ISSN: 2661-3719(Print); 2661-3727(Online)

大数据技术在网络安全中的分析与应用

滑　敏
山东省邮电规划设计院有限公司　山东济南　250101

摘　要：现阶段，伴随着我国社会经济发展水平不断的提高，国内社会领域市场范围内部的各行各业都实现了高速的发展。当今社会是互联网信息技术快速发展并实现广泛应用的社会，社会领域市场范围内部的许多高新企业的崛起与互联网信息技术的发展密不可分，企业依托于快速发展的互联网信息技术并将这种快捷高效的网络系统应用到企业的日常经营管理当中，不但大幅扩宽了企业或许行业信息的渠道，同时也显著提高了企业的经营管理效率。
关键词：网络安全；大数据技术；信息储存

Analysis and application of big data technology in network security

Min Hua
Shandong Post & Telecommunications Planning & Design Institute Co. , Ltd. , Jinan 250101, China

Abstract: At the current stage, as China's socio-economic development continues to advance, various industries within the domestic social market have experienced rapid growth. Today's society is characterized by the rapid development and widespread application of internet information technology. The rise of numerous high-tech enterprises within the social market is closely intertwined with the development of internet information technology. These enterprises leverage the rapidly evolving internet information technology and incorporate its swift and efficient network systems into their daily business operations. This not only significantly expands the channels for accessing industry-related information, but also greatly enhances the efficiency of their business management processes.
Keywords: network security; Big data technology; Information storage

引言：

本品文章主要论述了关于网络安全分析工作领域中大数据分析技术的实际应用，主要通过理论与实践相结合的方式，不单分析了网络安全受到威胁的主要因素，研究如何将大数据分析技术应用到网络安全分析工作的技术途径，并在一定程度上伸出了我国大数据分析技术在网络安全分析工作的实际应用发展现状[1]。

一、大数据分析技术在网络安全分析工作领域中的应用优势

由于互联网信息技术在社会环境当中不断地发展，社会内部的信息总量不断地增加，尤其是针对社会领域内部整体的互联网信息系统而言，公司企业受到网络攻击的概率也大大增加，企业内部的信息安全性严重降低，而传统的安全分析技术已经无法良好地适应当前快速发展的互联网环境，因此其自身也无法有效地识别企业互联网系统内部的各个安全隐患和安全漏洞[2]。通过相关领域技术研究人员的实践分析，通过应用大数据分析技术，可以有效地实现大规模的互联网信息数据收集并同时对其所收集的信息数据进行分析与汇总，将这部分数据进行高效率的分类并分析这些数据信息的优点与特征，有效地识别企业互联网系统内部的安全隐患与安全漏洞，在我国当前发展阶段，社会领域网络空间的安全作为重要的国家安全要素，因此涉及网络安全分析领域工作的重要性不言而喻。

1.大数据分析技术的正确性

企业或者社会当中的互联网信息系统在日常的运转过程当中，通常会直接采用真数据流的形态进行一般的数据传输工作，而在大数据分析技术领域当中，针对互联网系统内部的真数据流的实际传输情况进行实时的记录，从而建立起系统化的真数据流分析模型，并通过对

真数据流的信息传输形态和已建成的分析模型进行比较研究，分析互联网系统中的数据信息匹配程度，进而得出互联网系统内部是否存在网络安全隐患[3]。

2.据分析技术的有效性

在大数据分析技术在网络安全分析领域的实际应用过程当中，除开其自身可以广泛地获取互联网系统内部的信息传输以及系统运行历史数据，大数据分析技术还可以利用互联网系统内部的云计算技术，实现快速的建立数据流的信息传输变化模式，由于其所建立的数据流变化模式对于信息存储机制的实际需求相对不高，在后续的实际应用过程当中，可以实现数据流的快速对比工作，从而有效避免了传统安全分析技术对于信息存储机制的要求过高的情况。而对于网络安全分析体系来讲，会用大数据分析技术进行相关的工作流程，其实际的工作效率更高，分析效果更精细化[4]。

