大数据时代网络安全及预测技术研究

杨基慧

（吉林司法警官职业学院　吉林长春　130000）

摘要：随着计算机网络技术的飞速发展，人类的生产和生活方式发生了巨大的变化。随着计算机网络技术的飞速发展，大数据已经成为一个新兴的概念，它不仅标志着数据量和类型的增加，而且还提高了数据生成和处理的效率，但也使得网络安全问题变得更加突出。在大数据时代，深入研究网络安全技术，以有效降低网络安全风险，具有十分重要的意义。

关键词：大数据时代；网络安全；预测技术

前言：随着 21 世纪的到来，计算机网络技术的发展变得越来越迅猛，它已经深深地影响着我们的生活，从网上购物到网上聊天，从物流跟踪到网上银行，因而信息量不断增加，信息种类越来越繁杂。大数据时代下的网络安全是指在网络环境中保护数据的安全和隐私，身份验证。是指通过设置不同的身份验证方式来保护网络环境，防止未经授权的用户进入网络。数据备份和恢复。是指在网络发生故障或攻击时，保护数据免受损失和破坏。随着信息的快速增长和广泛流通，保护信息的安全已经成为当今社会的重中之重，大数据背景下的网络安全问题越来越受到广泛关注。

一、大数据时代与大数据时代的网络安全

“大数据”是一个新兴的术语，它诞生后就一直受到广泛关注。21 世纪的到来，计算机网络技术的进步可谓惊人，它对我们的日常生活产生了巨大的影响，从网上购物、社交媒体、物流追溯、电子支付，以及各种各样的信息，使得信息的数量和多样性都在不断增长。随着科技的飞速发展，数据信息的价值日益凸现，它们能够以惊人的速度传播、存储，为不同领域的研究、应用提供了强大的支持，使其能够更有效地实现。随着社会的发展，“大数据”的影响力日益扩大，它的内容涵盖了各行各业，让每一位公民都能够从中获益，它的数据可以帮助我们做出更明智的选择，并且能够为我们的决策和实践提供强大的支撑。随着大数据技术的发展，它对我们日常生活产生了深远而持久的影响。大数据的作用与影响已经是不争的事实，但是大数据背景下数据信息的产生也是以计算机网络技术为依托的，诚然，计算机网络技术在社会发展中起到了不可忽视的重要作用，但是，它也同样带来了网络安全问题。网络安全是一个不可忽视的问题，它对信息的存储和传输构成了严峻的挑战。造成网络安全问题的潜在因素是多种多样的，包括不同的技术和领域，对大数据时代的网络安全问题预防造成了一定的困难。随着大数据技术的不断发展，信息的传播和交换变得更加便捷，但同时，由于信息的外部暴露，也存在着被盗取、破坏等风险。为了保护计算机网络安全，应该从管理、技术等多个角度出发，建立一套完善的防护体系，以有效应对各种安全威胁，不断提升信息和数据的安全性。

二、大数据时代网络安全问题分析

1、全民层面上的认识不足

自大数据的概念提出以来，它迅速被人们所熟知，并且发展迅猛，几乎已经渗透到了我们日常生活的各个方面。然而，大多数用户仍然只是简单地记住了它的名称，而没有意识到自己的隐私受到了严重的威胁。当用户访问和利用这些资源时，他们也会将自己的个人隐私暴露出来。例如在网络购物过程中，用户的个人信息、地理位置甚至重要的个人隐私都会暴露出来。重点在于大多数用户没有意识到这些问题，给大数据时代的网络安全带来了潜在的风险。

2、文件层次上的安全性不足

文件是数据的载体，绝大部分的数据是以文件的形式存在的。然而，文件的安全性对于整个数据分析和处理流程至关重要。近年来，文件的体积变得越来越大，云时代的到来使得用户更倾向于将文件存储在第三方平台或云端，以便通过网络获取和使用。虽然这种方式带来了巨大的好处，但也伴随着严峻的安全挑战。由于用户的敏感信息极易受到外部侵犯，而且第三方平台又没有足够的安全措施来保护这些数据，因此可能会对其造成严重的安全风险。黑客们不仅会攻击相关平台，还会窃取用户信息，这严重破坏了文件存储和传播的安全性。

