Scientific Journal of Information Engineering
Volume 11 Issue 2, 2023, PP. 1-4

Analysis and Research of Information Security Technology in Big Data Environment of the Digital Economy

Tengqiao He

School of Physics and Electronic Engineering, Sichuan University of Light and Chemical Industry, 644000, China

Email: 2075203801@qq.com

Abstract

With the rapid development of the digital economy and the widespread application of big data technology, the scale of global information exchange and data transmission continues to expand. The digital economy, based on internet, mobile communication, and the Internet of Things (IoT) technologies, leverages techniques such as big data analysis and artificial intelligence to drive innovation and development across various industries. However, this digital economy in the big data environment presents certain security risks and threats. Therefore, this article aims to conduct an in-depth analysis and research on information security technologies in the digital economy's big data environment, with the goal of providing guidance and recommendations for better safeguarding information security in the digital economy environment.

Keywords: Digital Economy; Big Data; Information Security; Technical Analysis

数字经济大数据环境的信息安全技术分析与研究

何腾峤

四川轻化工大学，物理与电子工程学院，四川宜宾 644000

摘 要：随着数字经济的迅速发展和大数据技术的普及应用，全球范围内的信息交流和数据传输规模不断扩大。数字经济以互联网、移动通信和物联网技术为基础，利用大数据分析和人工智能等技术手段，推动了各行各业的创新和发展。然而，这种数字经济大数据环境下存在着一定的安全隐患和威胁。基于此，本文将对数字经济大数据环境下的信息安全技术进行深入分析与研究，旨在为更好地保护数字经济环境下的信息安全提供指导和建议。

关键词：数字经济；大数据；信息安全；技术分析

引言

信息安全成为数字经济发展中一个重要问题。在数字经济大数据环境下，各种敏感信息和商业机密的泄露、篡改和盗窃现象频繁发生，严重威胁企业和个人的利益。例如，金融机构面临着网络欺诈、资金盗取等风险；电子商务平台存在用户信息安全的问题；物联网设备的连接和数据传输过程受到黑客攻击[1]。因此，需要对数字经济大数据环境下的信息安全技术进行深入分析与研究，以应对不断变化的安全威胁和挑战。

1 数字经济大数据环境下信息安全所面临的挑战

数字经济是指在信息技术的支撑下，以数字化为基础，以数据为驱动，通过互联网和其他数字化技术进行生产、交换和消费的经济形态。而数字经济大数据环境指的是在数字经济背景下，形成的以大数据为核心的信息生态系统；同时也是数字经济运行和发展所需的基础设施和支撑环境。在这样的背景之下，如何保障数据信息安全也面临着严峻挑战[2]。首先，随着数字经济的快速发展，数据量呈指数级增长，而这些

数据储存在各种云平台、移动设备和传感器等多个终端上，使得数据的安全性面临更大的风险。数据泄露[3]、数据丢失、黑客入侵、恶意软件攻击等安全事故对数据安全构成了巨大威胁。其次，由于数字经济大数据环境中数据流动迅速，数据交换和传输过程中存在很多安全漏洞。例如，传统的加密技术可能无法适应高速数据传输的需求，造成数据在传输过程中容易被窃取或篡改。同时，移动设备和物联网的普及也给数据传输带来了新的安全挑战，如无线网络安全、蓝牙和 NFC（近场通信）安全等。此外，此外，数字经济大数据环境中广泛采用人工智能和机器学习算法，这些算法的训练和应用过程中可能存在隐私泄露和数据滥用的风险。例如，恶意用户可以通过攻击机器学习算法来获取敏感数据，或者利用算法的弱点进行数据篡改和误导。

2 数字经济大数据环境下的信息安全技术分析

2.1 数据加密技术

数据加密技术在保障数字经济大数据环境信息安全中起到了重要的作用。它通过对敏感数据进行加密处理[4]，确保数据在传输和存储过程中的机密性和完整性。具体来说，可以采用对称加密算法和非对称加密算法对数据进行加密，而加密算法的选择则取决于对安全性的需求和计算效率。在数字经济大数据环境中，一般采用对称加密算法保护数据的机密性，采用非对称加密算法实现数据的机密性和身份验证。对称加密算法就是使用相同的密钥对数据进行加密和解密，常见的对称加密算法有 AES、DES 和 3DES 等。数据发送方和接收方在传输数据之前，需提前约定好密钥，确保密钥的安全性。而非对称加密算法就是使用一对密钥，分别是公钥和私钥。公钥可以自由发布给任何人，私钥则是保密的。发送方使用接收方的公钥对数据进行加密，只有接收方持有相应的私钥才能解密数据。常见的非对称加密算法有 RSA、DSA 和 ECC 等。

