大数据时代计算机网络信息安全问题分析

王丽萍

（邯郸市职教中心商贸信息部　河北　邯郸　056004）

[摘　要]大数据时代下，大体量、多元数据的传输，对计算机网络信息防护体系提出更高需求。为增强计算机网络信息安全防护能力，应深度分析大数据下计算机网络信息的传输特性，找寻计算机网络信息安全问题，才能逐步完善计算机网络信息安全防护体系。文章围绕计算机网络信息安全问题进行探讨，仅供参考。

[关键词]大数据；计算机网络；信息安全

【DOI】10.12252/j.issn.2096-6261.2021.08.1076

引言

大数据时代是互联网技术发展的一个重要阶段，数据多元化处理，真正确定信息资产价值，完成对不同领域的数据化根植与应用，为社会发展提供有效助力。目前数据信息已经深度融入人们的日常工作及生活中，数据信息的多元化传输，为行业领域的发展做出巨大贡献。但是在大数据体系下，大容量的数据信息传输，加大网络运行负担，从而使计算机网络面临着一定的漏洞风险，此类风险极易被不法人员所利用，造成用户及企业计算机网络信息的损失现象，严重影响到社会稳定发展。对此，应针对计算机网络信息安全问题产生点进行分析，并制定出以技术、管理为驱动的防护体系，保证计算机网络运行的安全性及可行性。

一、大数据下计算机网络信息的传输特性

第一，规模大特点。在现代计算机系统建设及发展过程中，大数据技术的涵盖面是全面切合到整个计算机体系中，其可支撑大规模的数据操作，以及配合线下服务实现多功能运转，确保每一类技术体系的实现，正确驱动计算机系统的运行，同时也可保证数据服务的针对性。

第二，可靠性特点。大数据技术采用的各类关键应用系统无论是在数据传输，还是在预算方面，均可保证每一类数据体系具有较高的可靠性与安全性，确保计算机集群性能是随着数据对接服务能力的提升而逐步增加的，提高数据计算运行的安全性，满足计算机系统的发展诉求。

第三，通用性特点。大数据技术与传统的计算机设备而言，以数据核心及系统预算功能为主体，实现对库数据库的应用及驱动，其产生的技术属性是作用于不同计算机设备之上的，而不是以设备型号为基准实现的，提高大数据技术的应用属性，真正适用于整个计算机行业的发展进程中。

二、大数据时代下计算机网络信息安全问题

数据大体量多元化传输作为大数据体系的主要特征，庞大的数据流量在网络系统中进行运算、传输及存储，极大增强网络运行负担，令计算机网络信息面临着严重的漏洞风险问题。

（一）计算机网络问题

计算机网络具有开源式、共享式的运行特征，数据信息存储是以数据传输指令为核心，进行全域化的数据运算及处理，这在一定程度上增加网络数据存在的脆弱性。特别是对于大数据时代下，数据信息传输多元化特征，造成在没有数据传输限制的制约下，产生无序性、繁杂性的数据运行机制，此类模式也将会为不法人员提供以技术为切入点的攻击路径，严重影响计算机网络安全。

（二）黑客以及病毒所引发的攻击

目前计算机网络安全威胁最大的是黑客以及病毒，两者造成的风险均将令计算机网络产生大面积瘫痪或数据永久丢失的问题。

第一，黑客攻击主要是指不法人员利用主动攻击手段，完成对计算机系统及其网络的定向攻击。此类攻击行为分为非破坏型与破坏型两种，其中非破坏型是指对系统运行造成一定的干扰，其本身并不会造成内部数据的损失，例如，通过拒绝攻击服务以及信息炸弹等，降低计算机系统的运行效率，起到数据阻隔的作用。破坏性动机则是主动入侵计算机系统，完成对各类保密数据的窃取以及损毁。

第二，计算机病毒攻击则是指不法人员在计算机程序中植入具有破坏性质的数据，此类数据既可以影响计算机设备的正常运行，同时也可以自动生成与复制各类程序代码，其具备隐蔽性、潜伏性、破坏性等特征，在计算机病毒的生命周期内得以大范围的蔓延。计算机网络病毒也是由人员制造的，其本身是无法独立运行的，而是植入到某一个系统或文件之中对计算机系统进行潜伏性以及引导性破坏，例如，混合型病毒，其作用于不同系统以及文件程序中，可以实现阶段型的损坏。

