面向大数据的软件定义安全服务

何利文[1] 李杰[1] 陈向东[1] 鲁蔚锋[1] 孔令军[1] 王少辉[1] 黄俊[1]
[1]南京邮电大学，南京 210023
(helw@njupt.edu.cn)

Software Defined Security Services for Big Data

He Liwen[1], Li Jie[2], Chen Xiangdong[1], Lu Weifeng[1], Kong Lingjun[1], Wang Shaohui[1], and Huang Jun[1]
[1](School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, 210023)

Abstract Big data technologies are changing the traditional information security systems and their successful use will require new security models and new security design approaches to address emerging security challenges. This paper gives a detailed analysis of the new problems which the information security service system faced at three points: "client"、"connection" and "cloud", and proposes a "client-connection-cloud" information security system architecture for big data. The construction of information security and service system uses the method of separating terminal, network and cloud platform. By the layered uncoupled architecture, different level realizes the security service.

Key words big data; cloud computing; virtualization; software defined security(SDS); information security

摘要 大数据（Big data）技术的普遍应用正在改变着传统的信息安全体系，因此需要设计新的信息安全模型和新的信息安全处理方法来面对新型信息安全挑战。本文从"端"、"管"、"云"三个层面出发，详细分析了信息安全服务系统所面临的新问题，提出了一种面向大数据的软件定义安全服务的体系架构，采用终端、网络、云平台相分离的方式构建信息安全服务系统，通过分层解耦合架构，在不同层面实现安全能力的服务化。

关键词 大数据；云计算；虚拟化；软件定义安全；信息安全

信息时代的到来，信息技术在社会生产和社会交流各个领域中的广泛应用，给信息安全带来了很多问题，信息安全已经成为了信息时代国家安全最突出、最核心的问题[1]，信息安全问题及其所产生的价值已经开始得到了学术界、工业界以及政府部门的高度关注。2012 年 3 月，美国政府推出"大数据研究与开发计划"[2]，通过提高从海量数据中提取知识和观点的能力，从而加快科学与工程发现的步伐，加强美国的信息安全，实现教育与学习方式的转变。从国家安全战略层面来看，大数据安全问题已对美国国家信息安全造成了战略和战术方面的双重重大挑战。美国有关机构对大数据投入巨资，其目的是解决美国军事和国家安全中的大数据挑战，提升维护美国国家安全和信息网络安全的能力[3]。2011 年 11 月，英国政府公布了《网络安全战略》，该战略继承了 2009 年发布的《英国网络安全战略》，旨在提出切实可行的网络安全实施计划和方案，通过保障网络安全促进经济的繁荣发展。2011 年德国发布《德国网络安全战略》，旨在大力推动安全网络空间的建设，通过推动德国网络空间的战略部署于执行保障体系，保障经济与社会的健康发展。2013 年 5 月，日本"信息安全政策会议"制定了"网络安全"最终草案，针对日益复杂的网络

攻击，草案提出了多项网络信息安全强化措施，其中包括在自卫队设立“网络防卫队”。“棱镜门”事件以来，各国政府对信息安全的重视也已上升为国家安全的高度。基于国际社会信息安全面临严峻考验的大背景，2014 年 2 月，中央网络和信息化领导小组宣告成立，在北京召开的第一次会议上，习近平总书记提出了“没有网络安全就没有国家安全，没有信息化就没有现代化”的国家信息安全核心思想。由此可见，对政府而言，提高信息安全防护能力，增强信息安全事件的检测能力和事后追责处置能力，是政府推动国家信息安全建设的所要面对的首要问题。能否确保信息安全平台的机密性、完整性、可用性，将很大程度影响到整个国家的信息安全和经济的健康发展。

目前，随着数据存储技术、数据传输技术、数据分析技术以及计算技术的进步，信息技术领域的大数据（Big Data）[4-7]时代已经到来，作为虚拟化、物联网、云计算等新型信息处理技术的逻辑衍生产物，大数据具有规模性（Volume）、多样性（Variety）、高速性（Velocity）和价值性（Value）4 个“V”的特性[8,9]，是指无法在一定时间内用传统数据库软件工具对其内容进行抓取、管理和处理的数据集合[4]。由于大数据具有深度挖掘的能力，可以被广泛应用在信息控制、信息传输、信息处理等领域，因此，通过大数据分析技术可以为信息处理领域的各种问题提供新的解决思路，例如通过大数据分析技术来提高各信息系统的安全。信息安全问题贯穿于大数据产业链的各个环节，主要包括终端（Client）、网络（Connection）、业务（Cloud）三大基础领域，对应信息终端控制系统的安全[10,11]、信息传输网络的安全[12-14]和云计算的安全[15]。终端、网络和业务三者在信息安全领域的发展具有一些内在的规律和辩证的关系，在面向大数据的信息安全问题的研究当中，需要正确把握这些规律，综合考虑终端、网络和业务的关系，协同解决。

