网络安全分析中的大数据技术应用

徐国涛*
中国石油化工股份有限公司天津分公司信息档案管理中心，天津 300271

摘　要：随着信息技术的不断发展，信息技术下的产物开始在各个领域中流行起来，它对人们的生活和工作都带来了极大的便利，既能更好地满足人们生活的日常所需，也能够使人们的工作更加高效地完成。但是，从目前的情况来看，我国的网络信息安全的状况存在一定的问题，对人们的安全产生一定的威胁。我国一直致力于此方面的工作，随着大数据技术的出现，对网络安全分析中出现的问题也提出了更好的解决策略。文章对大数据技术在此方面的应用进行研究，希望可以为网络信息安全保障提供借鉴。

关键词：大数据技术；网络安全；应用研究

一、引言

随着我国的信息科学技术不断发展，网络信息技术也得到了快速的普及，人们更多地关注网络安全问题的重要性。网络安全对于个人隐私有着直接的联系，同时会对国家的机密信息形成影响，由于大数据技术的不断成熟和发展，使得信息数量在不断呈现爆炸式的增长，这在很大程度上加大了计算机网络安全的管理难度，与此同时，这也对当前的网络安全模式提出了更多的发展空间。只有不断地加强对大数据的管理，才能更多地保证大数据网络信息的安全稳定发展。

二、概述

利用大数据技术能够对计算机网络存储的数据进行全面系统的分析，通过分布式算法，能够快速、准确、及时地找到网络安全隐患，并进行有效处理，避免安全隐患对网络运行安全造成伤害及威胁。在安全隐患尚未构成威胁或者伤害之前，就将安全隐患消除在萌芽状态，从而保证计算机网络能够长期、安全、稳定、可靠运行。而且还能对网络安全分析结果进行直观展示，判断安全隐患出现的规律和发展趋势，再结合实际情况对安全风险进行科学合理的规避及处理[1]。基于此，开展网络安全分析中的大数据技术应用探讨就显得尤为必要。

三、网络安全分析中大数据技术应用的意义

随着互联网的迅速发展，给人们提供了更多的生活便利，同时也给网络安全分析带来了更大的负担，具体表现在以下两方面。

第一，网络安全需要处理的数据量在不断地增多，并且数据的种类也呈现多种多样的趋势，这就需要结合多维分析法，才能产生更好的效果。

第二，随着数据量的增加和传输速度的加快，要完成对数据的有效分析，就必须提高对信息采集的速度，这无疑增加了网络安全分析的难度。

相比较传统网络安全分析系统而言，应用结构化的数据库，通过对数据储存，这种方式使得网络安全的运营成本增加，为了降低成本，通过对数据进行应对处理，降低数据的大小，提高储存的容量，但是这种方式一般会导致数据在处理过程当中出现丢失的情况，并且长时间储存信息也会造成数据的丢失，相比较传统的网络安全分析而言，在面对复杂的数据处理过程当中，不能充分地发挥好具体的作用，这种分析的速度和访问的效率都满足不了，当下的网络发展的需求[2]。

相比较而言，大数据技术对于当今的网络安全分析取得了以下较为明显的效果。

第一，大数据技术能够提升网络安全分析的数据储存量，对于复杂的非结构化的数据，大数据源能够保证效率的

* **通讯作者：**徐国涛，1987 年 3 月，男，汉，甘肃天水人，现任中国石油化工股份有限公司天津分公司网络管理，工程师，本科。研究方向：网络安全、信息安全。

前提下进行有效的分析，这就需要保证数据的完整性。

第二，在大数据技术的使用背景下，可以降低网络安全分析的运营成本。在这过程当中，会使用分布式的数据库，相比较传统的机构化的数据库而言，它相对经济实惠，并且对于硬件的要求比较低，在低要求的设备中进行数据分析，也能保证平稳运行，从而大大地降低网络安全分析系统的成本。

第三，在大数据技术下，最为显著的特点是能够保证网络安全分析系统的工作效率，在大数据技术下能够完成对非结构数据的储存以及处理这种数据储存以及访问的速度是非常快的，使得系统数据分析处理要求较高。

四、大数据技术在网络安全分析中的应用

（一）做好网络监管工作

网络安全监管部门需要切实做好网络监管工作，在充分重视网络安全监管的同时，对监管手段进行完善，建立起相应的安全防范系统，及时发现网络中存在的信息安全问题，采取有效措施进行防护和应对，进一步提升安全监管系统的预见性，将监管部门的职能充分发挥出来。管理人员应该重视对网络安全监管人员的培训工作，促进其专业能力的提高，在进行新人招聘的过程中，应该适当提高录用标准，正式入职前还应该做好岗前培训和考核，合格人员才能上岗。通过这样的方式，一方面能够提高员工对于网络安全监管工作的重视；另一方面则能够提高员工的专业能力，确保其能够通过对大数据技术的合理应用，做好网络安全防护[3]。