（三）数据漏洞方面

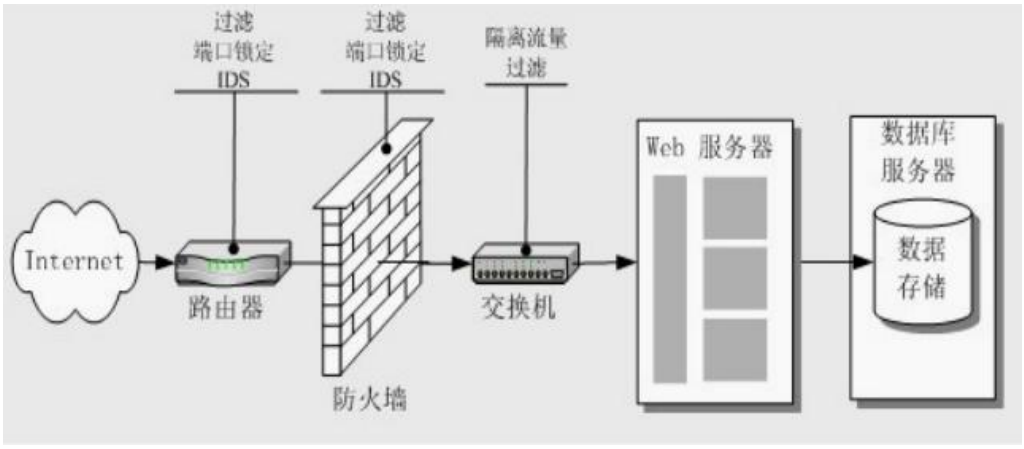
软件开发具有专业性特点，其需要针对软件程序的组件以及运行过程中所产生的进行精确分析，确保功能在具体表述过程中是符合用户操作诉求的，达到前期预设的基准。但是此过程中所呈现出的数据漏洞问题，则表现在文件传输协议的匿名性以及电子邮件在传输过程中所产生的病毒渗透性问题。与此同时，在人员操作过程中，数据的转换与对接极有可能增强软件开发过程中的数据遗漏问题，增加数据漏洞的产生风险，进而引发出严重的网络安全问题。

三、大数据时代计算机网络信息安全防护对策

网络安全问题的频发是目前社会矛盾的主要动因点，在大数据时代下，安全问题所产生的迫害性更加巨大与频繁，严重影响着人们的日常工作及生活。对此，要全面提高计算机网络系统安全防护机制的建设及使用，增强网络系统的安全属性，为人们提供更为优质的技术服务。

（一）合理运用防火墙技术

从现阶段计算机网络安全问题的产生原因来讲，大多数是内部数据遭到损坏或者是主要信息被篡改，进而引发一系列的数据安全问题。防火墙技术的应用，则可以在内部环境与外部环境之间构筑出一个过滤性质、阻隔性质的防护体系，其既可实现对外部数据协议的检测，也可对内部人员操作提供一个警醒作用。此外，防火墙系统的研发与应用，从基本层面上杜绝的非法干扰及入侵的问题。从技术角度来讲，防火墙系统是按照拓扑结构完成对网络系统的防护设定，保证在不同应用场景下，防火墙的阻隔功能可全面实现对数据信息的管控与防治。如图一所示为网络防火墙的工作原理图示。此类防火墙技术的实现是全过程作用于计算机网络之中的，可以过滤由内到外，由外到内的数据，同时防火墙的运行机制呈现出的数据检索功能，只有在符合安全策略

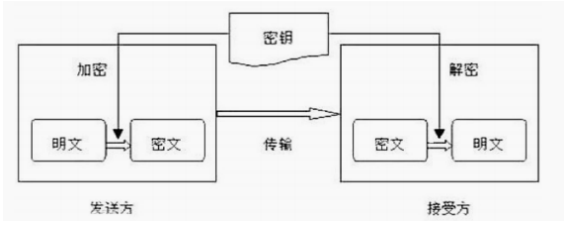


图一 网络防火墙的工作原理图示

前提下才可以完成对数据包的传输。防火墙还具备预防侵入的功能，因为防火墙本身是介于内网与外网之间的，为保证系统的安全运行，需要通过对不同路由器以及交换机之间完成数据分析与组合，增强防火墙的介入能力，提高数据信息传输的安全性。