除此之外，近年来随着软件定义网络（Software Defined Networks, SDN）技术[15]的提出和开放式网络基金会(Open Networking Foundation, ONF)在其开源项目上的贡献，学术界和工业界开始关注 SDN 技术在信息安全领域的应用，即软件定义安全(Software Defined Security, SDS)[16]。本文依据当前信息安全领域的新形势，从“端-管-云”整体协调的思想出发，剖析终端控制系统、信息传输网络和云计算的信息安全问题，提出了一种面向大数据的软件定义安全服务架构，从而为提高各生产、生活等领域信息系统的安全提供一种有效地解决方案，保障社会资源安全。

1. 相关关键技术

1.1 软件定义安全

软件定义安全(Software Defined Security, SDS)是 SDN 技术在信息安全领域的延伸，原理是将物理及虚拟的网络安全设备与其接入模式、部署方式、实现功能进行了解耦，底层抽象为安全资源池里的资源，顶层统一通过软件编程的方式进行智能化、自动化的业务编排和管理，以完成相应的安全功能，从而实现一种灵活的安全防护[17]。就工作机制而言，SDS 可以分解为软件定义流量、软件定义资源、软件定义威胁模型，三个举措环环相扣，形成一个动态、闭环的工作模型：

软件定义流量：由软件编程的方式来实现网络流量的细粒度定义及转发控制管理，通过将目标网络流量转发到安全设备上，来实现安全设备的逻辑部署和使用。

软件定义资源：通过管理中心对安全资源进行统一注册、池化管理、弹性分配，在虚拟计算环境下，管理中心还要支持虚拟安全设备模板的分发和设备的创建。

软件定义威胁模型：对网络流量、网络行为、安全事件等信息进行自动化的采集、分析和挖掘，实现对未知的威胁甚至是一些高级安全威胁的实时分析和建模，之后自动用建模结果指导流量定义，实现一种动态、闭环的安全防护。

1.2 大数据安全分析技术

大数据安全分析，简单来说就是通过对数据包、网络流量和元数据的持续处理，查找出那些可能属于非法或可疑网络活动，从而实现安全事件的“事中”发现和响应。就工作机制而言，大数据安全分析包括数据的采集、数据的预处理、分布式存储、分析挖掘和可视化展示几个环节，具体为：

(1) 数据采集与预处理

大数据环境中，数据主要分为结构化数据、半结构化数据和非结构化数据，同时数据又具备实时和非实时性的特征，因此在大数据的采集与预处理过程中会采用一些与传统数据不同的方法和工具，其中比较重要的环节便是数据 ETL（Extract Transform load, 提取、转换、加载）过程。ETL 负责将分散的、异构的数据源中的数据抽取到临时中间层以后、进行清洗、转换、集成，最后加载到目标数据库或者相应的文件存储系统中，作为数据分析和挖掘的基础。

(3) 分布式存储

在大数据领域中，典型的分布式存储技术有 Google 的 GFS 和 Hadoop 的 HDFS，其中 HDFS 是在

Google 公开发表的论文基础上的开源实现。GFS 和 HDFS 均采用主从控制模式，即主节点存储元数据、接收应用请求并且根据请求类型进行应答，从节点则负责存储数据。当用户访问数据时，与主节点交互的只有指令，并根据主节点返回的数据存储位置，直接与存储节点交互获得数据，避免主节点出现瓶颈。在大数据场景下，通常采用 NoSQL 数据库来消除关系数据库的关系型特性，以简化数据库结构。

(4) 分析挖掘

大数据分析挖掘技术的典型代表是 Hive 和 Mahout，其中 Hive 是一个基于 Hadoop 的 PB 级数据仓库平台，在 Hadoop 之上管理和查询结构化数据并完成海量数据挖掘。Hive 定义了一个类似于 SQL 的查询语言 HQL，能够将用户编写的 SQL 转化为相应的 MapReduce 任务来运行，这样，习惯于使用 SQL 的用户，也能够方便地完成并行计算。Mahout 是一个机器学习与数据挖掘算法库，提供了一些可扩展的机器学习领域经典算法的实现，如集群、分类、推荐过滤等，与 Hadoop 结合后可以提供分布式数据分析挖掘功能。

(5) 可视化分析

大数据可视化分析旨在利用计算机自动化分析的能力，充分挖掘人对可视化信息的认知能力借助人机交互式分析方法和交互技术，辅助人们更为直观和高效地洞悉大数据背后的信息、知识与智慧[18,19]。支持大数据可视化分析的基础理论主要包括认知理论模型、信息可视化理论模型、用户界面理论模型等，具体包括文本可视化、网络可视化、时空数据可视化、多维数据可视化等。