在数字经济大数据环境中，数据加密技术的应用可以保护敏感数据不被未授权的访问者获得。同时，密钥的安全管理和分发也是关键的一环。为了确保密钥的安全性，可以采用安全的密钥管理和分发机制，如密钥交换协议、公钥证书和密钥定期更新等。

2.2 访问控制与身份认证技术

在数字经济大数据环境中，访问控制和身份认证技术扮演着关键的角色，旨在保护数据的机密性和完整性，并限制未经授权的用户对数据的访问。这些技术是确保数据安全的重要手段。首先，访问控制策略是实时数据保护的基础。基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）是常见的策略。RBAC 通过将用户分配到不同的角色，并为每个角色分配特定的权限，来限制用户对数据的访问。ABAC 则根据用户的属性（如所属部门、职位级别等）来确定其访问权限。这些策略可以根据组织的需求进行灵活配置，确保只有具备适当权限的用户可以访问特定的数据。其次，身份认证技术用于验证用户的身份，并确保只有经过身份验证的用户才能获得数据访问权限。单因素认证是最基本的认证方式，通常包括使用用户名和密码进行验证。双因素认证引入了第二个验证因素，例如手机验证码或指纹扫描，以增加认证的安全性。而多因素认证则结合多个不同的验证因素，如指纹、面部识别、密码等，以提供更高级别的身份验证保护。这些认证技术有效地防止了未经授权的用户获取敏感数据。值得注意的是，在数字经济大数据环境中，随着技术的不断发展和安全威胁的不断演变，访问控制和身份认证技术也在不断演进和创新。例如，基于生物特征的身份认证技术（如指纹识别、虹膜扫描）和基于行为分析的访问控制技术（通过分析用户的行为模式来判断是否存在异常活动）等，都在提高数据访问安全性方面发挥着重要作用。

2.3 虚拟化技术

虚拟化技术在数字经济大数据环境下也扮演着重要的角色，它可以提供更高级别的信息安全保护和资

源管理。虚拟化技术主要包括服务器虚拟化、网络虚拟化和存储虚拟化。首先，服务器虚拟化通过将一台物理服务器划分成多个虚拟服务器，每个虚拟服务器都可以独立运行不同的操作系统和应用程序。这种虚拟化技术可以提高服务器资源的利用率，降低硬件成本，并且可以隔离不同的业务应用，增强安全性。通过服务器虚拟化，可以将不同敏感级别的数据隔离开来，确保数据之间的相互影响最小化，从而减少安全风险。其次，网络虚拟化可以将一个物理网络划分为多个逻辑网络，每个逻辑网络都能够独立配置和管理。网络虚拟化可以提高网络安全的隔离性，确保不同业务应用之间的网络流量互相隔离，防止未授权用户访问敏感数据。此外，网络虚拟化还可以实现虚拟专用网络（VPN）和虚拟局域网（VLAN）等安全机制，对数据传输进行加密和隔离，提高数据传输的安全性。最后，还可应用存储虚拟化将多个物理存储设备（如磁盘、固态硬盘等）组合成一个逻辑存储设备，提供集中式的管理和控制，实现数据存储的隔离和备份，确保数据的安全性和可靠性。此外，存储虚拟化还可以提供数据加密和访问控制等安全功能，保护敏感数据不被未授权的用户获取。

