基于云平台的大数据信息安全保护策略分析

王　权
（武威职业学院，武威 733000）

摘要：随着互联网＋政策的逐渐深入实践，基于云平台的硬软件系统的研发速度也迅速提高。政府、企业都开始建立和建设服务云平台，但是云平台的大数据信息安全仍然是技术难题之一。许多传统的安全防护手段和策略对于此类应用场景都失去了效用，因此需要重新考虑和实施信息安全保护的策略。

关键词：云计算；大数据；信息安全保护
doi：10.3969/J.ISSN.1672-7274.2019.09.070
中图分类号：TP309　　**文献标示码：**A　　**文章编码：**1672-7274（2019）09-0093-02

1 引言

云平台是一种新型的软件部署架构，能够与大数据技术相结合，设计研发相关大数据产品。大数据可以针对各行各业的相关数据进行处理分析挖掘，还能够为企业带来很多经济效益，云平台可以承载大数据的数据量，也是许多企业青睐的部署方式。但是现在大数据的利用率仍然不高，很多企业不知道如何使用大数据中的信息，并且大数据信息安全层面也会面临很多威胁，因此需要从多个层面对云平台的大数据信息进行安全保护。

2 云平台和大数据概述

大数据近些年的应用范围非常广泛，应用速度也很快，大数据的发展层面已经非常广泛，它已经不仅仅是单纯的应用到IT行业的发展中，而是应用到全社会各类企业的发展中，利用大数据对重要数据的处理方式体现出其快捷高效的优势。大数据不仅在对庞大信息量的处理方式中能够游刃有余，而且对于多种类、各种类型的复杂性的资料和数据也能高效完成，大数据的应用规模及复杂程度远远超出了普通数据处理的能力。大数据的发展和存在在我国信息社会的不断发展过程中是非常有必要的，显得非常有意义，对企业的高效发展提供了快速而有效的关键技术，从而能够保障企业的可持续发展。

云平台是一个可以利用自身的容纳性强、运行速度快的特点通过互联网对大量的数据进行计算的平台，云计算在对大量的复杂型数据进行处理时会按照一定的准则将不同的数据分布到不同的计算机中进行处理操作，这不仅能够在短时间内处理大量的数据信息，还能够提升数据处理速度，特别适合数据密集型的计算。

基于云平台的大数据软件是一个复杂的生态系统，而大数据软件基础支撑平台是支撑这个复杂生态系统可持续发展的核心。因此，要求大数据软件基础支撑平台能充分反映最新大数据技术和DaaS的发展趋势，并能随着这些发展趋势的发展而发展，从而确保大数据软件平台能可持续发展。大数据软件平台要具备全面且功能强大的大数据感知与获取能力，至少具备能从业务信息系统、智能设备、数字设备、互联网上感知和采取数据的能力，并且能够持续对源数据进行采集和获取。源大数据在获取时难免会夹杂一些噪声，因此要对源数据进行筛选和清洗。大数据的种类繁多，同构数据和异构数据都会存在源数据中，因此会对大数据后续分析操作进行干扰，影响到数据处理的准确性、一致性以及完整性原则。大数据软件平台需要具备强大的数据清洗功能，能够对同构数据和异构数据进行分类和清洗标准化等处理。另外一方面，通过预处理后的数据必须能具备保真性和可溯源性，并能够为后续的数据存储、分析与挖掘、访问与服务、展示与可视化、治理，还能够对数据安全保护进行设置。大数据软件平台最重要的功能是对数据进行分析和挖掘，也是大数据技术核心体系的体现，在大数据技术中，数据处理分析挖掘都是比较重要的步骤，也是体现数据价值的方式。大数据软件平台可以对大数据进行智能化的分析，并能提供功能较为完善的数据挖掘功能。平台具有完善数据分析与数据挖掘接口，不但能使用业界主流的数据分析与数据挖掘工具，而且能使用业界主流的数据分析与数据挖掘语言。