2. 信息安全问题

2.1 终端控制系统安全问题

目前，各种设备终端越来越呈现智能化或者集成化，并且与互联网或者云平台广泛连接，以及与信息管理系统相集成，产生了大量的信息交互需求，从而给信息安全带来了潜在的威胁。其中，比较典型是工业控制系统面临的信息安全问题[10,11,21-23]。例如，2010 年伊朗什尔核电站遭到的“震网病毒”（Stuxnet）攻击[24]，集中于中东地区工业系统的“火焰病毒”（flame）攻击等。概括来说，工业控制系统中，常见的安全事件主要有：1）对 PLC(可编程逻辑控制器)、DCS（分布式控制系统）或者 SCADA(数据采集与监视控制系统)中的程序指令进行非授权修改；2）对控制系统中软件或者配置进行修改；3）在控制系统中安装恶意软件等。一个大型的工业控制系统中往往可能遭受以上几种方式的组合攻击，控制系统中遭受的这些安全问题通常是经过周密策划和实施，针对特定对象进行长期的、有计划的攻击，具有高度的隐蔽能力、潜伏期长、攻击路径和渠道不确定，比较典型的是高级持续攻击（Advanced Persistent Threat, APT）[25]，APT 入侵的途径主要是把包括控制器、可编程逻辑控制器、远程终端单元、组态编程软件、数据采集与监视控制系统，以及智能手机、平板电脑等终端作为入侵和攻击的对象。通过零日攻击获取 APT 权限，注重对其动态行为和静态文件的隐蔽，攻击的渠道多元化，难以实施检测和采用单一的技术手段来对信息系统进行防护，往往造成比较严重的信息安全事件。

2.2 信息传输网络安全问题

信息传输网络主要包括有线网络和无线网络，有线网络的安全问题主要包括：电磁安全，设备安全、链路安全、信令网安全、同步系统安全、终端安全、网络业务安全、网络资源安全、流量冲击、通信内容安全、有害信息扩散等。面临这些信息安全威胁，有线网络安全可以分为网络自身安全、业务提供安全、信息传递安全和有害信息来控制四个层面。针对这四个层面，为了消除有线网络领域的安全威胁，以及满足企业和用户的各种合规性安全要求，安全业界推出了各种各样的有线网络安全解决方案，主要有：防火墙技术、数据防护技术、入侵检测技术、抗攻击网关技术、网络溯源技术等[26]。无线网络主要是指无线传感器网络或者移动通信网络，其安全特征与有线网络有所不同，相对有线网络，无线网络的安全问题更加复杂，其主要原因是无线信号具有广播特性，从而可以被截取、篡改、甚至是伪造等[27]。

针对信息传输网络，一种典型的攻击方式是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应，通过扰乱传输网络系统中的流量信息来使系统崩溃。具体的攻击方式是通过向服务器发送大量的连接请求，从而造成服务器无法正常应答而瘫痪，或者伪造虚假的 IP 地址发送连接请求，使得服务器的应答无法送达目的地址，从而产生海量的垃圾数据占用服务器的空间和阻塞信息通信通道。典型的攻击方式称之为分布式拒绝服务攻击（Distributed Denial of Service, DDoS）[28]。DDoS 借助客户/服务器技术，通过采用分布式的方式控制分散的信息系统或者智能信息终端，将多个计算机终端联合起来作为攻击平台，对一个或者多个信息目标发动信息拒绝服务攻击，从而成倍地发挥信息拒绝服务攻击的破坏力，对信息传输网络具有极大的潜在威

胁。

2.3 云计算安全问题

云计算是当前信息技术领域关注的焦点，它体现了网络即计算机（Network as a Computer, NaaC）的思想，通过虚拟化技术，将大量存储资源、软件资源与计算资源链接在一起，形成巨大的共享资源池，从而为用户提供一种便捷化的 IT 服务。然而，随着云计算技术的不断普及和推广，云计算安全问题开始成为云计算服务中不可避免的重要问题。就云计算的三种服务模式而言，IaaS(Infrastructure as a Serive)基础设施及服务涉及到的信息安全主要体现在服务器、存储和网络硬件及其相关软件等方面，PaaS(Platform as a Service)平台及服务的信息安全主要体现在操作系统、访问控制、数据传输以及数据安全等方面，SaaS(Software as a Serive)软件即服务的信息安全除了 IaaS 和 PaaS 所面临的信息安全问题之外，还需要特别关注多租户应用数据安全的保护等问题[29-32]。具体而言，云计算所面临的安全问题主要包括账户控制、多租户问题、数据控制问题、恶意攻击以及管理控制台安全等[29]。总结起来主要有：1）云计算服务计算模式引发的安全问题；2）云计算的动态虚拟化管理方式引发的安全问题；3）云计算中多层服务模式引发的安全问题[1]。