二、据发展环境当中存在的网络安全威胁因素

1.网用户网络安全意识薄弱

在当前快速发展的互联网信息技术的影响之下，互联网信息技术已经在社会各领域实现了广泛的实际应用，但是从总体上来看，大部分人在日常生活中使用互联网相关产品的过程当中，对互联网系统安全问题缺乏正确的认识，互联网安全意识相对匮乏，并且一旦在日常生活中接触到互联网系统安全相关问题也不懂得如何进行正确的风险预防，因此导致社会环境内的网络系统安全性能整体不高，数据信息安全性较差[5]。虽然大部分计算机系统内部存在有关互联网系统安全相关的预设，并且具备一定的安全保密程序，具有基本的互联网安全性能，可以如果用户在日常的使用过程当中主动接触到包含网络病毒的软件，或者出于某些个人诉求解除了计算机预设的互联网安全保密程序，并且由于我国大部分用户在使用互联网系统的过程当中没有受过有关部门的正确指导，其遭受到网络攻击的可能性非常大，甚至可能会出现企业重要商业机密文件或者数据信息的泄漏以及损毁等等情况。

2.互联网空间当中隐匿的黑客与病毒

互联网系统在开发之初就是开放性质的，因此世界范围内大部分国家的互联网空间具有高度的社会开放性。社会当中的人们在使用互联网信息系统的过程当中很容易遭受网络黑客以及病毒软件的供给，从而导致自己的隐私数据或者企业关键商业机密泄漏，而且不同型号的计算机设备在接入到互联网系统的过程当中会产生各种各样不同的互联网信息安全问题和技术漏洞，因此尽管在互联网信息技术高速发展的今天，相关的互联网信息安全技术不断地更新，计算机科学技术水平不断突破，可同时相关技术的发展也为黑客以及病毒提供了发展的技术基础，互联网系统内部的信息环境也处在不断的发展变化当中，黑客网络攻击的迅速性、隐匿性，以及病毒软件的感染能力都在不断地提高，对计算机设备的使用者产生巨大的安全危害。因此，只要企业或者个人的计算机设备遭受黑客的网络攻击抑或是病毒感染，就很容易导致计算机内部的互联网信息系统被破坏，给企业或者个人带来不可估量的经济损失以及其他损失。

在互联网信息技术高速发展的现代社会，为了提高我国网络空间的安全性和运转稳定性，提高社会各个领域各个行业的互联网信息技术利用率和覆盖率，就需要从事互联网安全分析领域的技术工作人员加强对互联网空间内部黑客和病毒的抵御能力，减少其对于我国互联网空间安全性以及运转稳定性的威胁。

3.技术领域中存在的安全漏洞

计算机设备的互联网系统主要由设备内部的硬件与软件构成，除了移动硬盘等容易受到硬件破坏以及网络病毒的感染之外，计算机内部软件层面也存在许多网络安全漏洞，一旦计算机设备的使用管理人员无法及时的识别互联网系统当中代码编制的错误，将导致计算机设备所接入的互联网系统整体陷入网络安全风险当中，导致其更加容易遭受到互联网空间中的黑客攻击和病毒感染。从我国目前的社会互联网环境来看，互联网系统的应用模式整体的安全性能水平较低，一旦社会当中的计算机设备受到互联网黑客的非法侵入，相关的管理人员无法及时地排查并采取有效的化解措施，并且一旦对互联网黑客攻击拦截不及时，就很容易导致企业以及个人的商业机密信息以及隐私数据信息泄露，为企业或个人带来巨大的经济损失以及其他损失。

三、据分析技术在互联网安全分析工作领域的实际应用与发展

在当前大数据分析技术快速发展的时代背景影响之下，社会范围内的计算机设备安全问题已经逐渐引起企业管理人员以及有关部门的重视，计算机设备在接入到互联网系统并为社会的正常运转、企业市场的经营管理、居民日常的生活等等方面进行服务的同时，也带来了前所未有的互联网安全威胁。为了提高我国网络空间的安全性与社会互联网系统的运转稳定性，相关领域的技术研究人员应当有针对性地开展关于计算设备安全技术的深入研究与分析，为我国的计算机设备网络安全提供基

