基于大数据分析的网络空间安全优化方法

何健[1] 曾德胜[2]

（罗定职业技术学院 广东罗定 527200）

摘要：近年来，网络技术持续发展，人们对网络空间的应用越来越广泛，大数据时代下，网络环境逐渐复杂化，各种隐蔽且持续的网络攻击对网络用户隐私安全造成威胁，网络空间安全无法得到完全的保护，这时，仍采用传统的网络安全防护措施实施静态控制，只能被动防护无法有效抵御新型网络攻击，因此，需要对大数据分析实施网络空间安全保护进行研究，通过大数据技术对计算机网络中出现的不安全数据进行全面系统的分类，并有效剖析危及安全的原因、并及时处理，进而提高了计算机网络运行的稳定性，因此值得大范围推广应用。

关键词：大数据分析；网络空间安全；优化防范

引言

随着互联网的不断发展以及广泛应用，通过互联网而生成的资料数量越来越庞大，随着网络安全攻击方式逐渐增多，传统网络安全分析技术面对一些新型网络安全隐患无法及时有效地查找并阻截，进而影响当前互联网发展。大数据分析技术可以实现大规模数据收集，并对这些数据进行有效的分类，这和当前网络发展模式的匹配度非常高，因此，在网络空间安全中应用大数据技术可以更好地别系统中生成的安全隐患，保护网络空间安全。

一、大数据分析的网络安全的概述

（一）大数据

现阶段，我国经济常态化发展，科学技术的不断进步，使得互联网逐渐融入于人们日常生活、学习和社会发展之中。而且数据对人们方方面面都有直接的影响，为了能力高效运用数据，产生了大数据技术，并逐渐应用到各个领域。大数据技术就通过全新的数据处理形式对庞大的数据信息进行有效处理，使得信息决策能力不断增强，还可以简单化和具体化信息处理的流程。在大数据技术的不断发展和应用期间，大众的生产生活以及各个领域都发生很大的改变，在云计算平台上，大数据作为信息的核心，大量信息资料能够被广泛汇集起来，在一个体系中根据对应情况加以细分与整合，从而能够给经济社会的各个领域带来新信息内涵和新机会等，大数据能够给经济社会的各个行业带来效益。大数据的特点如下：（1）海量的数据信息，大数据的数据库是一个较为庞大的体系结构。(2）速度快，通过一定的技术手段对大量信息资源进行统一管理，同时又能够在很短的时间内对其内容进行深入研究与更新。(3）多元化，大数据分析具备普遍性，涵盖信息更多，能够被广泛应用到行业开发中。由此可见，大数据分析所产生的作用已引起更多人的重视。

（二）网络安全

所谓的互联网安全就是为了保障互联网可以持续运行，采用一些相关技术手段低于外界对计算机的干扰与影响，使得网络空间的相关数据信息更加安全，避免数据信息的泄露与遗失。另外，通过有效的技术方法对网络完全分成很多种类，然后对不同种类信息进行相应的保护，从而提高整个网络系统的安全。

二、大数据分析在网络安全中的应用优势

在网络不断发展过程中不仅数据信息量大幅度增加，对网络安全的攻击方式也层出不穷，并且很多网络入侵方式存在较强的目的性与潜伏性，导致网络袭击隐患在庞大的大数据系统中难以快速有效地识别。大数据分析技术能够对网络庞大的数据进行全面分类与分析，能够准确找到网络安全隐患，保障网络空间安全。故此，大数据分析在网络空间安全分析中具有一定的优势。

第一，正确性。在互联网运行中数据传递都是采用真数据流的状态进行，因此大数据挖掘技术在互联网中的主要运用就是先记录下真实数据流状态，从而形成真实数据流的分析模型，然后再进行比较分析真数据流状态，在建成的系统中就可能存在着网络安全风险。第二，安全性。在大数据分析的技术应用中，不但能够对整个系统的运行过程历史数据进行大量的采集，在数据库中利用云计算技术能够建立对数据流的模式，这就能减少大数据分析方法对数据库管理机制的高度要求。在对网络空间的分析中，应用大数据分析方法还能够使大数据分析的准确性大大地提高[1]。