3、数据存储方面的安全性不足

随着大数据技术的发展，许多人已经开始使用移动存储设备，如 U 盘和硬盘，以便更快地处理和传输数据。然而，由于数据量的非线性增长，许多人会将更多的数据和文件压缩在一起，这样一旦移动存储设备发生故障，造成的数据损失将无法弥补。除了结构化的数据外，许多非结构化的数据也有其独特的弱点，而且它们的存储方式也可能会出现各种问题。改变防滑模式和管理机制，以及提升服务器软硬件的性能，都会对数据存储产生重大影响。

4、大数据时代的网络环境安全风险

随着大数据时代的到来，网络技术的发展为人们提供了更加便捷的使用体验，然而，由于其具有高度的公开性和隐私保护，目前的网络安全防护仍然存在一定的漏洞，许多情况下，仅仅通过简单的认证就能够获得访问权限。随着大数据技术的发展，人们可以更加便捷地使用网络，但同时也给网络攻击者提供了更多的机会，从而增加了网络安全的风险，而且很难有效地保护网络信息的安全性。例如数据安全风险方面，随着网络数据变得越来越复杂，许多数据缺乏稳定的结构，从而使得它们的安全性受到了极大的威胁。另外，由于数据的存储模式各异，使得它们容易出现安全漏洞，从而给用户带来极大的损失。大数据时代文件安全风险方面：操作系统的安全功能受到限制，文件安全性能受到影响，信息文件的保护能力也受到削弱，从而增加了文件被恶意攻击的可能性。因此，大数据时代的网络信息存在很大安全隐患。

5、大数据时代的网络信息的监管制度尚不完善

在当今这个大数据时代，随着互联网的普及，许多领域都受到了影响。中国目前正处在这一进程的初级阶段，并且正在与世界各地的企业和组织建立联系。鉴于目前的情况，若要确保网络信息的安全，必须建立一套完善的、严格的网络监管体系，以及强化对个人和企业的安全教育，以防止大量的信息被

非法盗取，并防止不正当的交易活动。由于各种因素的影响，在大数据时代，一些网络信息管理制度与实际情况存在冲突，这使得监管力度无法发挥最大效果，从而导致大数据时代网络安全问题日益严重。从国家管理层面上来说，处在大数据时代就表明了对网络环境的安全体系的建设必然任重而道远。

三、大数据时代背景下网络安全防范技术与措施

毫无疑问，我们正处在一个充满机遇的大数据时代。随着计算机网络技术的发展，现代社会的生活变得越来越便捷，信息和数据的快速传输已经成为当今时代的一个重要特征。在大数据时代，网络安全受到了广泛关注。为了提高当前的网络安全水平，我们应该从以下几个方面努力。

1、全民层面提高网络安全意识

在计算机网络技术高速发展的现代社会，要从每一个用户出发，提升用户的自身的网络安全意识，规范用户的行为。加强网络安全教育。政府可以组织网络安全的教育活动，向公众普及网络安全知识，提高公众的网络安全意识。营造良好的网络安全文化。政府可以通过宣传、教育、舆论等方式，引导公众树立正确的网络安全意识，养成良好的网络习惯。加强法律法规建设。政府可以制定一些法律法规，对违反网络安全规定的行为进行处罚，维护网络安全。在大数据时代，海量数据信息是宝贵的资源，应当遵守法律法规，尊重和保护数据信息所有者的权利，并且合理利用这些资源。为了确保个人信息安全，我们应该加强对个人隐私的保护，防止个人信息的外泄，并维护个人隐私权。进行网上购物或者网上银行时，确保所处的环境是安全的，以避免个人信息被非法使用。