由于缺少相对应的安全技术的支撑和研发周期长，当前云计算商业服务还不十分重视云计算信息安全方面的投入，但长远来看，云计算安全问题的解决是保证云计算服务正常运营的根本途径，值得关注。

2.4 大数据自身的信息安全问题

大数据的产生主要依赖于互联网时代爆棚式的崛起，网络中各种网络阅读器、行业专用终端、带网关/存储功能的家庭服务器、第四屏（平板电脑、网络盒子）等终端的应用产生了大量的用户数据，这些用户数据经由信息通信网络连接上互联网或者云计算平台，再通过网络或者云计算平台中的软件（SaaS）进行转换，从而实现用户的信息消费需求。大规模的数据生产、分享和应用给用户的生活和工作带来了极大便利，但由此产生的海量数据也给信息安全的保护带来了新的挑战。

从技术角度来看，由于大数据包含了大量的非结构化或者半结构化的数据（例如文本、音频、视频数据），主要采用 NoSQL 类数据库（非关系类数据库）技术来解决传统关系数据库的查询和索引技术在大数据处理中受限制的问题，从而实现大数据存储的可扩展性、可用性和灵活性[33]。关系型数据经过长期的改进和完善，设置了相对严格的数据访问控制和隐私管理体系，而在 NoSQL 数据库技术中还没有形成做这样的数据安全维护机制。另外，由于数据的非结构化和半结构化特征，数据状态分散，NoSQL 数据库需要不断对数据添加属性，其前瞻安全性变得异常脆弱。

大数据的核心价值是海量数据的分析与利用，从大数据分析的角度来看，大数据采用数据挖掘、机器学习等数据分析技术在给商业应用带来价值的同时，也面临着极大的信息安全与隐私泄露风险。大数据时代，数据的共享与分析将成为未来大数据应用模式的趋势，数据运营商既是数据的生产者，又是数据的存储、管理和使用者，用户对信息数据的收集、存储、管理和使用均缺少规范和监管，用户不可能完全屏蔽自己的信息，更无法通过单纯的技术手段来限制运营商对用户数据的使用，从而给数据运营商或者黑客掌握和使用用户信息的可能性，造成用户信息数据的泄漏[34]。

大数据背景下，用户面临的信息安全威胁不仅仅局限于个人隐私的泄漏，还在于基于大数据的用户状态和行为的预测[35]。数据运营商或者黑客运用其所掌握的用户信息进行深入挖掘和分析，从而更加准确地掌握用户的行为方式，精准投送运营服务或者黑客攻击，从而极大地威胁用户的信息安全。另外，由于大数据的价值密度极低、刻意伪造数据、人工干预数据的采集、数据的多媒介传输等因素的影响，数据来源的真实性、数据传输路径、数据加工处理的工程均会导致数据的可信性降低,出现一些无意义或者错误的数据，最终影响到信息应用系统安全。

3 面向大数据的软件定义安全服务架构

2010 年 9 月，华为在中国国际信息通信展览会上，首次提出以“云-管-端”的模式来重塑 ICT（信息、通信、技术）产业的理念。其核心理念是通过将未来通信与消费的世界的业务 IT 化、网络 IP 化、终端智能化的方式，形成一个“云-管-端”协同的世界。大数据时代，终端早已由原来具备简单的通话或者数据采集功能逐步转化为了与网络、业务和应用相融合的智能化终端，承载了大量的用户信息，其终端的开放性和灵活性给信息安全的保护提出了极大地挑战。随着终端数量和类型的极大丰富，终端互联越来越普遍，出现了低功耗传感网和高可靠的移动互联网、无线传感器网络等，并且出现了大量以终端类型聚类的应用，形成了互联的延伸网络“物联网”。用户的信息通过智能化的管道进行传输，一方面提供了强大的业务处理能力，另一方面也给带来了新的信息安全问

题。云计算平台是信息服务的核心，云计算平台由云计算技术将各种各样的资源以服务的方式通过网络交付给用户，云计算应用的用户和信息资源高度集中，从而造成较高的安全风险，安全事件的后果较传统应用要高出很多。