2.4 安全监控与日志审计技术

安全监控和日志审计技术是数字经济大数据环境下信息安全的重要组成部分。首先，安全监控技术通过实时监测网络流量、系统日志等信息，及时感知和识别潜在的安全威胁。它可以对网络中的异常流量和攻击行为进行监测、分析和应对，比如监测到病毒、恶意软件、网络入侵等，及时发出警报和采取相应措施进行阻止[5]。安全监控技术中常用的工具包括入侵检测系统（IDS）和入侵防御系统（IPS）。IDS 能够持续监测网络流量，并通过与已知攻击模式的比对来发现异常行为，及时预警并采取相应措施。而 IPS 在 IDS 的基础上增加了主动阻断功能，可以主动拦截和阻止恶意流量，提高网络安全防护效果。其次，日志审计技术通过收集和分析系统和应用程序的日志信息，能够对用户行为进行审计和分析，以发现潜在的安全问题。日志是记录系统和应用运行状态的文件，包含了用户的登录、操作和访问记录等重要信息。通过对这些日志进行审计，可以及时发现异常活动、非法操作或趋势性问题。日志审计技术能够帮助企业建立用户行为记录和快速恢复机制，对安全事件进行溯源和分析，帮助发现威胁来源和做出应对，从而提高信息安全的防护能力。

安全监控和日志审计技术的应用可以帮助企业及时发现处理潜在的安全事件，提高信息安全的保障水平。通过持续监测和分析，可以加强对网络环境的实时感知，准确识别安全威胁，并采取相应的阻断和排查措施。此外，日志审计技术还可以协助企业建立完整的安全审计与监管体系，促进数据合规性和安全管理的落地。

2.5 数据备份与恢复技术

在数字经济大数据环境中，数据备份与恢复技术是保障信息安全的重要手段。数据备份的目的是将数据复制到另一个存储介质上，以便在数据丢失或损坏时进行恢复。对于大数据环境来说，数据备份需要考虑数据量大、备份时间长的问题，因此需要考虑备份策略、技术的选用来提高效率。常见的备份策略包括完全备份、增量备份和差异备份。完全备份是将系统的所有数据都备份一次，适用于较小的数据集。增量备份只备份自上次备份以来发生变化的数据，可以减少备份所需的时间和存储空间。差异备份则仅备份自上次完全备份以来发生变化的数据块，比增量备份更加高效。此外，还可以采用分布式备份技术，将数据备份到多个地理位置或存储节点上，提高备份的可靠性和容错性。

3 未来发展趋势

在数字经济大数据环境下，信息安全技术的研究与实践仍然面临许多挑战和机遇。随着大数据的广泛应用，探索更加安全和高效的数据隐私保护方法成为主流，关注差分隐私、同态加密等，保护用户敏感信息。同时，致力于发展 AI 安全防御机制，如对抗性样本生成、模型鲁棒性增强等，以应对恶意攻击者可能

利用 AI 算法造成的威胁。

此外，对网络安全防护的关注也在不断增加。研究基于 AI 的网络入侵检测系统、软硬件协同防御等新技术和方法，以应对不断变化的网络攻击。以及探索安全的数据共享机制，如安全多方计算、区块链等，以确保数据在共享和分析过程中的安全性。另外，随着用户身份管理的复杂性增加，创新基于生物特征的身份认证技术、多因素身份验证等方法，提高身份管理的安全性和便捷性。

4 结语

综上所述，数字经济大数据环境下的信息安全技术对于保护数字经济发展和数据安全至关重要。随着科技的迅猛发展，我们面临着越来越复杂和智能化的网络安全威胁。只有不断跟上技术的步伐，掌握最新的安全技术和方法，不断探索和创新，抓住机遇，建立一个安全可信赖的数字经济环境，才能更好地保护用户的数据安全，推动数字经济的繁荣和可持续发展。

参考文献

[1] 陈敏儿. 大数据环境下信息安全问题及防范措施[J].网络安全技术与应用,2021(03):50-51.

[2] 张娜,侯雅楠. 数据隐私保护与信息安全问题研究[J].办公自动化,2023,(01):6-8.

[3] 唐金成,莫赐聪. 数字经济时代网络安全保险创新发展研究[J].西南金融,2022,(01):52-64.

[4] 基于大数据背景下隐私计算的网络安全技术应用探讨——评《大数据时代的隐私》[J].中国科技论文,2022,(11):13-14.

[5] 胡卿汉,何娟. 基于联盟链的供应链金融信息安全问题思考[J].物流科技,2021,(02):168-172.

【作者简介】

何腾峤（1999-），男，汉族，本科，电子信息工程，四川轻化工大学。Email：2075203801@qq.com