大数据时代计算机网络安全技术应用风险研究

李　砚

（四川蓉城蕾茗科技有限公司，四川　成都　611130）

摘　要：现阶段人们的生活与互联网之间的联系日渐紧密，人类社会已步入大数据时代，网络安全的重要性尤为突出。我国作为全世界互联网用户量与数据量最高的发展中国家，网络安全领域的问题始终备受关注。分析大数据时代下网络安全特征与安全风险，综合应用网络安全保密技术、防火墙技术、数据加密技术、认证技术以及入侵检测技术等，积极应对网络安全风险，全方位保障计算机系统数据安全，利用大数据解决网络安全问题，为用户营造和谐稳定的网络环境。

关键词：大数据时代　计算机　防火墙　入侵检测　网络安全保密

中图分类号：TP393；TP311.13　　**文献标识码：**A　　**文章编号：**1003-9082（2023）04-0001-03

引言

计算机网络技术对现代社会的发展产生了深远的影响，大数据技术不仅为人类生活提供便利，也提高了社会生产效率。随着数据的集中，其中最备受关注的问题当属网络安全问题，如何保障网络数据使用安全，且不受到任何泄露与非法篡改的威胁，这是未来网络安全技术研发的重要目标。大数据时代，数据分析与处理技术在互联网环境下应用普遍，人们必须采用最新的方法对数据的采集与传输过程加密，避免重要信息泄露，防止用户信息被黑客入侵窃取，同时加强网络安全管理，不断优化网络安全技术的实现路径。

一、大数据时代计算机网络安全特征

现阶段大数据技术主要涵盖数据采集、数据存储、数据挖掘等内容，数据采集就是应用网络爬虫方式将网络与设备中的信息收集在一起，再对这些数据信息集中管理，或者使用传感器采集各行业与领域的数据，再按照一定的形态进行数据存储。网络安全分析采集、存储网络日志、用户行为中的信息，分析其中的漏洞或者潜在攻击，判断是否会产生信息盗窃威胁，以此提前预防网络安全风险，保护计算机系统稳定运行。由此可见，大数据技术是网络安全维护与计算机稳定运行的重要基础，计算机网络安全在大数据时代下主要呈现出以下特征：

1.安全系数高

采用防火墙与数据加密的技术形式，保证网络数据库安全运行，用户将数据从计算机上传到云端，再对数据内容加密处理。和以往的存储平台相比较，云处理中心为用户带来更加便利的服务，通过对称加密与公开密钥加密、身份认证等安全技术的应用，为数据安全提供保障[1]。

2.运算效率快

大数据与云计算联合应用，使计算机网络覆盖范围扩大，运行效率显著提升，人们在应用计算机处理数据时速度更快，数据的传输更稳定，随着大数据的发展，虚拟现实与人工智能开始用于数据处理环节，这在一定程度上降低了网络运行的成本，给人们的生活带来便利。

3.信息资源共享

以大数据技术与云计算应用为基础，用户可通过共享平台得到信息，再将各类交互数据及时传输到平台，使数据流动性增强。用户依靠云平台完成数据存储与共享，提高信息传输时效性，解决信息资源在开发期间的利用不足问题，也为计算机网络安全奠定了有利条件。

二、大数据时代计算机网络安全风险

1.黑客攻击隐患

实际上，黑客攻击也是计算机网络中长期存在的安全问题，黑客一般会在网络环境下以恶意攻击与盗取破坏信息为目的，给计算机网络运行带来安全隐患。受到利益的驱使，网络黑客凭借互联网信息的传播性和共享性特点，编写针对性计算机程序后，对网络目标造成蓄意破坏。此外，也有一部分网络黑客在展开攻击行为时缺少明确的目的，只是为满足自己的欲望，对网络环境展开破坏，这类网络黑客拥有较高的计算机操作技能，给网络环境带来了安全影响。

互联网的使用核心目标体现在提升工作的有效性，互联网安全威胁会影响工作的落实。计算机网络终端面对的安全问题主要体现为两方面：一方面，来自外部的安全威胁。网络终端与互联网相互接通，采用这种方式后，操作者从互联网获取信息，同时计算机之间需要互联网完成双向联通，这在一定程度上为病毒与黑客恶意攻击提供了融入的渠道，也对互联网的使用造成了安全威胁。常见的网络攻击主要有DDoS攻击、勒索病毒攻击以及SQL攻击等；另一方面，内部攻击。这种威胁主要源于使用者不良操作

或蓄意进行的破坏行为，比如操作者交叉应用U盘，导致信息系统在不知情的情况下受到病毒侵染，引发数据遭受破坏。当使用者浏览带有潜在威胁的网页与电子邮件时，此时计算机设备有可能受到病毒侵害，这在一定程度上会给计算机设备与网络运行带来安全威胁[2]。