面向大数据的信息安全分析是主要是通过收集和分析信息终端、信息传输网络和云计算平台中产生的海量与安全相关的数据，采取实时的安全关联分析，以检测系统的漏洞和防御入侵，保障信息系统的安全。本文依据大数据的关联分析能力，从“端-管-云”整体架构的思想出发，将“端”、“管”、“云”三部分进行解耦合，采用 SDN 技术，虚拟化技术，提出了一种面向大数据的“端-管-云”的软件定义安全（Software Defined Security, SDS）服务架构，通过将各部分的实现细节进行抽象后，构建出统一的系统架构如图 1 所示：

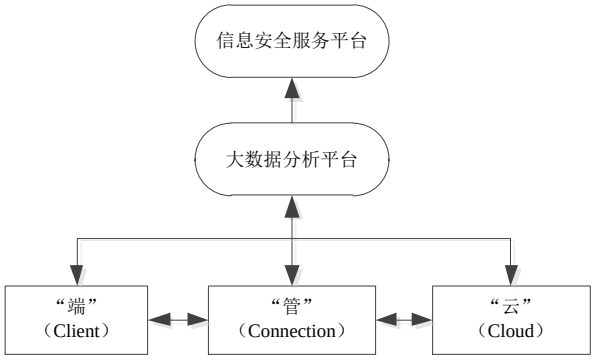

图 1　面向大数据的“端-管-云”信息安全服务架构

图 1 所示的面向大数据的“端-管-云”信息安全体系架构，既清晰地展现了信息安全系统宏观层次的统一性，又保留了各业务单元细节实现上的灵活性。信息安全管理平台采用“端”、“管”、“云”分离的方式构建面向大数据的信息安全服务体系，通过这样的分层解耦合架构，在“端”、“管”、“云”三个不同的层面采用软件定义的控制逻辑，从而实现安全能力的服务化。通过深度分析接口，根据策略按需导入信息系统的流量数据到大数据安全分析平台，对需要进行深入分析的数据进行基于大数据技术的存储和挖掘，通过对一个时间窗口和空间范围内大量的数据持续关联分析，检测和发掘出信息系统面临的信息安全问题。

面向大数据的信息安全服务系统的核心是以强大的云计算能力提供安全服务，利用大数据处理技术挖掘深层安全问题，同时为传统物理网络和基于云计算技术的虚拟化网络提供安全服务。安全服务模型的定义、安全服务生命周期的管理、安全服务包的的封装、安全服务的交付、安全服务的度量、安全资源池的构建、安全服务框架的实现、虚拟化网络内部网络流的抓取和引导、基于网络流存储的大数据检测分析等。

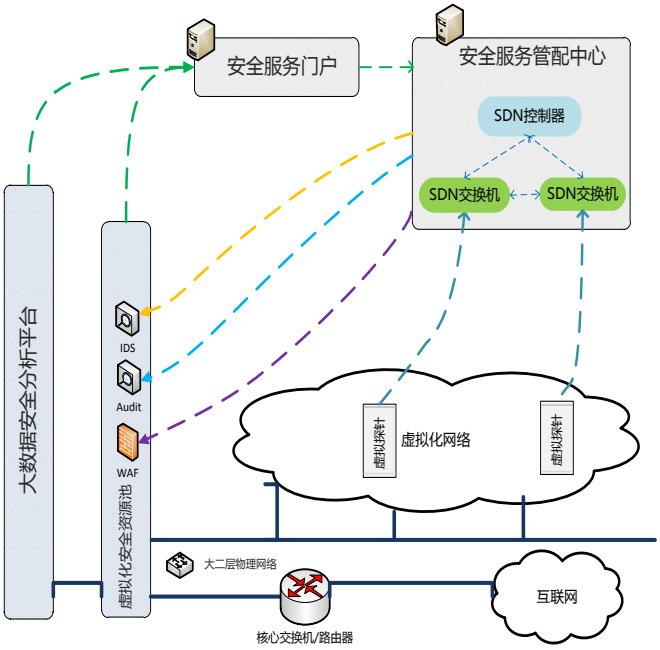

图 2　面向大数据的软件定义安全服务平台架构

图 2 给出了面向大数据的软件定义安全服务平台的部署架构。图中安全服务门户主要解决服务可视化问题并向用户提供软件定义安全服务的人机交互接口。安全服务的交互接口为用户提供了对服务的选择、定制，如用户从其网络中划分一个 vlan，并为该 vlan 部署一个防火墙和一个 Web 应用网关，即以这个 vlan 为服务对象，选择了防火墙和 WAF 服务，并可以为其所选择的服务制定需要处理的网络流量大小。

安全服务管配中心主要实现对安全服务内容的封装和管理。通过网络流量的导流和分流实现安全服务的配置，即把需要提供服务的流量从网络中抓取或者引导出来，送往安全服务平台下的安全服务资源池进行安全服务。流量抓取和导引的方式是通过修改 SDN 交换机的配置或嵌入 openflow 规则来改变特定网络流的流向，从而实现流量的导出。