2、加强对数据分析与管理

数据的重要性在于它们的有效利用，而这一切都需要从数据的分析和管理入手。为了更好地处理和管理数据，我们需要加强对数据的敏感性，并且要深入研究它们的特征，以便采取有效的措施来确保数据的安全。同时，我们也要加强对安全防护的重视。应当加强技术支持，并结合完善的数据安全管理制度，以确保数据的安全使用。在开发管理系统时，应该重点考虑数据安全，并致力于保障未来的信息安全。通过全面提升数据安全，我们可以实现更高效的管理。

2.1 加强数据存储及传输的安全保障

随着大数据时代网络技术的飞速发展，必须在网络中加强对数据的存储、传送等方面的安全，而采用加密的方式来增强信息的安全。密码文本是对数据进行加密而产生的。而且，即便是犯罪嫌疑人获得了这些档案，他们也无从追查，所以，这些档案是不会被窃取的。增强资料储存与传送之安全性，是一种切实可行且行之有效之安全等级。

2.2 加强对计算机网络安全的监管力度

部分互聯网用户在上网时，这可能是由于用户的口令设定被泄漏，或是由于使用者的网管在使用时没有注意到网路的安全性，而造成通讯系统及回路的故障。因此，在使用因特网时，无论是计算机使用者还是电脑安全控制者都要重视网络安全，做好电脑的维护与管理工作，也就是电脑使用者要了解电脑的功能，并能很好的完成相关工作。在大数据环境下，如何提高数据的管理与安全，提高数据的安全性。电脑使用者和网路安全管理人员还必须透过各种途径，来认识到安全管理策略的性质以及对网路资料及资料安全性的防护，强化资料的管理，强化网络安全性，以保证网路的可控性。

3、对数据存储和流通进行加密

数据存储和流通进行加密是数据安全中的两个重要方面，它们可以保护数据免受未经授权的访问和使用，从而防止机密信息泄露或被非法使用。加密技术的主要目的是确保数据在存储和传输过程中的安全性，同时保留一定的保密性和可识别性。具体而言，加密技术可以分为以下几类：对称加密技术是一种使用两个密钥来对数据进行加解密的技术，其中一个密钥用于加密数据，另一个用于解密数据。通过使用两个密钥，攻击者只能得知解密所需的密钥，而无法到达完整的数据内容。非对称加密技术是指使用两个密钥来对数据进行加密。其中一个密钥用于加密数据，另一个密钥用于解密数据。通过使用不同的密钥，攻击者只能获取加密后的数据内容而无法到达解密所需的密文。在这种情况下，攻击者只能获取加解密后的数据内容。其中一个密钥用于计算生成的密文，另一个钥用于解密生成的密文。而非对称密码学则是指使用不同的密钥来对数据进行加解密，这需要更高水平的安全性和保密性。

需要注意的是，不同种类的加密技术适用于不同的场景和需求。因此，在选择加密技术时，应该根据实际需求和风险偏好来选择最适合的技术。同时，也应该考虑使用相关的安全策略和工具来管理和监控你购买回国或得到使用到时才启用该策略和工具。现在，许多文件加密软件都采用了先进的技术，例如指纹识别和人脸识别。为了提高数据传输的安全性，采用加密协议和签名技术对数据进行加密，可以实现两种不同的方法：一种是单向加密，另一种则是双向加密，以确保数据的完整性、准确性、可靠性。线路加密旨在确保信息安全，但是双端加密更多地依赖于专业的安全软件，它们可以有效地实现信息的安全传输，从而确保信息的安全性和完整性。