三、大数据分析的网络空间安全中存在的问题

（一）网络用户的安全意识低

虽然，网络应用技术已经基本普及，大多数人的生活、工作、学习离不开网络，但整体来看，大部分网络用户在实际使用过程并不了解或极少了解网络空间安全问题，这也表明，网络用户的安全意识比较低，在日常使用中未能采用有效的安全隐患预防措施，导致网络数据安全性降低。一些网络用户具备安全意识，在电脑系统中设置保护密码，促使网络数据的安全系数提高，但是在使用期间没有启动监管系统，同样无法有效地保障网络空间的安全，很有可能导致网络数据信息的损失和泄露。

（二）互联网病毒和黑客的风险

互联网具有高度开发性的环境，所以，网络用户在使用互联网信息技术期间很容易遭受病毒和黑客的入侵，使得网络数据信息遭到破坏和盗用。虽然计算机网络类型有很多种，但是使用过程中的信息安全技术漏洞也呈现出现各式各样，尽管信息技术不断发展和提升，互联网病毒也随之发生相应的变化，这就导致互联网病毒的适应性与感染力之间提升，进而对计算机网络空间安全的危害依然存在，甚至危害性更大。但是如果用户网络受到病毒感染或黑客攻击，将会造成信息系统丢失或破坏，会给企业甚至社会个人造成经济损失。在网络时代的今天，要想使网络数据的利用率得到提高，就必须加强对网络病毒和黑客的防范，从而降低对计算机安全的危害[2]。

（三）缺乏网络空间安全维护人员

为了提高网络运行的速度和安全性，需要有人员对网络进行适当的维护，而且网络维护人员的专业基本知识和技能要扎实，在面对黑客攻击或病毒感染时才能有效地处理，确保消除网络安全隐患的同时，保障网络中重要数据的安全性。然而，普通的网络用户不具备安全维护能力，而大多数企业内并没有建设网站维护岗位，通常也会有维护网络的人员，但这些维护

人员的综合素质比较差，这对维护网络信息安全有很多不利的方面。

四、基于大数据分析的网络空间安全优化方法

（一）合理使用补丁程序

网络运行期间进行程序安装无可避免地存在一些漏洞，这就加大网络安全的潜在危险，部分不法人员会借助这些漏洞恶意攻击用户网络空间，很大程度上影响网络的正常运行。一般情况下，企业在面对软件漏洞时会研发一些弥补漏洞的补丁，以此维护网络控量安全。另外，计算机使用人员也要及时对系统漏洞进行查找，及时发现. 以便对漏洞进行处理，在查找漏洞时可用网络防护软件来进行，比方说，360 防护软件等。

（二）加强用户权限管理

要想有效解决网络中用户权限管理的问题，就应该使用多重验证的方式，降低系统漏洞的存在，杜绝黑客入侵的机会。通过设置与之对应的安全防范措施，随时检测用户的权限，对于数据资料的修改、添加、删除等一系列敏感操作，应展开多次重复验证，避免不法分子窃取或破坏数据资料，进一步保证网络空间安全[3]。

（三）加强网络安全保密技术应用

目前，电脑的安全加密技术主要有 RSA 和 DES，基本都可提高电脑的稳定性。从一九八七年 RSA 算法正式引入以来，历经了几年的发展沿用至今，其间曾经过大量各种形式的网络攻击测试，并对当前的较大的且多数网络的威胁也有着一定抵抗作用，不过，RSA 算法的主要密码加密的可靠性却直接受到了密钥长度的影响，从技术理论出发，当锁钥密码的长度越长时，在实际使用中安全才能到达一个较大的水平，如果加密的长度不够，实际应用中网络空间遭受攻击的可能性较大。在科技不断进步和发展下，RSA 信息加密技术的可靠性受到质疑。DES 属于对称加密方法，在实际应用中需要双方用户协同合作才能起到安全保障作用，主要原理就是，在数据传输与处理期间，传输与接受的双方共同掌握密钥，才能实现数据的传输，通常这种方法在金融信息安全领域使用较为普遍，目前人们最常用的 ATM 机所采用的密码方法便是 DES 科技，是目前应用中相当普遍的一种密码系统。

（四）信息数据镜像与备份技术

大数据时代的到来，通过非法入侵的方式偷盗互联网数据或信息的情况经常发生，使得互联网数据安全问题日益严峻。在网络应用中使用信息数据镜像与备份技术，在网络遭受攻击无法启动、信息缺失时，能够帮助信息系统恢复正常运行，并快速找回网络数据。信息数据镜像与备份技术主要应用到企业、数据网络设、政府信息机构等，在经过信息系统及时备份的情况下，可以借助备份数据快速恢复网络运营，降低用户的经济损失。目前，手机“云备份”、企业“云备份”等云端备份成为信息系统备份技术的使用方式[4]。