虚拟化平台主要实现安全服务的配置。信息安全系统把需要提供服务的流量从网络中抓取或者引导出来，送往安全服务平台下的安全服务资源池，并通过大数据安全分析平台对所抓取的流量进行分析，从而实现精准的信息安全服务。流量抓取和导引的方式主要有两种：一种是通过自动化的配置一个连接在虚拟交换机上的虚拟机来实现对同虚拟网络内流量的抓取；另外一种是通过修改虚拟交换机的配置或嵌入 Openflow 规则来改变特定网络流的流向，从而实现

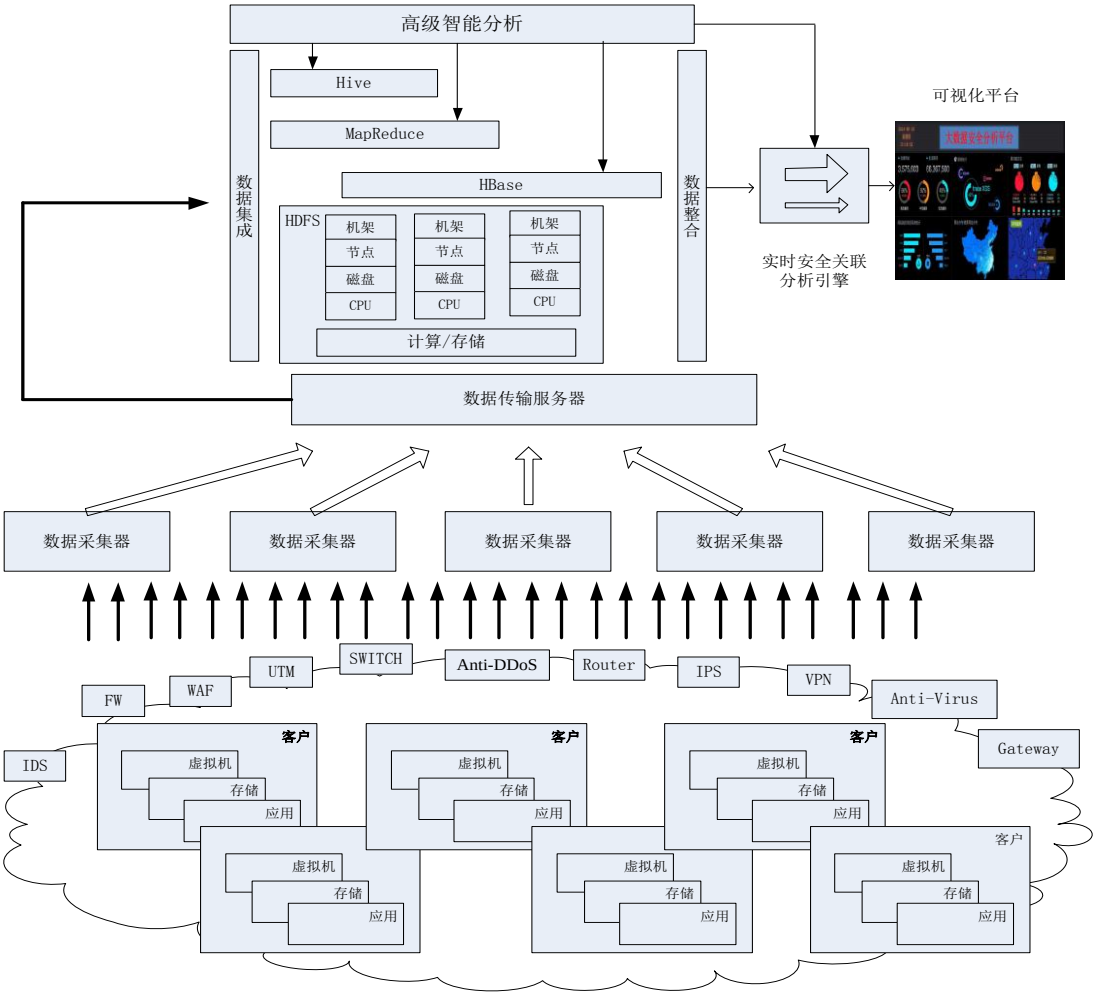

图 2　大数据安全分析平台架构

流量的导出。为了能够实现平台无关性，本文描述的信息安全服务系统采取封装开源云管理平台——Openstack 的 API 的方式来实现对 VMWare、Xen 和 KVM 等云平台的兼容。在虚拟化平台设计中，通过对 Openstack 平台的封装，提供了一个专门用于安全服务配置的 API，与第三方软件解耦合，从而可以方便地实现信息安全服务系统的升级改造。

