 DOI: https://doi.org/10.26549/bdai.v1i1.6765

Design of Computer Network Security Defense System Based on Big Data and Artificial Intelligence Technology

Wen Liu

Heilongjiang Network Space Research Center, Harbin, Heilongjiang, 150090, China

Abstract

In order to further improve the security and effectiveness of the computer network security defense system, this paper studies the design of the computer network security defense system based on big data and artificial intelligence technology, first introduces the current situation of the computer network security in the big data era, then analyzes the functional requirements of the computer network security defense system in the big data era, and finally advances The design of computer network security defense system based on big data and artificial intelligence technology is given. The practice shows that the design can effectively improve the security of the computer network security defense system, effectively improve the intelligent degree of the computer network security defense system, effectively improve the backup and recovery function of the computer network security defense system, and has a certain reference value.

Keywords

big data; artificial intelligence; computer network security; defense system

基于大数据及人工智能技术的计算机网络安全防御系统设计

刘文

黑龙江省网络空间研究中心，中国·黑龙江 哈尔滨 150090

摘　要

为了进一步提升计算机网络安全防御系统的安全性，笔者进行了基于大数据及人工智能技术的计算机网络安全防御系统设计研究，首先介绍了大数据时代计算机网络安全的现状，然后进行了大数据时代计算机网络安全防御系统的功能需求分析，最后进行了基于大数据及人工智能技术的计算机网络安全防御系统设计。实践表明，该设计能有效地提升计算机网络安全防御系统的安全性，有效地提升计算机网络安全防御系统的智能化程度，有效地提升计算机网络安全防御系统的备份及恢复功能，具有一定的参考价值。

关键词

大数据；人工智能；计算机网络安全；防御系统

1 引言

随着计算机信息技术在各行业领域中的深层次应用，尤其是云计算相关技术比如各种云计算服务的提供商为用户提供云存储和云计算等服务的广泛应用，在这种背景下云计算的网络安全问题越来越受到人们的重视。但是从目前网络安全技术发展的现状来看，相关的预警技术以及安全访问技术和相应的网络监测技术相对来说都发展滞后，这使利用现有的网络安全系统来防御各种入侵的过程中表现出了较高的漏检率，因而传统的计算机网络防御系统已经无法适应大数据和云计算服务背景下的对网络安全防御系统的需求。

近年来人工智能技术的出现为各行业领域中的很多现实的问题提供了切实可行的解决方案。由于以机器学习和深度学习为特征的人工智能技术能将复杂的现实问题数学化，并能实现非常复杂的非线性的拟合能力，因而在很多现实问题上都具有非常好的表现。基于此论文对基于大数据与人工智能技术的计算机网络防御系统的设计进行了研究，以期利用当前人工智能技术能在一定程度上解决目前云计算服务背景下的网络安全问题。

2 大数据时代计算机网络安全的现状

2.1 网络入侵技术水平的不断提升

虽然近年来计算机网络防御系统的水平越来越高，但是网络入侵的水平也越来越高，并且网络入侵者不受各种规则

 DOI: https://doi.org/10.26549/bdai.v1i1.6765

限制可以利用各种资源、利用各种技术、采用各种形式来实现对网络的入侵，因而总体上来看网络入侵和网络防御水平呈现一种胶着前进发展的状态。并且随着网络相关知识的普及以及互联网的开放性使越来越多的人开始自主学习相关的网络安全知识。在这种背景下越来越多的人开始掌握计算机网络安全的相关知识，但是相关的法律意识却没有得到增强，因而不少具有一定网络安全知识的人开始利用相关的网络安全知识为了自身的利益或者出于好奇的心理来对其他网站进行攻击，肆意的盗取网站用户的个人信息并且进行贩卖，从而攫取自身不正当的利益。一般情况下入侵者都是采用病毒或者是木马的形式来对网站发起攻击，并且随着人工智能技术的飞速发展，相关的病毒和木马的制作技术也经历了飞速发展的阶段，大量具有很大威胁性和隐蔽性的病毒出现。此外网络安全技术的发展进一步也刺激了网络入侵技术的提升，当前云计算仍然面临着全方位的威胁 [1]。