3 信息安全保护策略

针对基于云平台的大数据软件的基本情况，对于大数据信息安全保护的策略主要有建立安全保护制度、提高安全意识、设置防火墙以及研发入侵检测系统等方面。

3.1 建立大数据信息安全保护制度

目前没有特别成熟的大数据信息安全保护制度，大数据信息在企业、政府等多种应用场景的适用范围并不受到保护和约束。企业政府之间的数据共享、数据控制以及数据所有者权限问题都逐渐显露出来。大数据产业的持续发展离不开制度的约束和限定。大数据时代发展的趋势将是政府行业企业等方面强强联手多方合作努力来为数字经济的发展提供动力。大数据行业发展的共识需要使用者和管理者保障数据安全并且对数据的适用范围加以规范化。企业的数据化管理和实践需要对数据规格进行高效流程化的管理。例如需要数据制造者对数据保护战略进行规划，建立相关数据隐私管理部门或者制定一些行业适用的隐私保护规定等方面的措施。大数据的监管体系需要政府行业和企业都具有新的思路，才能够加快数字中国建设。相关参与者和专家学者们需要从消费者的角度出发，将数据的合规使用划分为行业标准中，力争建立一个公平有序的竞争环境，并且对于行业领域内的风向变化，需要审慎包容的态度来进行处理。

3.2 提高相关人员安全保护意识

大数据可能会被很多人所经手，所以需要提高每个人对于大数据信息安全的保护意识。基于云平台的大数据信息安全非常重要，一旦存在非法访问或者黑客病毒攻击，数据信息会极大可能被篡改和丢失，因此需要每个人都具有一定的安全保护意识。具体做法有以下几点：数据管理员需要对大数据软件或者系统进行定期漏洞扫描，如果发现存在异常需要进行排查和解决；建立健全大数据信息安全制度和体系，主要包含平台安全、软件安全、数据信息安全、数据控制安全、数据分析安全、数据共享安全等方面，这几个方面都要考虑透彻；每个数据操作或者控制的用户都需要在自身访问权限角色下进行操作，不能越权或者使用他人权限角色；数据管理员和其他用户要对本人的数据操作进行备份日志，防止因为非主观因素造成的数据损失，并且对数据传输进行加密；对容易篡改和获取数据的病毒或者网络攻击加以防范，定期维护更换防病毒软件系统。

3.3 设置防火墙

防火墙是计算机系统中比较重要的安全保护措施之一，是存在于网络层的一种安全防护设备，主要是由硬件和软件两个部分

作者简介：王　权，男，汉族，1982年生，讲师，硕士，主要从事计算机科学与技术教育教学研究。

所组成。防火墙相当于对外界信息进入系统的一个防护网，能够对外部网络中疑似未授权的访问操作以及非法访问程序进行拦截和提示，进而对计算机系统进行保护。防火墙一般都具备一套独立的网络安全规则，需要对系统进行验证授权等操作才可以网络访问，在计算机中安装防火墙后，外部网络的数据和信息等内容都需要通过防火墙的排查才可以接收到。

一般每个计算机都具备防火墙，但是可以自己选择是否开启，不开启防火墙是具备一定的风险的行为，因此基本用户所在计算机都会开启防火墙防止数据信息被泄露或者篡改，因此防火墙能够对大数据信息安全提供一定的保障作用，但是也不是完全安全。防火墙技术通俗来说就是给计算机系统安全控制设置了一定宽度的边界，能够对计算机进入和流出的数据信息进行控制和筛选，对访问计算机或者系统的操作进行检测。当防火墙安装完成之后，将会把网络分成不同的区域，在内外交互访问的每个关卡上都设置了加密信息，能够对网络进行监督和控制，对数据信息的流入转出进行记录转化成日志。防火墙可以控制所有本网络的数据信息，也能够对没授权的访问数据进行隔离，除非机主和管理员进行放行才可以访问计算机系统，因此能够很大程度上防止病毒入侵或者数据的篡改，如果受到攻击，防火墙可以进行告警并且处理网络层面的攻击。