2.网络环境下的病毒隐患

网络病毒通常是拥有计算机技术的人员，通过编写计算机程序后形成的具有强大破坏力的方式。与黑客攻击方式相比，网络病毒的传播没有明确攻击目标，产生的根源就是人为造成计算机系统大面积病毒感染。现阶段的计算机病毒有两种类型，一种是从利益角度产生的病毒，这类病毒感染之后，如果病毒无法自行解决，就需要购买发布者的查杀程序解决，此时病毒的发布者就可以获得利益。还有一种病毒是由人们的恶作剧产生，比如“熊猫烧香”这一病毒就是学生因无聊而创造的，虽然病毒的危害比较小，但依然会给用户带来不便。随着大数据技术的发展，计算机病毒类型日益多样化，比如间谍病毒，这种病毒一般是通过计算机脚本传播，具有极强的感染能力，可以在短时间内造成大面积计算机病毒感染。

3.计算机操作系统的自身安全隐患

当前计算机操作系统中最具代表性的是Windows系列，设计人员难以将所有网络风险考虑在内，操作系统在程序上会存在潜在的安全漏洞，所以网络黑客会利用这些漏洞去盗取或者攻击计算机信息。因操作系统引发的安全隐患主要体现为以下几点：（1）TCL协议漏洞引发计算机操作系统安全风险。目前计算机网络都是以TCL协议搭建的，但TCL协议自身存在一定的不足，最初的协议设计旨在完成计算机间的通信。大数据时代下，计算机之间可以实现通信共享，现有的TCL协议无法满足计算机操作安全需求，其中存在的漏洞也会让网络攻击行为产生。（2）计算机系统漏洞，如今越来越多的软件系统被开发应用，这虽然提高了数据运行效率，同时也会引发网络安全问题。比如计算机网络系统自身的安全设计存在漏洞，给网络系统的稳定运行造成安全威胁。操作系统漏洞通常可以采用下载补丁的方式修复，从而随时减少新出现的安全隐患，保护操作系统运行安全。

三、大数据时代计算机网络安全技术

1.数据分析技术

面对时空维度内的海量数据，必须依靠强大的分析理论与方法才能处理数据。使用大数据技术进行网络安全分析，对于数据信息的分析主要是依据数据具体类型与特征展开，采用合适的分析方法，为网络安全提供技术支持。依靠大数据技术进行数据实时分析与处理，采取流式计算和CEP技术，经过数据分析对信息内的安全隐患及时发现并解决，保证数据全面性与准确性，提高网络安全性。分析历史安全数据时，可采用离线处理方式，在分布式存储与计算的方法下实现对历史数据的精确分析。

数据分析技术联合不良信息监测报警技术，实现对数据信息的有效监测与及时报警。网络内的普通信息和恶意信息有时难以辨认，所以使用相应的监测报警技术可以为使用者提供信息验证服务。网络中常见的不良信息主要有虚假交易信息、虚假资金往来、带有攻击性的病毒链接，对此监测报警技术的应用能够及时将不良信息过滤，并做出安全提示，经过网络检测与用户使用期间的举报，形成相应记录，再对这些记录做好监控，保障计算机网络安全。当用户对不明的链接尝试进入时，系统会提出报警与预警。

2.网络安全保密技术

RSA与DES是当前最主要的安全加密技术，可为计算机网络安全提供必要保障。其中RSA算法应用的最广泛，它能够抵御当前一致的网络密码攻击，且RSA算法加密安全度可以接受钥匙长度带来的影响。只要保证钥匙密码长度，RSA算法就能保证网络安全。DES数据加密算法也是对称加密算法的一种，再使用期间要求使用者相互配合，数据传输时发送方和接收方必须同时持有密码，只有这样才能完成数据传输。与此同时，DES加密技术目前被用于金融数据安全领域，比如AT机使用的句式DES加密技术，也是当前使用最普遍的密钥系统之一[3]。

3.防火墙技术

虽然防火墙无法阻止所有黑客攻击行为，但是防火墙的防御功能却尤为显著，该技术是计算机网络的第一道屏障，防火墙可以帮助计算机过滤大多数恶意攻击与访问行为。大数据时代下，大数据技术为防火墙技术的应用提供了一定的技术支撑。网络用户将防火墙等级设置成高级别防护等级，确保防火墙可以24小时全天开启，以此降低黑客攻击与病毒感染的发生几率。现阶段的防火墙技术已经具备了自动过滤的功能，可为计算机系统提供多层保护，每层防火墙可针对各类安全风险进行自动过滤，从而使计算机操作系统安全风险能够降到最低。

支付宝拥有十亿用户和庞大的电子现金流，阿里平均每天会被黑客攻击16亿次，而阿里网络安全团队为支付宝建立的风控防火墙与自我防御系统，能够采用大数据测算风险操作积极抵御黑客、病毒的攻击。科学设计Internet防火墙和周边防火墙，全方位保护服务器，使内外网络有效隔离。依靠防火墙进行内网的有效划分，确保内网重点网段

