Qu

Beijing Institute of Space Mechatronics, Beijing, 100020, China

Abstract

This paper aims to comprehensively analyze and summarize the network security in the big data environment. In the current Internet era, with the continuous expansion of data scale, network attacks are becoming more and more diversified, so the research on network security has important practical significance. With the rapid development of big data technology, network security audit under big data environment has become an important means to protect the security of information system. This paper reviews the network security audit techniques for big data environment.

Keywords

big data; network security; security audit; deep learning

面向大数据环境的网络安全审计技术综述

屈春春

北京空间机电研究所，中国·北京 100020

摘　要

论文旨在对面向大数据环境下的网络安全进行全面的分析和总结。在当前互联网时代，随着数据规模不断扩大，网络攻击也越来越多样化，因此对于网络安全的研究具有重要的现实意义。随着大数据技术的快速发展，大数据环境下的网络安全审计成为保护信息系统安全的重要手段。论文对面向大数据环境的网络安全审计技术进行了综述。

关键词

大数据；网络安全；安全审计；深度学习

1 引言

随着互联网的发展和应用场景的变化，数据规模不断扩大，而传统的安全审计方法已经不能够满足需求。因此，论文旨在提出一种新的基于深度学习的方法来实现对大数据环境中的数据进行安全审计。这种方法可以通过使用神经网络模型，自动识别异常的行为并给出相应的预警提示 [1]。

2 网络安全审计技术综述

2.1 网络安全审计技术

在当今信息化时代，随着互联网的发展和普及，网络安全问题日益突出。为了保障网络系统的安全性，网络安全审计技术成了不可或缺的一部分。网络安全审计技术是指对计算机系统进行全面而深入的检查，以发现并修复潜在漏洞的过程。它可以帮助企业和组织更好地保护自己的数据和隐私，提高网络系统的稳定性和可靠性。网络安全审计技术主要包括以下几个方面：一是网络流量分析，通过对网络中的所有数据流进行监控和分析，找出可能存在的攻击行为；二是端口扫描，通过对网络上的各个端口进行扫描，查找出是否存在未被授权的访问点；三是漏洞检测，利用各种工具和方法来探测网络中存在的漏洞，及时修复漏洞以增强网络的安全性。

此外，还有一些其他的网络安全审计技术如入侵检测、恶意软件检测等等。网络安全审计技术的应用范围非常广泛，不仅适用于大型企业的 IT 部门，也适用于个人用户。对于企业来说，网络安全审计技术可以帮助他们识别和预防黑客攻击、病毒感染等问题，确保公司的业务稳定运行；对于个人用户而言，则可以通过网络安全审计技术来保护自己在网上使用的隐私和财产安全。总之，网络安全审计技术已经成为现代社会中不可忽视的重要组成部分之一 [2]。

2.2 网络安全审计技术与入侵检测技术的关系

在当今信息化社会中，随着互联网的发展和应用范围不断扩大，网络安全问题也日益突出。为了保障计算机系统的安全性，需要采用一系列的技术手段进行监控和管理。其中，网络安全审计技术是一种重要的工具。而入侵检测技术

【作者简介】屈春春（1986–），中国北京人，本科，工程师，从事计算机网络安全与人工智能服务研究。

则是一种针对攻击者行为的研究方法，主要用于发现潜在威胁并采取相应的防御措施。因此，网络安全审计技术与入侵检测技术之间存在着密切关系。一方面，网络安全审计技术是实现入侵检测技术的重要基础。通过对系统中的数据流进行分析，可以识别出异常的行为或漏洞，从而为入侵检测技术提供可靠的数据支持。另一方面，入侵检测技术也可以作为网络安全审计技术的一部分，用来监测和控制访问权限以及用户的行为，以防止恶意软件的传播和黑客攻击事件的发生。总之，网络安全审计技术和入侵检测技术相互依存、相辅相成，共同维护了计算机系统的安全性。