2.2 网络入侵的方式多样化

网络形式和结构的发展使网络入侵越来越趋于多样化。例如，当前移动网络技术的发展以及其与互联网之间的连接，网络结构日趋复杂，影响到了网络体系结构中的物理层以及各种非物理层，并且应用层终端的不断增多也为计算机网络安全增加了非常大的隐患。人们在非常方便使用各种网络终端设备来访问互联网的时候，各种终端设备所携带的病毒也会通过这些外部终端的设备进入到互联网的其他设备当中，由于网络设备的连通性使出现大面积网络设备感染病毒成为可能，造成了网络设备的巨大的安全隐患。虽然不同的终端设备所能执行的可执行程序不同但是病毒呈现了智能化的趋势，不少病毒甚至可以在不同操作系统设备之间进行变异和传染，给互联网中的设备造成了很大的安全隐患。此外网络结构的日趋复杂化必然带来网络漏洞的增加，使网络入侵者可以在网络的很多环节来实现对网络的入侵，这使网络的防御者防不胜防，使当前网络完全防护的形势日趋严峻和复杂。

2.3 用户网络安全意识的普遍缺乏

当前绝大部分的网络设备使用者都不具备网络安全的相关知识与防护意识，这在普通的网络用户群当中体现得尤为明显，在相对专业领域中的网络用户群中具有一定的网络安全的防护意识但是这种意识也相对较为淡薄。网络安全相关知识的缺乏以及网络安全意识的淡薄为网络入侵者提供了可乘之机，有数据显示绝大多数的网络入侵事件都是由于网络用户的网络安全意识淡薄因素造成的。

举一个非常简单的例子，如网络安全密码的设置，不少网络用户为了方便记忆采用了相对较为简单的网络安全密码这非常容易被网络入侵者所破解。此外还有很多用户在经常使用一些公共网络来访问自己的安全隐私账户如银行账户，这也存在着极大的安全隐患。但是如果用户一旦注意到这些问题并且采取相对简单的应对措施就能在很大程度上杜绝这种网络入侵事件的发生。

从另外一个角度来看不论是网络的使用者还是网络的入侵者的法律意识都相对较为薄弱，这使他们在使用利用网络来窃取破坏他人信息和数据的时候变得肆无忌惮，这也是导致目前网络安全问题频发的一个非常重要的因素。如果网络入侵者都具备较好的法律意识与安全意识，那么就会在很大程度上对网络入侵者的行为产生威慑作用，使网络入侵者不敢随意入侵别人的网络，否则会承担相应的法律责任，严重的会承担相应的刑事责任 [2]。

3 大数据时代计算机网络安全防御系统的必要性

2.1 基础设施层的虚拟化功能

对于大数据时代的计算机网络安全防御系统来说，基础设施层除了必要的硬件设施以外，还应提供将硬件资源虚拟化的功能，从而利用大智移云技术实现硬件资源的合理分配和共享，进而提升计算机网络安全防御系统的集成能力和并发能力。

就当前大数据背景下的网络完全防御系统来看，基础层主要是由一些网络的基础硬件的设施组成。在现代网络防御系统设计的过程中可以充分利用这一点，也就是硬件资源的虚拟化。这种虚拟化可以带来很多好处，如可以实时对网络中的任意的节点进行监测和实时的监控，如果基础网络层中的任意一个节点出现了异常的网络的流量那么都会防御系统通过相对简单的安全监测算法都可以十分容易的监测到，而且网络中可观测的节点数量的增多对于人工智能技术的应用也提供了样本数据，因为物理层能在一定程度上反映出入侵行为，而不同节点对于这种入侵行为的表征重要性是不同的，那么虚拟化就可以极大地提升可观测节点的数量使最终可观测节点空间能充分表征网络入侵的行为，使之成为表征网络

 DOI: https://doi.org/10.26549/bdai.v1i1.6765

入侵行为的完备字典，通过对其稀疏化就可以使网络入侵识别的效率得到极大的提升。

2.2 中间件层的管理功能

对于大数据时代的计算机网络安全防御系统来说，中间件层负责整理数据的输入流和输出流，科学合理地分配系统资源，有效地进行系统安全访问控制，监控系统的运行状态，从而保证该系统的稳定运行。因此，大数据时代的计算机网络安全防御系统的中间件层应具备为大数据应用中心提供必要的资源分配、安全监测和均衡负载等功能。

从网络结构的角度来看，网络的中间层的主要作用为管理数据的流入与数据的流出，对相应的资源进行合理的分配，进而实现对网络中其他设备和资源的安全的访问，与此同时对系统的安全状态进行实时的监控，确保网络系统能安全稳定的运行，所以从这个角度来看网络的中间层可以为网络中的大数据的传输提供相应的资源分配，安全的监测以及相应的负载均衡等功能。从网络入侵的角度来看，网络入侵行为也会在很大程度上影响到中间层，进而在中间层的相应状态上体现出来，因而中间层的相应的状态空间也可以作为识别和发现网络入侵的部分。通常情况网络基础层和中间层作为应用层数据的最终表征，也是大数据采集最为关键的部分。