安全服务资源池是提供安全服务的实体，也是构建安全服务系统的核心。本项目中以网络流量作为度量安全服务的单位，通过流量抓取和引导的方式把流量导入到资源池中，而最终用于实现安全功能的是传统的物理安全设备，即在安全服务实施的整个过程中，网络流是被服务的对象，因此本项目采用支持 Openflow 规则的 SDN 交换机来构建安全资源池的服务承载通道。这样整个安全服务就由服务对象、承载通道和服务实施端构成，其中服务对象是通过软件定义的安全域，由部署在网络中的虚拟探针或导流产品按照安全域的划分把属于一个安全域的流量抓取或引导到一个承载通道中；承载通道在 SDN 交换机中以流的方式来实现，通过对安全策略转换而来的 openflow 规则的控制，来把符合特定规则的网络流引导到对应的网络接口上，而此接口所连接的即是物理的安全设备，如 IDS、UTM 等；服务端实施端的安全设备包括所有旁路接入和串行接入的常规物理网络安全产品。对于不支持自身虚拟化的安全设备，采用一组轻量级如 10 兆或百兆级别的设备组成资源池，基于 openflow 协议对接入端口的负载进行控制，来实现按需的安全服务的伸缩能力。

全网络流存储可以有效的实现事后的取证和分析，特别在对于云计算这样一个相对较为陌生，安全问题处于不断被暴露和被挖掘过程中的环境中，而对于如 APT 等有特定目的性的、多阶段的高级攻击手段的检测也具有较通常实时监控的安全方法具有更好的检测能力。对存储的网络流的检测相对于实时的检测将会是大数据级别的，这里需要在存储策略、存储方式、检测分析方法等方面进行相应的研究和探索，以实现充分利用大数据平台的强大分析能力，快速有效的从海量数据中获取真正有用的信息。图 3 详

细描述了图 2 介绍的大数据安全分析平台的总体架构，如图中所示，大数据安全分析平台不断采集来自信息终端控制系统、信息传输网络和云计算平台的安全事件进行存储，并对所采集的数据进行集成、映射、关联和约简等一系列的大数据分析处理，最终通过高级智能化的大数据安全分析实现对信息安全事件的检测和深度挖掘。

面向大数据的软件定义安全服务的核心是利用大数据分析技术对软件定义网络中的安全事件进行实时关联分析，通过大数据安全分析平台对安全事件构建海量信息安全事件库以及海量历史安全事件库，并对海量安全事件数据进行深度挖掘，最终实现高效、精准的面向大数据的软件定义安全服务。

4 结束语

信息安全技术和服务将是未来保障各种信息系统安全可靠的根本。因此，在信息技术高速发展的今天，发展我国自主可控的信息安全服务已经到了刻不容缓的地步。大数据给信息安全带来了新的挑战，但其本身也是解决信息安全问题的重要手段。本文从终端、网络和云计算三个层面详细分析了信息安全服务所面临的挑战，提出了一种面向大数据的软件定义安全服务的体系架构，从底层技术上解决大数据在云计算信息安全上自主可控的问题，提升信息安全产品以及专业化服务水平，增强信息系统的自主可控能力，保障国民经济和社会信息化的健康快速发展。

参 考 文 献

[1] 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83

[2] Big Data Across the Federal Government [EB/OL]. [2012-3-29]. http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf

[3] 陈明奇, 姜禾, 张娟, 等. 大数据时代的美国信息网络安全新战略分析[J]. 信息网络安全, 2012 (8): 32-35.

[4] Manyika J, Chui M, Brown B, et al. Big data: The next frontier for innovation, competition, and productivity[J]. 2011

[5] Howe D, Costanzo M, Fey P, et al. Big data: The future of biocuration[J]. Nature, 2008, 455(7209): 47-50

[6] McAfee A, Brynjolfsson E, Davenport T H, et al. Big Data[J]. The management revolution. Harvard Bus Rev, 2012, 90(10): 61-67

[7] Brown B, Chui M, Manyika J. Are you ready for the era of ‘big data’[J]. McKinsey Quarterly, 2011, 4: 24-35

[8] Beyer M A, Laney D. The importance of'big data': a definition[J]. Stamford, CT: Gartner, 2012

[9] Villanova University. What is big data? [EB/OL]. http://www.villanovau.com/resources/bi/what-is-big-data/#.VAbAa_mSmSz

[10] Stouffer K, Falco J, Scarfone K. Guide to industrial control systems (ICS) security[J]. NIST special publication, 2011: 800-82

[11] Alcaraz C, Fernandez G, Carvajal F. Security aspects of SCADA and DCS environments[M]//Critical Infrastructure Protection. Springer Berlin Heidelberg, 2012: 120-149

