探讨网络安全分析中的大数据技术应用

张瑞丰
（广东胜通和科技服务有限公司，广东 广州 510665）

摘　要：随着网络技术的不断普及推广，网络中的复杂性也逐渐显现。本文基于大数据技术，对当前网络安全分析中使用大数据搭建平台的方式运用图表做了直观说明，之后仔细探讨了在网络安全分析中对大数据技术的具体应用，具体表现在对数据的采集、查询、储存、分析和复杂数据的处理。通过本文的讨论希望帮助大家能够在网络安全分析中更好地利用大数据技术。

关键词：网络安全；大数据；技术应用
中图分类号：TP393.08　　**文献标识码：**A　　**文章编号：**1004-7344(2022)39-0109-03

0 引言

网络安全问题是互联网运用中最为紧要面临的问题，随着社会发展水平的提高和科技的进步，传统的网络安全分析技术已经不能适应时代的需要，用户的信息不能享有隐私性，网络安全攻击等现象频繁出现，给社会经济造成了极大的不良影响，借此，对大数据技术的合理使用能够将网络安全隐患进行精准控制，并对潜在问题及早发现进行预警，也是网络安全分析的未来发展重点趋势。

1 大数据技术下网络安全分析平台的建立

为了促进大数据技术能够在网络安全分析中充分发挥作用，就要建构一个完善的数据分析平台，以便大数据技术能够在网络安全分析工作中发挥最大的作用。利用大数据技术建构的网络安全分析平台如图1所示。

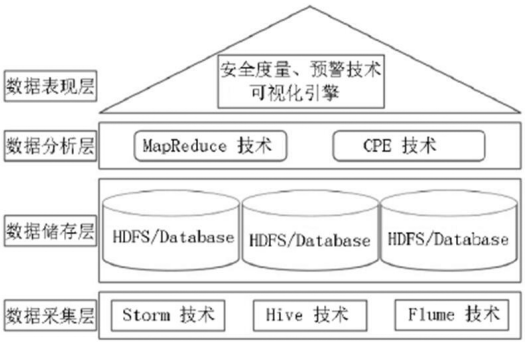

图1 大数据技术的网络安全平台架构

根据图1可以看出，大数据技术下网络安全分析平台主要从四个模块进行，分别是数据采集、数据储存、数据分析以及数据表现。数据采集层在整个分析平台中处于最基层，是将网络用户的行为数据进行采集整合，在大数据技术的支持下，这项工作能够做到更高效。第二层的数据储存，主要的工作就是为采集到的数据提供一个存储平台，以便为之后的分析和展示提供充足的理论基础，帮助网络安全分析工作维持基本的质量保障。第三层即数据分析层，它对于网络安全信息的分析不仅是来自原始数据的分析，还要分析相应的关联数据，以便找出网络安全中潜在的攻击隐患，为之后网络安全分析工作的开展提供一定的参考指导。第四层也就是最终的数据表现层，也可以称为数据展示层，这一层级能够将网络安全数据信息十分直观的表现出来，但是这一层级的实现需要完善的安全分析技术以及可视化技术和风险预警技术，这三项技术的加持才能保证数据展示的全面，缺一不可[1]。

在进行网络安全分析时，分析功能的使用是以数据采集作为基础的，通过大数据对不同类型的网络安全数据进行采集分类，再由数据分析层级按照分析规定实行其分析功能，对用户的数据信息采集是实时的，要通过用户在网络上正在进行的网络活动在线进行，这增加了数据信息的时效性。传统的原始数据采集利用的是离线方式，即在用户已经停止使用网络后对其的网络运行轨迹采集分析。大数据技术可以将在线与离线二者进行结合，利用Flume技术来进行双向采集。

依据大数据技术建立的网络安全分析管理平台，主要是通过对攻击路径的监测来对安全问题进行预警，使用DDoS技术，只要在平台上预先设立程序，系统就会自动对来访的攻击路径进行拦截，并且在此系统运行期间，还会对各项网络安全信息进行自动收集，拓宽拦截路径，并将所获取到的信息输入安全管理平台中，以便DDoS系统在遭受威胁时，安全管理分析平台

能及时发现并作出补救措施。

2 数据技术的应用

2.1 数据采集

网络安全分析工作主要是对采集到的流量等数据进行分析，将大数据技术应用于网络安全分析之中，主要使用的采集工具就是 Flume，这种工具的组成如图 2 所示。

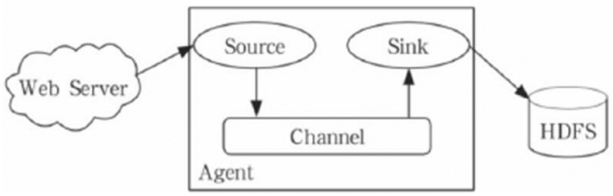

图 2 Flume 技术及其结构组成

Flume 技术在进行网络安全分析数据的采集中能够将在线采集与离线采集充分结合，从而实现采集工作的系统化，并且这项采集技术同时包含了采集和存储两项功能，在实际的应用中具有极高的效率。