（五）注重网络隔离的运用

在网络空间安全保护中可以通过安装相应的杀毒软件和防火墙的方式实现。网络用户要使用杀毒软件对计算机网络中的病毒实施查杀，保障计算机系统正常运行，同时使用杀毒软件时应关注软件的更新动态，及时升级软件增强杀毒能力。另外，网络用户可以借助防火墙保护网络信息，防止不法分子使用不良手段时盗取网络数据信息。网络数据在传输过程中通过防火墙检查输出数据，查看数据中是否存在问题，一旦数据存在问题，防火墙会阻止数据的传输，并实时监测网络运行情况，防止异常情况的发生。目前，防火墙的类型比较多，如过滤型防火墙和代理型防火墙。其中过滤型防火墙通常会检查网络数据包，如果其中信息存在问题，防火墙将会采取阻止措施，避免存在危险的数据信息进入网络空间。代理型防火墙主要服务与计算机服务器和客户端，当客户端想要获得服务器中的任何一种信息时，需要向代理防火墙发送求情信号，然后结合客户要求调取服务器中的相关数据信息，再向客户端传送，这样可以满足客户端的要求，这种做法能够确保网络信息的安全性，同时对网络空间安全的维护起到良好的作用。

（六）提高网络安全防范意识

以网络的身份验证环节为切入点，以保证网络能够安全运作，并为其提供了对应的运行基础。而通过身份验证可以采取有效防止黑客或是不清楚身份用户进入互联网的措施，从而全面落实了网络空间安全的防范意识，可以有效防护网络数据完整性、机密性，从而避免非授权用户对互联网进行浏览以及传输个人信息资料。而且，在实际使用网络过程中，当使用者熟悉最基本的安全知识、网络安全应用习惯之后，便能在一定程度上提高网络安全管理水平。再例如，当用户在使用计算机和互联网时，就应该在公用计算机或应用操作系统中同时展开文字信息的应用和数据资料的操作工序，而不要在保存统计数据信息时使用相同的密码。另外，用户需要时常对数据资料进行整理并展开恢复操作，防止在后续的使用中发生网络端口遭受到攻击、数据丢失难以恢复等一系列问题[5]。

结束语

为了促进社会和谐发展，人们要对大数据时代下网络空间信息安全加以重视。人们要认识到大数据的作用，增强自身的安全防范意识。相关人员要对大数据进行有效分析，发现网络空间安全中存在的问题，积极研发信息技术对网络环境进行维护，同时还要做好网络环境的监管工作，努力营造健康的网络环境，真正保护网络数据信息的安全，进一步促进网络有效发展。

参考文献：

[1]张新刚,王高华,田燕,孙晓林,张婷.大数据环境下的网络空间安全威胁分析与应对策略[J].卫星电视与宽带多媒体,2020(01):78-79.

[2]蒋莹.大数据技术在网络安全分析中的应用[J].今日自动化,2022(5):113-115.

[3]卞春花.基于大数据技术的网络安全态势感知研究[J].通信电源技术,2022,39(17):140-142.DOI:10.19399/j. cnki.tpt.2022.17.043.

[4]赵云.大数据时代网络空间安全问题思考[J].科学与信息化,2021(18):36-37.

[5]金如佳.大数据技术在网络空间安全分析中的应用探究[J].信息与电脑(理论版),2019(03):180-181.

何健，男，汉族，1978-10，江西修水人，罗定职业技术学院副教授，本科学历，硕士学位，研究方向：主要人事网络技术、信息安全技术、高等教育教学研究。

曾德胜，男，汉族，1980-08，广西武宣人，罗定职业技术学院副教授，硕士研究生，研究方向：主要从事数据挖掘、大数据技术、信息安全研究。

基金项目：本文系广东省教育厅科学研究项目“基于大数据分析的网络空间安全关键技术研究”阶段性研究成果（项目编号：2019GKTSCX132）；广西多源信息挖掘与安全重点实验室项目“大数据时代背景下数据安全与隐私保护技术研究”（项目编号：MIMS20-05）。