（二）采用数据加密技术

数据加密技术在数据网络中实现全过程性的加密处理，且可依据不同场景完成对不同数据的针对化加密（如图二所示，为数据加密解密原理），例如，链路加密、节点加密、端对端加密等，保证不同数据系统在实现过程中是符合安全性可靠性运行诉求的。在链路加密中，可以看成是在传输效果中加密的一种形式，针对数据链路层中所传输的数据进行加密处理，起到数据传输路径中的全过程加密。数据节点加密则是针对固定设备完成密码设定与加密处理，与链路数据加密相比，其具有较高的安全性。数据加密技术在具体应用过程中可以作用于网络数据库、电子商以及专业网络中，通过不同应用场景完成对数据的精细化处理。其中在网络数据库中通过数据加密技术的实现，增强对网络数据库运行的安全加固处理。在电子商务中，针对与电子信息及其活动相关联的商务模式进行一体化的数据加密处理，例如，交易期间通过用户名密码对称以及非对称加密，完成对数据信息的终端化保护，防止用户在执行各类指令期间产生数据损失问题。在专用网络中，则是采取加密算法，对各类计算机设备及应用系统之间进行对接式加密，最大限度保证主机及各类应用的安全。



图二 数据加密解密原理

（三）加强对计算机网络系统的监控和监测

从病毒侵袭以及黑客入侵形式而言，具备突发性特点，对计算机网络造成严重损毁问题。这就需要计算机网络的运行区间，应具备独立性以及预见性的数据防控机制，通过检测识别出当前网络运行中所存在的异常问题，起到数据检测与处理的效果，防止计算机安全问题的蔓延，将问题消灭在隐患之中。例如，入侵检测技术的实现，通过签名分析法与统计分析法，完成对计算机网络系统内部的数据核验处理，既可以针对各类攻击行为以及预期攻击路径进行分析，也可以通过精密算法及统计算法完成对各类攻击行为的全域化调查，规避数据运行期间的各类隐患现象。

（四）加强对应用系统的完善

软件系统在研发过程中所存在的漏洞，将影响后期运行质量。对此，设计及运维期间，承接应用系统及软件开发的公司，必须做好及时更新，及时发现软件运行之间存在的漏洞问题，并做好更新处理，提醒用户进行更新，防止病毒问题的蔓延。但是在此过程，各类软件程序的制定必须具备预见性功能，因为一旦软件更新，黑客攻击手段也针对软件更新后的各类系统进行针对化攻击，到下一次软件更新时所产生的时间差问题，将造成软件应用安全空白区的现象。为此，需要实时化对软件进行更新处理，增加黑客攻击的破解难度，降低被攻击概率。

（五）增强用户的防范意识

用户作为计算机设备及网络系统运行的主要驱动体，自身的操作行为直接决定着网络信息具备的安全等级。因此，应进一步提高网络操作人员的专业技能以及对网络安全意识的认知度。例如，提高这个计算机用户的安全素养，对各类病毒及黑客攻击行为可以起到辨识的作用，防止出现误操作的问题，避免浏览危险网站以及接受不明来历的邮件，这样才可以杜绝安全问题的产生。

四、结语

综上所述，计算机网络已经深度根植于人们日常工作与生活中，为社会发展提供有效助力。但是计算机网络也带来一定的风险问题，造成网络系统数据丢失的严重问题。对此，应深度挖掘网络信息安全问题的产生点，结合技术、管理等方面，构设出一体化的管理体系，增强计算机网络安全防护能力。

参考文献

[1]赵培琨. 大数据时代计算机网络信息安全及防护策略[J]. 计算机产品与流通，2020（05）：36+52.

[2]张俊玲. 大数据时代计算机网络信息安全与防护措施研究[J]. 信息技术与信息化，2019（04）：130-132.

[3]龙振华. 大数据时代计算机网络信息安全及防护策略[J]. 中国管理信息化，2019，22（06）：161-162.

[4]张黎明，刘燕. 大数据时代计算机网络信息安全与防护措施[J]. 电子技术与软件工程，2019（04）：190.

[5]孙文诗，冯乃勤. 大数据时代计算机网络信息安全及防护策略探究[J]. 山东农业工程学院学报，2018，35（12）：29-30.