2.2 数据查询

在网络安全分析中，对于数据的查询还能充分运用大数据技术，大数据技术能够帮助网络安全数据进行更加高效的查询，这是基于大数据的计算分类特性，其自带的检索能力能够将网络安全分析系统中的数据结构进行不断更新，所要查询的网络安全数据通过大数据的检索端口，经过初步的归类计算后会根据数据的类型特点进行分类，之后再进行系统计算，计算后的结果将直接显示在检索界面上，方便了对网络安全数据的查询。

网络安全数据的查询运用大数据后，其查询手段变的更为便捷，且高效的查询模式也能为客户提供更加全面的数据信息，数据的准确性也得到了极大优化，并且通过大数据技术，网络安全分析工作有了数据基础的支撑，也能得到更好的推广开展[2]。

2.3 数据储存

网络安全分析数据具有传播速度快和类型多样的特点，基于这种特性，使得对于这一类数据的处理难度较高，而对于数据处理的不全面就会导致网络安全分析工作无法得到有效开展。将大数据技术应用到网络安全分析平台中，能够极大程度的降低网络安全分析数据的处理难度，并且大数据基于网络环境，能够为网络安全分析数据提供更加广阔的存储空间，便于网络安全分析工作有效开展。

将大数据技术引用到网络安全分析平台中，其主要的存储工具是 H Base，这种存储工具具有空间大，检索便捷等特点。其读写程式如图 3 所示。

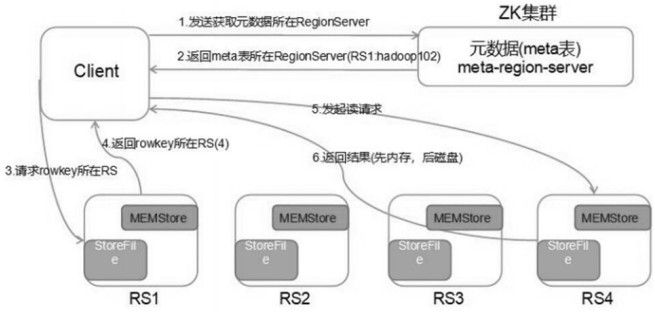

图 3 H Base 读写流程

由图 3 可以看出，这类存储工具能够对网络安全分析数据进行分类存储，极大程度的满足了对网络安全分析数据的使用需求。

利用大数据技术将网络安全分析数据进行处理时，要根据不同的数据特点来使用不同的算法进行计算，之后再利用分类计算的方式，再将分类计算结果进行分析统计，形成最终的储存报告。

2.4 数据分析

2.4.1 分析网络流量

利用大数据技术对网络安全进行分析时，其操作流程为首先使用分析工具进行数据分析，利用存储工具对网络端口的数据流进行采集和监控，之后对采集到的数据进行分析统计，将其中潜在的网络安全风险进行及时的排除，将隐患的可能发生扼杀在摇篮里。

在具体的分析过程中，首先利用 Storm 等专业的数据采集技术对病毒和恶意浏览事件进行规范化的数据采集。其次将采集到的信息利用 Chukwa 分析工具进行多角度分析，将数据中暗藏的风险进行提炼，这种分析工具能够对网络安全数据进行有效的采集，并依照不同数据的特性通过分布式的采集方式，以高效的采集速度进行，有效的提升了网络安全数据的采集效率以及采集准确性。

最后使用 CC 攻击检测等方式，将采集到的含有安全隐患的信息进一步检测分析，判断其中的危险性，并结合当时的网络环境对发现的安全隐患进行防范策略的制定，并使用相关防范工具，以保障安全隐患不会危及到网络运行安全。

2.4.2 分析 APT 攻击数据

针对性攻击对计算机的网络安全有着极高的威胁性，APT 攻击就是其中的代表，我们做了 2015—2019网络遭受 APT 的攻击次数，如图 4 所示。

根据图 4 我们可以看出，随着网络环境使用的越来越广，遭受 APT 攻击的次数也呈现了增长趋势，APT 攻击比之其他的网络安全威胁更加有针对性和潜伏性，并且影响时间较长，破坏性也极大。