（二）用户行为不良信息治理

用户行为不良信息治理主要是利用Hadoop、HDFS、Pig、Hive等技术和网络结构，来搭建大数据分析平台，从而对用户行为不良信息数据进行采集，同时建立用户行为分析模型，并对用户异常行为进行分类。通过安全大数据分析平台可以将用户的行为数据输入到系统平台上来，精确获知用户使用计算机网络的异常行为特征。再以此为依据，建设多维度的用户画像数据库，为网络用户行为不良信息治理提供必要的参考和指导，通过大数据技术可对用户不良行为进行智能化识别。大量研究和实例表明，利用大数据分析技术能够挖掘出更多潜在的不完全行为和违规行为，能够对网络安全分析的现有制度和体系进行补充。此外，将大数据技术应用网络安全态势感知、恶意软件检测等方面，可大幅度提升网络安全分析效果，及时找到不安全因素和隐患，进行有针对性的治理，保证网络安全。

（三）信息的检索与数据分析

对于信息的检索，可以采用Map Reduce作为架构形式，在这个环节，通过进行检索的方式，对内容进行分析和归类，大幅度提升信息的检索能力，由此可见，大数据技术在信息检索方面有着很大的推动作用，比如企业要想在开会之前寻找相关的内容，作为参考，就可以利用大数据技术进行信息检索，在这个过程当中，可以根据国内外相应的检索技术和参考文献进行对比分析，从而寻找出竞争对手。与此同时，大数据技术能够对同行业的论坛信息进行收集整理，并且及时了解出消费者的潜在消费意识和需求，通过数据分析得出消费者的消费意向，通过准确地对网络公共信息的采集和整理，甚至在这种大数据的检索功能，挖掘出潜在客户的一些信息和资料[4]。

数据分析也是数据解析的一种，该技术利用HIVE方法对数据进行展开分析，使用SQL中HIVEQL语言使HDFS和HBASE可以对不能构成结构式的数据进行检索。此外，大数据技术下还能够利用Mahout达到以Hadoop为前提的机械研究所有数据能够进行深度挖掘与整理解析。例如，政府机关以及军队可以对信息进行实时跟踪，了解国内外的新闻数据，并且通过这个数据整理出这个地方的政策法规，以及经济产业的信息。通过利用大数据技术解决与因特网隔离重要部门对于因特网的信息问题进行实时的解决，针对政府网站的各地址，网站的信息进行采集和整理。

（四）关注情报分析技术

IPV4/IPV6网络数据包情报分析技术能够从海量数据流中，准确筛选出具备指定特征的数据包，配合PPM概率预测算法或者相应的模式匹配算法，能够找出数据中可能存在的安全隐患。网络数据交换环节，必须遵循一定的规则和格式，这里的规则和格式主要是指网络协议，计算机网络可以分为多个不同的层级，而从保障不同体系计算机网络跨平台互联的角度，国际上提出了OSI模型，将网络分成七个层次，自上到下依次为应用层、表示层、会话层、运输层、网络层、设计链路层以及物理层[5]。IPV4/IPV6网络数据包情报分析技术可以在TCP/IP模型中实现，在对数据包进行组装的过程中，需要依照从上到下的顺序，针对每一层的协议进行封装处理，处理环节需要加上协议首部；在对数据包进行解析的过程中，应该反过来，依照从下到上的顺序，将数据包中的各层协议剥离。

五、结束语

采用理论结合实践的方法，探讨了网络安全分析中的大数据技术应用，探讨结构表明，在“互联网+”技术、云计算技术等愈发成熟的背景下，计算机网络在运行面临的威胁五花八门，为网络安全分析、网络安全监督管理、违规不良信息治理等构成了极大威胁。传统网络安全分析技术已经难以满足时代发展要求。而大数据技术是随着信息技术、网络技术发展而来的新型技术，具有与时俱进的优势，能够对网络安全威胁进行全面分析，从而保证网络的安全性。

参考文献：

[1]张宝飞.浅议网络安全分析中大数据技术应用[J].农村.农业.农民(B版), 2020(04):55-56.
[2]高娜.网络安全分析中的大数据技术应用[J].无线互联科技, 2020,17(19):151-152.
[3]毛乾旭.网络安全分析中的大数据技术运用探析[J].计算机产品与流通, 2020(05):76.
[4]崇阳.网络安全分析中的大数据技术应用分析[J].内蒙古科技与经济, 2020(20):77-78.
[5]周文.网络安全分析中的大数据技术应用研究[J].国际教育论坛, 2020,2(4):21.