2.3 应用层的服务功能

对于大数据时代的计算机网络安全防御系统来说，应用层主要是面向用户的，稳定、快捷和方面地为用户提供所需的服务，是整个系统的门户。因此，大数据时代的计算机网络安全防御系统的应用层应具备用户注册功能、用户登录功能、访问控制功能、权限分配功能、系统交互功能、非法入侵检测功能、系统备份及恢复功能等。

从网络结构的角度来看，应用层主要是最接近用户和面向用户的，网络入侵的发起开始以及网络入侵的最终目标往往都是在应用层体现的。应用层的各种应用软件是用户访问各种重要设备资源的接口，也就是最容易发生网络入侵的环节，因为不少网络入侵者都为了盗取电脑使用者的各种账户的信息。目前各种应用软件为用户提供了如用户注册、登录、访问、权限、交互一系列的功能。所以网络入侵和应用层的联系非常的紧密，关于软件操作的一些日志数据对于网络防护系统的设计来说是非常保护的样本资源。

3 基于大数据及人工智能技术的计算机网络安全防御系统设计

基于大数据及人工智能技术的计算机网络安全防御系统主要包括基础硬件虚拟化及网络数据采集模块、大数据智能分析及处理模块、网络安全智能防御及监测模块、用户管理及系统管理模块等 [3]。

3.1 基础硬件虚拟化及网络数据采集模块设计

首先，为了节省硬件投入，为基于大数据及人工智能技术的计算机网络安全防御系统设计了基础硬件虚拟化功能，该功能可以将部分非必要的基础硬件进行虚拟化，从而节省成本和提升系统的灵活性。

其次，为系统设计了一个强大的数据采集功能，能及时采集、传输和存储软硬件数据，并能将这些数据快速、安全地传送给大数据智能分析及处理模块。

最后，在数据采集过程中基于大数据技术和人工智能技术设计了智能包过滤功能，能提升网络数据的采集速度。

3.2 大数据智能分析及处理模块设计

首先，该模块对数据采集模块传来的数据进行初步过滤，根据病毒特征进行大数据智能分析，并将分析结果传递至网络安全智能防御及监测模块。

其次，该模块还能借助大数据技术从互联网上获取其他网络安全公司公布的病毒特征码，从而提升该模块的有效性。

最后，该模块还能学习智能化的特征，从而更好地发现未知病毒及木马。

3.3 网络安全智能防御及监测模块设计

首先，该模块对大数据智能分析及处理模块传递来的分析数据进行实时监测，一旦发现病毒和木马，及时采取相应的防御措施，启动智能化的网络安全防御工具，迅速查杀病毒和木马。

其次，该模块还能根据大数据智能分析及处理模块传递来的分析数据跟踪病毒和木马的来源，从而为公安机关的侦破提供证据。

最后，该模块还提供了防御效果评估功能，能对处理效果进行评估。

3.4 网络安全监测和响应模块的设计

通常情况下，网络防御系统可以有效发现网络的入侵或

 DOI: https://doi.org/10.26549/bdai.v1i1.6765

者是病毒木马的入侵行为，但是并没有进行下一步的操作。本环节就是在发现网络入侵以及病毒木马的入侵行为之后采取的进一步的措施，在这个环节网络防御系统可以采取路径检索和异常活动监测等技术来逐级地对系统中的病毒按照目录进行检索最终发现病毒所在的位置，并结合病毒的情况和危害程度给用户以警示最终对病毒和木马进行进一步的处理，确保网络系统的安全性。

3.5 用户管理及系统管理模块设计

首先，该模块提供了用户注册、登录、访问控制和权限分配功能。

其次，该模块提供了智能化的系统交互功能。

再次，该模块提供了非法入侵检测功能。

最后，该模块提供了系统备份及恢复功能。

4 结语

大数据和云计算下，网络安全形势发生了新的变化，网络的入侵行为也更隐蔽和多样化，但是大数据和人工智能技术也为网络入侵行为的监测提供数据基础和方法基础，未来基于大数据分析的人工智能技术一定会在计算机网络安全防御方面发挥重要的作用，并逐步得到推广和应用。

参考文献

[1] 谷守军 , 王海永 . 大数据时代人工智能在计算机网络技术中的应用 [J]. 电子制作 ,2017(06):30+37.

[2] 吴振宇 . 试析人工智能在计算机网络技术中的运用问题 [J]. 网络安全技术与应用 ,2015(01):70+74.

[3] 龚月瑛 , 乔月圆 . 大数据时代计算机网络安全防御系统设计研究 [J]. 信息与电脑 : 理论版 ,2019(20):199-201.