本的技术保障。

1.安全保密技术

目前世界范围内主流的计算机设备网络系统安全保密技术为RSA技术和DES技术，这两种技术作为重要的计算机网络系统安全保密技术为社会各领域的计算机设备的网络系统安全工作提供了基本的技术保障。

首先，RAS技术是在1987年提出的，并且经过长时间的发展与实际应用，经受了无数次各种不同类型的网络攻击的考验，现今依然被广泛地应用在社会各个领域各个行业当中，被从事网络安全相关工作的人员所认可。RAS算法虽然可以有效地域当前互联网空间当中绝大多数的基于网络密钥的黑客攻击，但是RAS算法对于存在密码加密情况的互联网安全保障性还是会受到网络密钥长短的影响，在技术层面和理论层面上来讲，只有确保网络密钥的长度足够长，在实际应用环节才能具备更高的安全性能。但是一旦网络密钥长度达不到基本要求，就很容易受到互联网黑客攻击的暴力且直接的穷举法破解。并且伴随着互联网信息技术进和计算机设备软硬件的不断发展与进步，以及分布式信息技术与量子计算机理论的不断完善，老牌RSA算法加密技术受到了巨大的技术挑战，其自身算法的安全性以及保密可靠性也越来越受到从业人员的质疑。

其次是DES密码算法技术，此技术在实际应用过程中对双方用户的协同合作要求较高，其算法技术的基本原理是当进行数据流的传输以及处理工作婚介，信息传输方和接收方必要共同使用对称密码，才能顺利地进行数据流的传输与接收工作。DES密码算法技术被广泛地应用于与金融相关的信息安全领域的互联网信息系统数据分析工作方面。

2.数据镜像与备份处理技术

伴随着大数据信息化发展时代的来临，社会范围内互联网空间中各类非法网络攻击以及黑客入侵以盗取企业商业机密信息和个人因素数据的情况时有发生，互联网空间内的数据信息安全形势日益严峻。将重要的文件信息资料进行备份处理，可以在计算机设备遭受到互联网黑客入侵或者病毒感染导致无法正常启动或者资料丢失的情况下，给企业的互联网信息系统正常运转以及重要信息找回工作提供可靠的数据支持。这种备份技术在社会范围内的企事业单位、公司内部、数据网络服务平台以及政府机关单位等等工作领域实现了广泛的应用，从而有效降低互联网黑客攻击以及病毒感染所造成的损失。

四、结束语

我国当前发展阶段，伴随着大数据信息化时代的来临，人们在工作生活中所遇到的诸多问题都可以依靠计算机互联网技术以及大数据信息技术有效地进行化解，从而摆脱了传统意义上的空间与时间的束缚，极大地促进了我国社会经济发展的速度。现如今，大数据分析技术在网络安全分析领域的实际应用，已经被广泛地应用于我国社会的各个领域各个行业之中，并且也成了我国社会实现进一步发展的重要方向。综上所述，国内从事互联网空间安全领域的工作技术人员应当提高对自身工作的重视，做好自身的互联网空间管理工作。

参考文献：

[1]李媛，鲁春燕.大数据技术在网络安全分析中的应用[J].网络安全技术与应用，2023（04）：71-73.

[2]孟卫娜.大数据技术在网络安全分析中的应用[J].科技与创新，2023（03）：159-161.

[3]狄晶晶.大数据技术在网络安全分析中的应用探究[J].网络安全和信息化，2022（11）：19-21.

[4]刘成.网络安全分析中大数据技术应用分析[J].网络安全技术与应用，2022（11）：49-50.

[5]高松涛，陈一鸣.网络安全分析中的大数据技术的有效应用[J].长江信息通信，2022，35（08）：137-139.