 DOI: https://doi.org/10.12345/bdai.v5i3.17400

Risk Assessment and Prevention of Information System Security Based on Big Data

Qingxiang Song[1] Ying Xu[2]

1. Jinan Real Estate Registration Center, Jinan, Shandong, 250000, China
2. Jinan Transportation Comprehensive Administrative Law Enforcement Detachment, Jinan, Shandong, 250000, China

Abstract

The rapid development and widespread use of big data have made its security risks increasingly prominent. This project is based on big data to evaluate and prevent security risks in information systems. Firstly, in-depth research has been conducted on issues such as data leakage, privacy breach, and malicious attacks in the big data environment. On this basis, a threat assessment model based on network attacks was proposed and analyzed. Secondly, research was conducted on data encryption, access control, and identity authentication in the big data environment. Finally, a summary of the existing problems in the research was made, and prospects for future research were presented.

Keywords

big data; information system; safety precautions measure

基于大数据的信息系统安全风险评估与防范

宋庆祥[1] 徐莹[2]

1. 济南市不动产登记中心，中国·山东 济南 250000
2. 济南市交通运输综合行政执法支队，中国·山东 济南 250000

摘 要

大数据的迅猛发展与广泛使用，使得其面临的安全风险问题日趋突出。本课题以大数据为基础，对信息系统的安全风险进行评价和预防。首先，针对大数据环境下的数据泄漏、隐私泄露、恶意攻击等问题，对其进行了深入的研究。在此基础上，提出了一种基于网络攻击的威胁评估模型，并对其进行了分析。其次，对大数据环境下的数据加密、访问控制、身份认证等进行了研究。最后，对现有研究中存在的问题进行了总结，并对今后的研究进行了展望。

关键词

大数据；信息系统；安全预防措施

1 引言

在信息技术飞速发展、信息化程度日益加深的今天，大数据已成为推动信息系统发展的重要因素。大数据具有对海量数据进行有效处理并从中挖掘有用信息的能力，已在金融、医疗、零售、交通运输等多个行业得到了广泛的应用。大数据的广泛应用，在为企业提供基于数据的决策支撑的同时，也给用户提供了更为个性化和智能化的服务体验。

大数据也给信息系统的安全带来了严峻的挑战。大数据时代的到来，给信息系统带来了更多的安全隐患，如数据泄漏、隐私泄露、恶意攻击等。这将会引起个人隐私、公司数据的泄露，甚至危及国家安全。因此，对大数据信息系统进行安全风险评价和防控具有十分重要的意义。

本项目拟对大数据信息系统的安全风险进行评价和预防，并对其关键技术进行深入研究。本项目拟在深入剖析现有安全隐患及危险因子的基础上，综合现有的安全评价与防护手段，以期为中国大数据信息系统的安全、稳定运行、数据安全与隐私保护等方面的研究与应用提供理论依据与技术支撑。

2 大数据信息系统安全风险分析

2.1 安全威胁与风险因素

大数据环境下的安全隐患及其影响因素研究是当前信息安全研究的热点。

首先，大数据环境下的数据泄漏是一个严峻的安全问题。随着大数据量的持续增加，数据泄漏所造成的损失日益严峻。大数据环境下存储了大量的个人信息，如个人身份信息、财务信息、商业秘密等，一旦数据被泄漏，将给社会带

【作者简介】宋庆祥（1979–），男，中国山东临沂人，硕士，高级工程师，从事数据结构和数据整理、数据分析模型构建、大数据应用、信息系统建设研究。

来巨大的经济损失。例如，有几家著名的公司就因为顾客信息被窃取而被索赔，而且公司的信誉和信誉也受到了很大的影响 [1]。

其次，大数据环境下的数据隐私泄露问题也是该领域所面临的又一重大安全隐患。大数据时代，个人隐私被不断收集、分析、使用，从而引发了隐私侵害。例如，在社交网络、电商平台等大数据环境下，用户的行为轨迹、偏好等隐私信息会被用来进行精准的广告投放、用户画像的构建，这将会导致用户的隐私泄漏、个人信息的安全性等问题，进而对用户的个人权利与信息自主性产生重大影响。

最后，网络中的恶意攻击也成为大数据环境下的一项重要安全隐患。恶意攻击是指各类网络攻击、恶意程序攻击等，它会造成大数据服务中断、数据篡改和窃取等严重后果。例如，黑客可能会透过系统的脆弱性与弱点，取得使用者的系统许可，篡改资料，甚或敲诈企业。此外，DDoS(Distributed 拒载服务) 攻击还会消耗系统的资源，从而影响系统的正常运作，带来巨大的经济损失与社会动荡 [2]。