[12] Slijepcevic S, Potkonjak M, Tsiatsis V, et al. On communication security in wireless ad-hoc sensor networks[C]//Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on. IEEE, 2002: 139-144

[13] Liu J, Xiao Y, Li S, et al. Cyber security and privacy issues in smart grids[J]. Communications Surveys & Tutorials, IEEE, 2012, 14(4): 981-997

[14] Pervaiz M O, Cardei M, Wu J. Routing security in ad hoc wireless networks[M]//Network Security. Springer US, 2010: 117-142

[15] Monsanto C, Reich J, Foster N, et al. Composing Software Defined Networks[C]//NSDI. 2013: 1-13.

[16] Li C, Brech B L, Crowder S, et al. Software defined environments: An introduction[J]. IBM Journal of Research and Development, 2014, 58(2): 1-11.

[17] 裘晓峰, 赵粮, 高腾. VSA 和 SDS: 两种 SDN 网络安全架构的研究[J]. 小型微型计算机系统, 2013, 34(010): 2298-2303.

[18] 任磊, 杜一, 马帅, 等. 大数据可视分析综述[J]. Journal of Software, 2014, 25(9).

[19] Staff C. Visualizations make big data meaningful[J]. Communications of the ACM, 2014, 57(6): 19-21.

[20] Ryan M D. Cloud computing security: The scientific challenge, and a survey of solutions[J]. Journal of Systems and Software, 2013, 86(9): 2263-2268

[21] Krotofil M, Gollmann D. Industrial control systems security: What is happening?[C]//Industrial Informatics (INDIN), 2013 11th IEEE International Conference on. IEEE, 2013: 670-675

[22] Rahimi S, Zargham M. Analysis of the security of VPN configurations in industrial control environments[J]. International Journal of Critical Infrastructure Protection, 2012, 5(1): 3-13

[23] Ericsson G N. Cyber security and power system communication—essential parts of a smart grid infrastructure[J]. Power Delivery, IEEE Transactions on, 2010, 25(3): 1501-1507

[24] Langner R. Stuxnet: Dissecting a cyberwarfare weapon[J]. Security & Privacy, IEEE, 2011, 9(3): 49-51

[25] Tankard C. Advanced Persistent threats and how to monitor and deter them[J]. Network security, 2011, 2011(8): 16-19

[26] Estevez-Tapiador J M, Garcia-Teodoro P, Diaz-Verdejo J E. Anomaly detection methods in wired networks: a survey and taxonomy[J]. Computer Communications, 2004, 27(16): 1569-1584.

[27] Li M, Lou W, Ren K. Data security and privacy in wireless body area networks[J]. Wireless Communications, IEEE, 2010, 17(1): 51-58

[28] Arunmozhi S A, Venkataramani Y. DDoS Attack and Defense Scheme in Wireless Ad hoc Networks[J]. arXiv preprint arXiv:1106.1287, 2011

[29] Zissis D, Lekkas D. Addressing cloud computing security issues[J]. Future

Generation Computer Systems, 2012, 28(3): 583-592

[30] Li Y A, Wu J B. An SLA based SaaS Security Level[J]. TELKOMNIKA Indonesian Journal of Electrical Engineering, 2013, 11(7): 4111-4121

[31] Vaquero L M, Rodero-Merino L, Morán D. Locking the sky: a survey on IaaS cloud security[J]. Computing, 2011, 91(1): 93-118

[32] Rodero-Merino L, Vaquero L M, Caron E, et al. Building safe PaaS clouds: A survey on security in multitenant software platforms[J]. computers & security, 2012, 31(1): 96-108

[33] Cattell R. Scalable SQL and NoSQL data stores[J]. ACM SIGMOD Record, 2011, 39(4): 12-27

[34] Mayer-Schönberger V, Cukier K. Big data: A revolution that will transform how we live, work, and think[M]. Houghton Mifflin Harcourt, 2013.

[35] 冯登国, 张敏, 李昊. 大数据安全与隐私保护[J]. 计算机学报, 2013, 37(1): 246-257

何利文，男，1968 年生，教授，研究方向：网络与信息安全、图像处理、云计算和大数据的技术与应用等。1996 年赴英国谢菲尔德大学攻读博士学位，1999 年加入英国电信，2004 年任英国电信首席安全研究员，2010 年任华为公司存储与网络安全产品线安全首席技术官和公司信息安全高端专家委员会专家，2012 年以“第二层次的高层次人才”、校长特聘教授加入南京邮电大学。IEEE 高级会员、全国青联 IT 联谊会常务理事、中国计算机学会大数据专家委员会委员。