可以独立运行，降低敏感网络安全发生率，防止局部风险给全部网络造成威胁。以安全域为前提的防火墙摆脱了过去只能连接内外网的角色，如今已出现内网、外网、DMZ的模式，并向着高端口密度发展。

4.数据加密技术

互联网安全中，数据加密技术的应用范围很广，一般会用在开放网络当中，常用的数据加密类型主要有“对称加密”与“非对称加密”两种，经过这两种类型的相互配合，以达到对用户网络中动态数据的安全保护。

对称加密是最便捷的加密方法，加密与解密都需要使用相同的密钥，这种加密技术存在较多算法，且可以保证加密文件的安全性，加密效率较高，所以对称加密通常会被用于多个加密协议中。对称加密采用＜256bit的密钥完成数据加密处理，在密钥大小设计环节，要同时考虑密钥安全性与解密效率，使加密过程简化，信息交换双方无需应用专门的算法。如果信息交换与共享过程中，密钥没有被泄露，那么相关文件与报文可以得到永久的保密，现阶段人们会在金融领域采用数据加密标准，DES对称加密技术的使用，使电子资金转账过程更安全。

非对称加密模式下，密钥被划分为公开密钥和私有密钥，成对的密钥内，任何一个都能作为公开密钥，此时另一个就是私有密钥。公开密钥用来进行加密处理，私有密钥用于解密，使用期间为保障数据安全，数据交换方会掌握私有密钥。大数据背景下，非对称加密技术的应用使数据交换双方无需提前进行密钥的交换，即可创造安全通信网络，且该技术也经常被用来进行身份认证与数字签名，全方位保障网络使用安全。

5.基于信息安全的PKI技术

大数据时代下计算机网络内拥有海量丰富的信息数据，为提高数据管理能力，保障数据处理效率的提升，需加大网络安全技术研发力度，建立相对完善的安全基础设施，保证用户数据传输期间的安全性。PKI技术主要是应用公钥理论构建安全服务体系，当前该技术主要用于电子商务领域。以网络运行方式为主的电子商务活动缺乏和现实的基础，所以采用网络技术进行双方关系验证尤为重要。PKI技术可以提供相应的验证方式，保持信息与文件的完整性，完整的PKI体系主要涵盖认证、注册、数据备份、证书管理等部分，可以让电子商务数据处理更灵活。

采用CA认证机构与RA注册机构，CA是保证信任度的实体，可为网络用户颁发证书，核实其身份，防止电子证书出现篡改或者伪造的可能。用户持有CA签发的证书后，该用户即可被信任。与此同时，还应使用RA注册结构，采用面对面登记与用户远程登记两种方式，保证PKI系统应用的灵活性。

6.认证技术

认证技术就是在消息传输期间对相应参数进行检验，谨防信息伪造与篡改的有效技术，该技术主要包含身份认证与消息认证两部分。其中，身份认证就是利用口令技术与生物认证技术，对网络操作者的身份予以认同，防止非法攻击行为对数据造成篡改；消息认证技术是对消息进行认证、对消息序号与操作时间进行认证，可以此验证消息原文完整性与真实性。比如消息内容认证，网络信息传输过程中，发送者在消息内加入鉴别码，对鉴别码与消息加密处理，再将消息传递给接收者，对方利用相应的算法解密消息，然后通过鉴别运算后得到相应的鉴别码，再将其与发送者添加的鉴别码相互对比，如果相等，说明该信息数据安全，否则就要拒绝接受该信息。

7.文件加密技术与网络访问权限

为达到保密要求，计算机内的文件数据保护措施就是文件加密技术，这是针对重要文件与资料采取的保护技术，可有效防止恶意用户盗取或破坏文件。文件加密技术可以对文件增加加密算法，再对恶意用户进行预防，防止其采用针对性方式。网络访问权限就是要求用户遵守网络安全协议，以特定的登录方式访问系统，谨防恶意用户非法访问。将文件加密与网络访问权限相结合，可为计算机的安全使用性能带来必要保障。

结语

总而言之，大数据时代背景下，人们对于计算机网络的依赖性增强。使用计算机网络安全技术能够保障网络安全运行，发挥计算机网络信息的应用效益。与此同时，还要注意网络安全引发的各类风险问题，比如操作风险、黑客攻击以及病毒等，有必要科学应用各类安全技术，建立防火墙，使用身份认证技术，以此保证计算机网络运行稳定。

参考文献

[1]李浩铭,乔桂林.大数据时代计算机网络安全技术应用分析[J].网络安全技术与应用,2022(03):70-71.

[2]王婷.大数据时代的计算机网络信息安全技术应用[J].信息记录材料,2021,22(12):86-87.

[3]何中国.计算机网络安全技术在大数据时代的应用[J].软件,2021,42(10):87-89.

作者简介：李砚（1983.04.04—），男，汉族，籍贯：天津市，学历：本科，研究方向：大数据软件开发。