4、针对性的加强网络防火墙与杀毒软件

使用网络防火墙和相关的杀毒软件可以为数据安全提供强大的保护，它们的防护机制各不相同。防火墙技术是一种有效的内部安全策略，旨在阻止非法访问和攻击。其功能是防止外部人员通过网络的非法入侵而进入网络系统之内。它能够有效地确保网络的安全性。网络交互的作用机制十分明确，它可以对数据进行检查，并通过严格的筛选程序，以确定目标网络中的数据是否合法，从而决定是否允许或阻止传输。网络防火墙的种类繁多，从代理型到检测型，从地址转换型到包过滤型，每种技术都有其独特的优势，可以有效地阻止新的内部网络攻击，为网络安全提供有力的保障。与传统的安全措施相比，杀毒软件可以迅速有效地抵抗攻击，它们与网络防火墙结合，构建出一道完善的内部和外部安全保护屏障。通过使用杀毒软件，可以实现快速更新病毒库，并有效地检测和清除受到感染的文件。为了保护自己的安全，建议用户定期升级和维护杀毒软件，以便有效地抵御黑客的入侵。当前，杀毒软件市场繁多，包括360、金山、瑞星等，因此，在选择杀毒软件时，应当结合个人需求，以确保安全性和可靠性。企业在保护数据安全方面应该使用免费且功能齐全的防病毒软件。

5、完善大数据时代的网络管理体系

为了更好地应对大数据时代的挑战，我们应该深入探讨并开发出更先进的网络信息安全技术，特别是要建立一个完善的、符合法律法规的网络环境，这样才能有效地控制和保护大数据时代的网络安全，进而提高整个社会的安全性。通过对计算机的实时监测，我们可以更好地了解它的健康情况，从而更有效地诊断出问题的根源。除了采取信息认证措施，使用者也能够有效地管理和监督计算机，从而大大增强了计算机的安全性。

为了确保信息安全，我们必须采取综合的措施，包括但不限于各种技术手段和策略，来构建一套完整的、有效的防御机制。为了确保信息安全，公司应该建立一个有效的组织架构，并设置专门的安全管理人员。

四、基于大数据技术的网络安全预测技术分析

随着网络环境的不断扩大，基于大数据技术的网络安全预测技术可以有效地分析和挖掘各种感知数据源，从而提升网络安全水平。通过采用先进的智能算法和安全模型，我们可以从多种不同的数据源，如用户终端、网络链接、应用系统和数据流量中收集有效信息，并将其转换成可视化的形式，以更加清晰地展示出潜在的危险，从而实现对危险的快速预警和有效的安全预测。

1、技术整体架构

网络安全预测技术构建过程中，需要应用大数据技术对整个防御链条各个环节中的各类数据进行采集、分析、处理，包括各类终端、边界、系统服务与应用等环节。其中，与网络安全相关的各类威胁信息是收集与处理的重点对象，这些信息收集完成后再统计存储于安全数据库中。利用大数据安全模型、分析算法及安全规划等方法，将数据库中海量的安全数据挖掘出来，对安全事件的发生与发展、潜在的威胁因素及发展趋势等做出分析、预判，最终生成网络威胁情报；以网络威胁情报为依据，实时监测网络安全威胁报警、重要的安全系统等，并做出网络风险预警，感知网络安全态势。

整个网络安全态势感平台技术架构主要包括 3 个层面：一是网络安全威胁数据汇聚与存储层，主要用于收集、存储各类网络安全威胁信息数据；二是大数据分析层，主要针对收集到的各类威胁情报进行分析处理；三是安全预测与预警业务应用层，主要生成各类预警业务报告、感知网络安全态势等。

2、网络安全威胁数据汇聚与存储层

各类数据由数据汇聚层与存储层负责采集与存储，大数据数据库存储采集到的原始数据并形成网络安全威胁信息数据库。在网络攻击跟踪的过程中，我们需要经历一些步骤。首先，我们需要确定攻击者的身份，并授予他们可以访问的权限。接下来，我们需要检查终端的操作和网络流量，并在发现恶意代码时立即发出风险提示。最后，我们还需要进行安全审计。由此可见，系统一旦受到网络攻击，所有环节均会有信息记录，因此安全预测数据源要尽量覆盖整个攻击操作链条的每个环节及要素。应用大数据存储与管理技术对分布式文件系统进行整合，如关系数据库、数据库集群等，存储海量感知数据源，并进行集中管理，以满足结构化数据、非结构化数据及半结构化数据的存储需求。