总体而言，大数据环境下，数据泄漏、隐私泄露、恶意攻击等是大数据信息系统面临的主要安全隐患。要有效地防范网络攻击，必须从强化数据的加密和隐私保护、建立完善的访问控制机制、提高系统的安全性等方面入手。要保证大数据信息系统的安全、稳定运行，维护用户利益和数据安全，必须建立一套科学、高效的安全风险评估和预防方法。

2.2 安全威胁建模与分析方法

针对大数据环境下的安全问题，提出了一种新的、有效的、可扩展的、具有广泛应用前景的安全威胁模型。

首先，威胁模型是一种系统的手段，它可以发现并刻画出潜在的安全威胁，并对其所带来的危害进行分析。目前主要的威胁建模方法主要有威胁模型（STRIDE、DREAD）、攻击树分析、威胁智能分析等。通过对威胁模型的研究，我们能够更加全面、深刻地认识到系统所面临的各种威胁，并据此提出有针对性的安全保护策略与措施。

其次，漏洞扫描器是一种能够发现并发现系统中的安全缺陷与薄弱环节的自动工具，其中包括软件缺陷、配置错误、非法存取路径等。常见的攻击检测工具有网络总线、开放 VAS、N 地图等。在此基础上，提出了一种新的安全攻击方法，即利用漏洞扫描技术，对系统进行周期性的安全扫描与探测，并能及时地发现并修补可能存在的安全缺陷，从而提高系统的安全性与稳定性。

再次，提出了一种基于风险评价的方法，即风险评价矩阵，它可以对企业所面对的安全威胁与风险做出定性与定量的分析，进而制定出应对策略与优先权。风险评价矩阵是对安全威胁进行建模与分析的关键，它有助于决策者了解系统所面对的安全威胁，并采取相应的安全对策与措施，将其造成的损失降到最低。

最后，在此基础上提出了一种基于网络攻击的威胁建模技术，基于网络攻击的漏洞扫描技术，以及网络攻击的风险评价模型。本项目的研究成果将有助于系统管理人员以及安全人员对其所面对的安全威胁有一个较为全面、深刻的认识，并能对其进行有效的检测与处理，从而提高系统的安全性与稳定性，从而保证大数据信息系统的正常运转与用户数据的安全性。

3 大数据信息系统安全防范措施

3.1 数据安全保护技术

针对这些问题，提出了一种新的解决方案。

首先，为了保证数据在存储、传输、处理等各个环节不受非法存取和篡改，必须采用数据安全防护技术。其中，资料加密是一种常见的资料安全防护方法，它将资料经过加密变换，以防止非授权使用者直接读取或破译资料。密码学有两大类，一种是利用同一密钥来加密、解密，一种是利用公开、私有密匙进行加密、解密，以保证数据的保密性与完整性。此外，为了减少信息泄漏的危险，还采用了一种将数据隐藏或替代的方法。数据屏蔽是指数据脱敏、数据匿名化等技术，它可以在确保数据可用的前提下，对数据的隐私和安全进行有效的保护。

其次，在大数据环境下，如何对用户进行访问控制和身份验证，是保障大数据信息系统安全的关键。在此基础上，提出了一种有效的访问控制方法，即在一定程度上限制了用户对系统资源、数据的访问，从而避免了非授权用户或恶意攻击者获得了系统中的重要信息。其中，基于角色的访问控制（RBAC）、基于策略的访问控制（ABAC）等。而身份认证是一种对用户进行身份认证的重要手段，其主要包括密码认证、生物特征认证、多因子认证等。

最后，在此基础上提出了一种基于网络安全技术的大数据信息系统安全防护技术。通过本项目的研究，可以有效地保护大数据系统中的数据安全与隐私性，避免非法存取与恶意攻击，从而保证大数据信息系统的正常运转与用户数据的安全。在实施过程中，要根据系统的安全性要求及特性，选用适当的安全保护手段，构建一个健全的安全管理系统，持续提高系统的安全性 [3]。

3.2 访问控制与身份认证

在大数据环境下，用户的访问控制和身份验证是保障数据安全的关键。

一方面，存取控制策略是一种策略性的安全手段，它可以有效地控制系统的资源及数据的存取。在此基础上，提出了一种基于用户身份、角色和权限的方法来实现对用户或系统处理的访问要求的方法。在此基础上，提出了一种新的安全机制，即在一定程度上保证了系统的安全稳定。常用的存取控制策略有：基于角色的存取控制（RBAC）、策略式的存取控制（ABAC）等，这些存取控制可根据具体的环境与安全要求来选取与配置，以提升系统的安全性与可控性。

另一方面，双因子认证是一种增强型的身份认证方法，它能够在同一时间对用户进行双重或多重身份元素的鉴别，从而提升了系统对用户真实度的鉴别能力。常用的双因子鉴别方法有密码鉴别和生物识别，密码鉴别和移动电话认证。双因子认证技术相对于传统的单一因子认证模式，在安全性、可靠性等方面都有很大的提高，能够有效地防范密码泄漏、伪造身份等方面的隐患。在大数据环境下，利用双因子认证可以有效地保护用户的身份，减少非法接入的危险，提升整个系统的安全性。