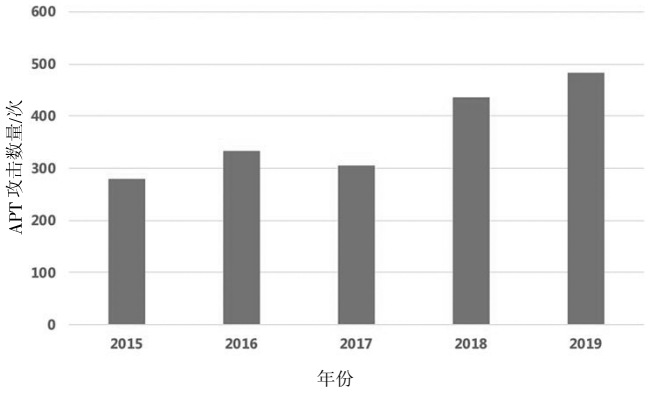

图 4 2015—2019 年网络遭受 APT 攻击数量

利用大数据技术能够将网络运行中的访问日志等流量进行全面的监控，进而将潜伏在其中的 APT 攻击进行发现找出，并且大数据具有自我学习的能力，可以根据既往的数据分析成果对 APT 攻击进行针对性的防御机制的建立，并依据既往数据制定一个遭受 APT 攻击后的拯救措施，进而达到预防的目的。大数据技术的使用还能将网络安全分析的各环节进行实时掌控，对欠缺部分进行及时的改进，切实有效的帮助网络安全提升到一个新高度[3]。

2.4.3 分析安全日志

对安全日志的分析是网络安全分析的核心关键，也是极为复杂的一项工作，大数据技术在目前的网络安全日志分析中主要使用的有 3 种形式。

(1)应用 QRadar 安全管理平台，目前在多数西方国家，利用大数据分析安全日志已经十分普遍，其使用的就是这种安全管理平台，它能将网络中大量的日志源进行集中整合，并在整合的基础上将原始的日志信息进行标准化处理，以便将网络安全中可能存在的隐患揭露的更加直观，并且这样直观清晰地数据处理能够帮助网络安全分析工作更加具有针对性和准确性[4]。

(2)将安全管理平台与威胁数据统计进行整合利用，将二者进行结合能够将网络平台中存在的恶意地址以及黑客轨迹等进行罗列，帮助网络安全管理更加有条理性。

(3)使用数据分析与数据存储相结合的数据仓库，能够将网络安全分析进行流程化的管理，并且从多方下手，分析结果也更为全面。并且基于数据仓库的庞大，其在网络安全信息分析中能够拥有更高的效率，这是传统的网络安全分析手段达不到的，最为明显的一点就是分析时间，传统网络分析技术需要用 30min 才能完成的分析利用数据仓库只需要 1min，效率之高令人赞叹。

2.5 数据处理

传统网络安全分析中对于复杂数据的处理分析是十分费时费力的，效率不高且准确性低，并且由于复杂数据处理起来的难度使得最终的处理结果只在表面而没有进行深度挖掘，更无法发现其中隐藏的潜在价值，例如航空航天等高科技数据信息。将大数据技术进行引用，基于大数据技术庞大的运算能力，能够帮助网络安全分析进行时将其中潜在的具有重大价值的信息挖掘提炼出来，并将其中的潜在风险进行摘除，充分保证了网络整体环境的平稳流畅[5]。

随着网络技术的逐渐进步，复杂数据也会越来越多的出现，伴随着复杂数据出现的就是潜藏在其中的僵尸网络，由于隐匿在复杂数据的环境下，传统的网络安全分析并不能发现，以致网络安全隐患出现，大数据技术能够对数据信息进行多方面的分析，通过多角度的探查能够搜寻到隐匿在复杂网络中的安全隐患，并将探查到的安全隐患进行发散性的关联分析，从而揪出其他潜在的隐患并进行针对性的处理。大数据技术能够确保网络安全分析中各类型的复杂数据都能得到精准分析，以保障网络安全分析工作的高质高效。

3 结语

综上所述，我们可以发现大数据技术的应用能够为网络安全分析带来更多的可能性，在当下网络不断发展的大环境下，网路上的信息存储会越来越多，这些信息关系着客户的隐私和财产安全，只有强化网络安全，才能充分保障每一个上网用户的权益，基于此，必须正确认识大数据技术的优势，将其进行充分发挥，为网络安全的稳定铺垫一个良好的平台。

参考文献

[1] 徐航，张冬冬.大数据技术在网络安全分析中的应用[J].数字技术与应用，2022，40(1)：240-242.
[2] 马晓峰.网络安全分析中大数据技术的标准化利用探讨[J].中国标准化，2022(8)：11-13.
[3] 管延生.大数据技术在网络安全分析中的应用[J].计算机与网络，2021，47(7)：53.
[4] 张洁.网络安全分析中的大数据技术应用分析[J].电脑知识与技术，2022，18(11)：20-21.
[5] 张亚男，罗莹，张政.通信网络安全中大数据技术的应用研究[J].网络安全技术与应用，2021(11)：64-65.

作者简介：张瑞丰(1983—)，男，汉族，广东汕头人，硕士研究生，主要从事 IT 管理工作。