3、面向威胁情报的大数据分析层

将安全数据转化为威胁情报的主要方法就是数据挖掘分析，而数据挖掘分析则包括数据预处理、模型设计、数据分析等 3 个环节。

3.1 数据预处理

数据预处理即将格式复杂、类型多样的原始数据转换成与系统数据规则相匹配的数据，这个过程即也可称为数据清洗。经过精心的数据处理，原始信息可以被转化为更加符合网络安全预测要求的基本信息，而且，这些信息可以根据已知的特征进行组织，形成一个完整的数据族，每个数据族拥有完全一致的特征。通过对数据的时序关系、交互特征、网际互连协议等进行深入分析，我们可以构建出一个完整的数据关系网络图谱。

3.2 模型设计

大数据模型设计的主要目的是将其所收集到的看似毫无关系的安全数据利用特定的计算与分析规则转化成可视化的信息。通过应用大数据技术构建的信息模型，可以有效地预测网络安全，其中包括数值统计模型、算法挖掘模型和攻击树推理模型，它们各自具有独特的优势。大数据所面对的工作对象是海量的、混乱无序的安全数据，这些信息会体现出某些特定的统计特征，系统能够通过分析统计特征发现与之对应的网络攻击。算法挖掘模型是分析海量数据中潜在的安全风险。攻击树推理模型是在海量信息数据中将原子级攻击识别并标记出来。在具体工作中分析这些步骤、原子攻击的先后关系等因素，可以将实际的网络攻击行为抽象为攻击链。由于攻击链中包括多个原子级攻击动作、多个基本攻击行为，这些动作、行为按照先后关系、时序关系及因果关系组成，攻击起点、攻击手法及攻击流程不同，所产生的攻击结构也有所不同，根据攻击树模型确定每个攻击行为在整个攻击链中的大致位置。

3.3 数据分析

数据分析的主要作用就是分析数据的流向、行为、脉络及层次，以算法程序层面的数据、实时模型设计及离线数据为主要依据，能够更好地发现海量数据中可能会对网络安全产生威胁的安全风险因素。通常来说，数据分析可以分为在线实时挖掘和离线挖掘 2 个步骤。Spark 框架可以帮助我们快速分析实时数据，并使用它来进行在线实时挖掘。我们首先会收集整个安全区域内的所有防护设施和安全系统的节点信息，然后使用数据仓库技术（Extract Transform Load,ETL）对这些信息进行预处理，并将处理后的信息存储到 Hive 数据库中。最后，我们可以使用命令接口来解析这些信息，并使用 Spark 的实时计算框架进行 RDD 操作。通过分析数据库中的表格，提取有用的文档和数据，并对其进行精确的计算。离线挖掘分析的主要数据是数据库中的历史数据，对数据库中历史数据循环、反复的挖掘实现深加工及累加利用。离线分析模型还需要维护一个来自离线分析的结果与实时分析反馈结果的已知安全事件仓库。

结语：综上所述，大数据技术的飞速发展形成新的网络安全形势，即海量的数据不仅数量大，而且类型多，必然会带来诸如数据分布式存储、数据标准化处理等一系列问题，其中数据源安全问题也是一个重要挑战。安全预测的部署有利于统一管理机构内部的网络安全，实时掌握网络运行的安全状况，并进一步优化网络安全策略。随着科学技术的发展，网络安全安全预测的研究已经取得了长足的进展，但仍然存在许多挑战。因此，为了提升网络安全安全预测的准确性和可靠性，学界必须加强对其理论和实践的探索，并不断改善和完善相关的技术和策略，以期达到最佳的防护效果。

参考文献：

[1]朱丽娜，张作昌，冯 力.层次化网络安全威胁态势评估技术研究 了，计算机应用研究，2018，28(11):78-89.

[2]胡华平，张 怡，陈海涛.面向大规模网络的入侵检测与预警系统研究 [J].国防科技大学学报，2013，25(1):21-25.

作者简介：杨基慧，1980.12，山东招远人，女，汉，硕士研究生，讲师，研究方向：计算机软件。