大数据技术在网络安全分析中的应用

朱常乐

（西安翔迅科技有限责任公司　陕西　西安　710000）

[摘　要]近年来，社会发展迅速，我国的网络行业建设的发展也有了提高。信息技术普及的时代，各种信息技术从应用领域的需求出发不断升级。面对网络环境中产生大量的数据，要做好安全分析工作，就要应用大数据技术。大数据作为数据分析、处理的工具，其所发挥的优势在于，能够在海量的数据信息中提取有价值的信息，对于不良信息作出准确的判断，因此对网络安全的判断提供有效的数据信息。本文主要从网络安全分析以及大数据技术应用进行介绍，提出大数据技术所具备的优势，进而浅析网络安全分析中应用大数据技术的流程。

[关键词]大数据技术；网络安全分析；应用

【DOI】10.12252/j.issn.2096-6261.2019.12.065

引言

随着技术的不断发展，人们越来越意识到计算机安全在工作与生活中的重要性。在计算机的使用过程中，用户虽然采用了各种方式以防止出现网络问题，但还是会出现很多问题需进行不断优化。

1 大数据时代加强网络安全的必要性

1.1提升数据的精准性

大数据时代下计算机网络安全扮演着十分重要的角色，能在一定领域中发挥越来越重要的作用。相较于传统的信息处理方式而言，大数据背景下的信息处理工作更具规模性、系统性、专业性，能从数据的来源、范围、数据的处理方式及后续维护等角度进行信息分析。从某种意义上说，大数据时代信息技术将信息处理工作摆在极其重要的位置，从而有效提升数据的准确性。而提升数据的准确性不仅需计算机网络平台的计算能力，而且需结合计算机网络安全技术，只有两者双管齐下，才能从不同角度保证数据的准确性。

1.2提升大数据平台服务水准

传统网络时代并未将计算机网络安全摆在十分关键的位置，导致很多用户及专业人士并未过度关注相关方面内容。大数据时代将网络安全放在十分重要的位置，对大数据平台提出很高标准和要求。大数据平台是储存信息的工具，用户可以根据自身需求选择相对应的内容，这就能在很大程度上体现数据平台的服务水准。随着用户不断增多、需求不断多样，为数据平台的服务水准带来全新的挑战，要尽可能地满足不同用户的不同需求。

2 网络安全分析中应用大数据技术所发挥的优势

2.1网络安全分析中应用大数据技术分析资料更加详实

当网络运行中存在安全问题的时候，其中所涉及的因素很多，所有与网络相关流程节点都有可能影响到网络运行安全。为了妥善解决这方面的问题，就需要提取网络运行中所产生的海量数据，并使用分析软件进行处理。对于这项操作，如果采用传统的模式，虽然可以分析数据，但是无法获得良好的效果，通常都是针对某一个具体问题收集资料并对资料进行分析，使得网络安全分析中所获得的结果不够精确，工作缺乏可靠性，不能发挥应有的价值。应用大数据技术对网络运行中产生的海量数据进行分析，不仅可以处理大量的数据，对于非结构化的数据信息也能够有效处理。将大数据技术充分利用起来，收集海量的信息，并对信息进行处理，使得分析资料多而且丰富，基于此所获得的结论精确度更高，有更高的可靠性。

2.2网络安全分析中应用大数据技术数据分析效率有所提高

使用传统的数据处理方法，对于海量的数据进行分析处理是存在一定的难度的。网络运行中所产生的数据信息有结构化的数据信息和非结构化的数据信息，在分析和处理数据的时候难以保证质量，而且效率很低。网络技术的普及，每天都会有大量的数据信息产生，一些关乎到安全性的数据也存在于其中，如果采用传统的数据处理工作必然会影响工作效率。发挥大数据技术的作用分析关乎到网络安全的数据，通过建立大数据技术信息分析平台并在数据分析中合理使用，可以在海量的异构数据中提取有价值的信息，实施分布式存储，并实施并行计算，数据信息的分析处理效率大大提高。

3 大数据时代下网络安全防控策略

3.1细化网络安全管理制度

首先，法律法规。网络环境具有复杂性特征，为对此加以控制，政府方面需要加强立法，为网络环境的安全提供基础保障。网络安全法要求运营商针对获取到的用户信息给予保密，构建起完善的隐私制度，确保其能够合法应用个人信息。其次，执行制度。大数据时代下，互联网信息内容管理与行政执法力度有必要进一步强化。国内在2017年推行《互联网信息内容管理行政执法程序规定》。其作用体现在能够加强网络环境中信息部门行政执法力度，以便于保护公民的合法权益，这属于推动网络环境健康发展的策略。现如今国内网络进入到一个全新发展阶段，相应的法律法规以及管理制度等也逐渐趋于完善，为管理工作的进行提供指导。将互联网行业自律公约作为方向进行分析，将会逐步构建起互联网行业自律机制，约束行业内人员行为。

3.2强化用户自身安全防护意识

对于不断出现的网络安全问题，仅仅靠制度的约束以及技术层面的控制显然并不能够达到理想的效果。为此，还应该在用户方面做出努力，提升其网络安全意识，在根源处控制各类网络安全风险因素。在应用计算机网络期间，需要对各类常见风险因素保持警惕性，可判断网络与所用软件的安全性，并能够及时发现网络中所推送的虚假或诈骗信息。同时，需要培养正确的网络应用习惯，个人信息设置环节应该提升密码破译难度，强化账户保护。在登录网站期间，避免访问具有安全风险的网站，也不能够直接在网站或浏览器中直接下载位置应用软件。3.3软件开发期间加强对安全问题的关注

应对层出不穷的计算机网络安全风险，软件开发企业在设计软件时也应该不断强化软件自身的安全性能。结合大数据时代带来的变化，对网络安全风险识别及防控技术进行优化，加强对于网络安全技术的研发。

结语

当前是信息时代，各种信息技术不断升级，特别是网络技术的应用过程中，每天都会产生海量数据。对于如此巨大的数据量进行处理，采用普通的数据处理工具不能获得良好的效果。要维护网络环境安全，就要对这些数据进行分析，明确数据的安全性以及所存在的隐患。大数据技术的应运而生，其特有的挖掘功能可以对海量的数据进行分类，将所需要的数据信息挖掘出来。应用大数据技术挖掘网络中的不安全数据，就可以按照这个目标将相关的数据信息提取出来，分析其中所存在的不安全因素，采取针对性的解决措施，从而维护网络安全。

参考文献

[1]王春海.探究大数据时代的计算机网络安全及防范措施[J].数码世界，2018，05（4）：242-242.

[2]韩鹏.大数据时代的计算机网络安全及防范策略的分析[J].信息与电脑（理论版），2019，425（07）：195-196.

[3]赵宝.大数据时代计算机网络安全防范应用与运行[J].电大理工，2019，000（001）：16-18.