因此，在大数据环境下，对用户进行访问控制和身份验证是一项非常重要的工作。本项目拟通过构建合理的访问控制机制，实现对系统资源与数据的严格限定，并引入双因子认证机制，增强用户的身份验证能力，从而实现对大数据信息系统的非授权访问与恶意攻击，保障大数据信息系统的安全性与稳定性。在实际应用过程中，必须针对不同的安全要求和特征，采用适当的访问控制和身份验证方法，构建一个完整的安全管理系统，以提高整个系统的安全性。

3.3 异常检测与应急响应

在大数据环境下，异常发现和突发事件应对是一个非常重要的问题。

其一，我们提出了一种新的方法来发现网络中存在的不正常的行为。其表现形式可以是非授权存取、不正常的资料传输、不正常的系统作业等。要想及时地发现并预防网络中的异常行为，就必须依靠基于规则的检测、机器学习的检测和行为分析等技术。本项目提出了一种基于分布式电源的分布式电源管理方法，通过对其运行状态的监测与分析，实现对其运行状态的实时监测与分析，并在此基础上提出相应的预警与阻止措施，以保证系统的安全稳定运行。

其二，安全事故应对机制是针对系统中出现的安全事故进行应急处置的一种机制。大数据环境下，系统规模大，数据量大，安全事故频发，对其进行有效的应对显得尤为重要。安全事件应对机制由预警体系、事件应对流程、应急队伍等组成，其目的是对安全事件进行快速发现、评估和处置，将安全事故对系统的危害降到最低。在构建安全事件应对机制时，要充分考虑到系统的安全性要求与特性，制订一套完整的事件应对方案，并进行应急演练，以保证一旦出现了安全事故，就可以快速、有效地应对，减少系统的损失。

因此，在大数据环境下，异常行为识别和突发事件应对是一个非常重要的问题。在此基础上，提出了一种新的基于网络的、可扩展的、可持续的、动态的、可预测的、可执行的、可维护的、有效的、可控制的、可操作的。同时，构建完善的安全事故反应机制，能够在突发事件中快速做出反应，将事故造成的损失降到最低。在实际应用中，还需对异常检测及紧急应对机制进行持续改进与优化，提升其安全防御能力，保证其安全稳定运行。

4 大数据信息系统安全评估与防范实践

大数据信息系统的安全性评价和防护技术是保证大数据信息系统安全性的主要途径。本项目的研究成果将全面、深入地挖掘网络安全隐患，提高网络的安全性水平，提高网络的安全性水平。在具体的实施过程中，通过对安全风险的分析、漏洞的扫描、策略的制定、应急预案的演练等一系列的技术手段来实现。一是在对网络安全风险进行分析的基础上，对网络安全隐患及风险因子进行了深入的分析，确定了网络的安全性要求及优先防护目标。二是采用漏洞扫描技术，对整个系统进行全方位的扫描与探测，及时发现并修补系统中的安全漏洞，从而增强系统的安全与稳定。在此基础上，本项目将构建一套完整的访问控制、身份认证、数据加密等安全控制方法，以保证数据的安全性与隐私性。在出现安全事故后，进行应急处置演习，做到事前做好准备，迅速做出反应，将安全事故带来的损失降到最低。总而言之，大数据信息系统的安全评价和预防工作，是保证信息系统安全性的一项重要措施。在对其进行科学、高效的评价和预防措施的同时，还可以保证整个系统的安全性和稳定性，对各种安全隐患和风险进行有效的预防。

5 结语

大数据环境下，信息系统的安全性问题越来越突出，对其进行安全评价和防护具有十分重要的意义。本项目拟对大数据环境下的安全风险分析、安全防护措施、异常事件检测及应急处理展开全面研究，以期为大数据环境下的安全保护提供理论支撑与技术指导。但是，随着科技的进步、威胁的变化，信息系统的安全性还有很长的路要走。在今后的发展中，应加大对安全技术的研发和创新，不断提高中国的信息安全防御水平。在此基础上，还应加大法制建设和执法力度，建立起全社会的信息安全保护机制。在此基础上，形成一个安全可靠的大数据环境，为数字社会的可持续发展做出贡献。

参考文献

[1] 杨云.大数据和移动互联环境下个人信息安全风险与防范研究[D].苏州:苏州大学,2018.

[2] 汪迎春.大数据时代个人信息安全的风险分析与防范研究[J].信息系统工程,2022(7):16-19.

[3] 朱瑞超.大数据背景下网络信息安全风险与防范策略研究[J].科学与信息化,2019(15):2.