2.3 数据挖掘技术

在大数据环境下，数据挖掘技术已经成为网络安全审计的重要手段之一。数据挖掘是一种从大量数据中提取有用信息的技术方法。它可以帮助我们发现隐藏在数据中的规律和模式，从而提高我们的分析能力和预测准确性。在网络安全审计领域，数据挖掘技术可以用于检测异常行为、识别恶意软件、监测攻击流量等方面。首先，数据挖掘技术可以通过对大量的网络日志进行处理来实现异常行为检测。通过对日志中的 IP 地址、时间戳、HTTP 请求等特征进行统计和分类，我们可以快速地找到一些可能与攻击有关的数据点。其次，数据挖掘技术还可以用于识别恶意软件。通过对已知恶意软件的行为特征进行建模和训练，我们可以建立一个模型来判断新的未知病毒是否是恶意软件。最后，数据挖掘技术也可以用于监测攻击流量。通过对攻击流量的特征进行分析和分类，我们可以了解攻击者使用的工具和策略，并采取相应的防御措施。总之，数据挖掘技术作为一种重要的网络安全审计手段，具有广泛的应用前景和发展空间 [3]。

3 大数据环境下的网络安全审计技术

3.1 大数据环境下的网络安全审计框架

在大数据环境中，网络安全审计技术面临着新的挑战和机遇。随着互联网的发展和数据量的不断增加，传统的安全审计方法已经无法满足需求。因此，针对大数据环境下的网络安全审计问题，需要建立一个全新的框架来进行分析和评估。首先，我们需要明确大数据环境下的网络安全审计的目标和范围。其次，我们可以通过对现有的数据库和应用程序进行深入挖掘和分析，以获取更多的信息和洞察力。最后，我们还需要考虑如何将这些信息整合在一起，形成一个完整的安全审计报告。在这个过程中，我们需要注意数据隐私保护等问题，确保我们的工作不会侵犯他人的利益。

总之，大数据环境下的网络安全审计是一个复杂的过程，需要综合运用多种技能和工具来完成。在未来的研究中，我们将继续探索更加高效和准确的方法来实现这一目标。

3.2 大数据环境下的网络安全审计流程

在大数据环境中，网络安全审计需要遵循一定的流程。首先，需要对企业进行全面的风险评估和漏洞扫描，以确定潜在风险点并制定相应的防范措施。其次，需要建立完善的数据备份机制，以便于数据恢复和分析。此外，还需要加强员工培训和意识教育，增强员工的安全意识和技能水平。最后，需要定期开展安全测试和监控工作，及时发现问题并采取相应措施加以解决。在实际操作中，大数据环境下的网络安全审计流程应该更加细致和科学化。例如，可以采用自动化工具来辅助审核过程，减少人工干预的时间和成本。同时，也可以通过云计算平台实现跨地域协同监管，提高效率和准确性。总之，大数据环境下的网络安全审计流程是一个复杂的系统工程，需要充分考虑各种因素的影响和制约条件，才能够取得更好的效果。

3.3 大数据环境下的网络安全审计方法

在大数据环境中，网络安全审计的方法也发生了很大的变化。传统的网络安全审计主要依赖于对系统进行手工检查和分析，但这种方式已经无法满足现代复杂的数据处理需求。因此，大数据环境下的网络安全审计需要采用更加高效、准确的技术手段来实现。首先，大数据环境下的网络安全审计需要借助人工智能技术。通过利用机器学习算法和深度神经网络模型，可以自动识别异常行为并快速发现潜在威胁。这种自动化的方式不仅能够提高检测效率，还可以减少人工干预的机会。其次，大数据环境下的网络安全审计还需要结合云计算技术。云计算提供了大规模的数据存储和计算能力，可以在短时间内完成大量的数据分析任务。同时，云平台上的虚拟化技术也能够提供高可用性和低成本的优势，为企业提供更可靠的服务保障。最后，大数据环境下的网络安全审计还需考虑隐私保护问题。由于大数据环境下的大量个人敏感信息被收集到一起，如何保证这些信息不被滥用或泄露至关重要。因此，必须采取有效的加密技术和访问控制措施来确保数据的安全性和保密性。

3.4 大数据环境下的网络安全审计工具

在大数据环境中，网络安全审计的技术和方法也发生了很大的变化。传统的网络安全审计主要依靠人工分析的方式进行，但是随着数据量的增加以及复杂性不断提高，这种方式已经无法满足需求了。因此，大数据环境下的网络安全审计需要借助先进的技术手段来实现。目前，大数据环境下的网络安全审计工具主要包括以下几种：

①自动化扫描工具：自动化扫描工具可以对大量的数据进行快速筛查，从而发现潜在的风险点。这些工具可以自动化地执行各种测试程序，以检测系统中的漏洞和弱点。例如，一些常用的自动扫描工具包括 Nessus、OpenVAS、Metasploit 等。

②机器学习算法：机器学习算法是一种基于统计学的方法，通过训练模型来自动识别模式并预测结果。在大数据环境下的应用中，机器学习算法可以用于风险评估、异常检测等方面。例如，利用机器学习算法可以建立一个智能监控系统，以便及时发现可能存在的威胁。

③深度学习算法：深度学习算法是近年来兴起的一种人工智能技术，它能够从大量数据中学习规律和特征，进而做出准确的预测或决策。在大数据环境下，深度学习算法可以用于攻击样本分类、恶意软件检测等方面。

④云计算平台：云计算平台是指一种按需获取计算资源的服务模式。在这种情况下，用户可以在云端使用虚拟机或其他资源进行工作。对于网络安全审计来说，云计算平台提供了高效率的数据处理能力和高可靠性的支持。

⑤区块链技术：区块链技术是一种去中心化的分布式账本技术，其特点是不可篡改性和安全性高等。在大数据环境下的应用中，区块链技术可以用于身份认证、交易记录等方面。总之，大数据环境下的网络安全审计工具具有多种多样的特点和应用场景，它们为网络安全审计带来了新的机遇和发展空间。

3.5 大数据环境下的网络安全审计评价

在大数据环境下，网络安全审计的技术和方法也发生了很大的变化。传统的网络安全审计主要关注的是系统中的漏洞和弱点，而大数据环境下的网络安全审计则更加注重数据的质量和安全性。因此，大数据环境下的网络安全审计需要考虑以下几个方面：首先，大数据环境中的数据质量是一个非常重要的问题。由于数据量庞大且复杂多样，数据的质量问题可能会对整个系统的稳定性产生影响。因此，在进行网络安全审计时，必须特别注意数据的质量问题，包括数据完整性、准确性和可靠性等方面。其次，大数据环境中的数据隐私也是一个非常关键的问题。随着人们个人信息保护意识的不断提高，越来越多的人开始重视自己的隐私权。因此，在进行网络安全审计时，必须特别注意数据隐私问题，确保用户的信息不会被泄露或者滥用。最后，大数据环境下的网络安全审计还需要考虑到数据的可视化和分析能力。因为大数据中包含了大量的非结构化的数据，所以对于这些数据进行有效的分析和可视化是非常重要的。

4 结语

论文对面向大数据环境的网络安全审计技术进行了综述，通过对不同技术的分类和应用案例的展示，展现了这些技术在保护信息系统安全方面的重要性和应用前景。随着大数据技术的不断发展，网络安全审计将成为保护信息安全的关键环节。未来，随着人工智能、区块链等新技术的应用，面向大数据环境的网络安全审计技术将迎来更多的挑战和机遇。

参考文献

[1] 钱明.基于大数据分析的网络安全审计技术的研究[D].北京:北京邮电大学,2018.

[2] 刘国城.基于大数据的互联网安全审计过程建模研究[J].兰州学刊,2018(3):12.

[3] 丁晨.大数据和人工智能技术在银行网络安全风险管理中的实践——日志安全审计分析业务[J].中国信息化,2019(5):3.