3.4 研发入侵检测系统

为了保护基于云平台的大数据的信息安全，对其系统进行入侵检测和检查是非常有必要的，能够从网络、主机或者服务器中搜寻到相关数据并对其进行判断和分析，结合系统的硬件和软件组合对网络系统中的异常行为进行及时的检测，判断是否有违背安全条例的指令存在，一旦发现有入侵行为，就应该对其进行及时的排除和检查，判断信息的安全性，加强对网络系统的安全保障。在对网络信息进行入侵检测的同时可以为云平台和大数据提供一个安全而稳定的运行空间，排除信息被侵入或窃取的风险的存在性，在进行大数据和云计算平台对数据的处理时能够对待不同企业的信息数据进行分开保密处理，从而能够保障信息的安全性和不可侵入性。常见的入侵检测系统的检测原理很多种，有的是根据入侵对象来进行分类，还有的是对入侵方式进行检测，还有的是根据平台进行检测。对于数据异常入侵的检测，需要确定主体是什么，比如包括主体的活动范围或者状况档案等层面，如果入侵活动和其他正常的不一样，比如网络连接异常、流量异常、地址异常等都可以被视为异常活动，但是依照主体行为来进行检测的方式很难确定活动档案和范围都是和正常不一致的，只能把异常活动进行分析和统计。此外还有基于主机的入侵检测方式，每个主机都有自己的审计日志，因此可以对审计日志进行分析，并且对网络连接情况进行监视，如果有异常的主题活动比如异常日志行为，入侵检测系统软件就会即时阻断防止进一步的损失。此种方法需要对网络中的所有数据包和信息流进行监视，因此可以在不同网段中监视数据，并且对可疑数据进行判断分析再决定是否放行。最近还有一类基于分布式系统的入侵检测方法，能够结合前两种的优势，结合分布式架构的特点进行入侵检测和防御，弥补其存在的不足之处。

4 结束语

随着大数据云计算等技术的快速发展，基于云平台的大数据信息安全需要每个人加以重视。大数据的合理利用和隐私保护都是需要相关部门和行业进行监督监管的内容。云平台可以承载的大数据量很多，因此需要对大数据进行安全管理，不论是数据存储还是数据共享，都需要提高安全意识，增加安全系数，制定安全规范，开启防火墙，建立健全安全体系，对网络数据进行入侵检测和安全防护，都是每个人需要考虑的内容。大数据的隐私性和共享性需要针对每个问题来具体分析，不能够让大数据过于曝露，大数据信息安全的保护需要每个人的共同努力。

参考文献

[1] 刘镇源 . 基于云平台的大数据信息安全机制研究 [J]. 通讯世界，2017（22）：43.
[2] 杨鑫 . 基于云平台的大数据信息安全机制研究 [J]. 情报科学，2017，35（01）：110-114.

（上接第 83 页）聚集、包覆，以及在外力作用下，分子的变化过程，同时绘出能量曲线、应力应变曲线，与分子变化过程相对比，让学生更加真实的感受不同温度下，分子的运动规律，使学生对计算材料科学产生浓厚的兴趣。

4 结束语

基于大数据分析的计算材料学教学是一门涵盖多种学科基础知识的综合学科，本文通过第一性原理，分子动力学，使学生从原子，分子的角度全面直观地了解材料的变化，极大地增加学生们学习的积极性与自主性。通过教学研究与材料模拟相结合，既能巩固学生的专业基础知识，又能促进理论与模拟的结合。同时可以根据教学实践的实际情况，可以对基于大数据分析的计算材料模拟进行相应拓展，加深学生对材料本质的理解。

参考文献

[1] 谭艳 . 大数据分析研究现状、问题与对策 [J]. 信息与电脑（理论版），2017（19）：143-144.
[2] 顾君忠 . 大数据与大数据分析 [J]. 软件产业与工程，2013（4）：17-21.
[3] 陈世敏 . 大数据分析与高速数据更新 [J]. 计算机研究与发展，2015，52（2）：333-342.
[4] 何文韬，邵诚 . 工业大数据分析技术的发展及其面临的挑战 [J]. 信息与控制，2018，v.47（04）：18-30.
[5] 韩伟红，贾焰，周斌 . 大数据分析关键技术与挑战 [J]. 信息技术与网络安全，2018，37（4）：11-14.
[6] 林海，郑家新，林原，等 . 材料基因组技术在新能源材料领域应用进展 [J]. 储能科学与技术，2017（5）.
[7] 赵梦璧 . 基于并行化智能优化算法的材料大数据处理研究 [D]. 哈尔滨：哈尔滨工程大学，2016.
[8] 刘阳 . 并行自适应遗传算法在材料学大数据处理中的应用研究 [D]. 哈尔滨：哈尔滨工程大学，2015.
[9] 熊志华，孙振辉，雷敏生 . 基于密度泛函理论的第一性原理赝势法 [J]. 江西科学，2005，23（1）：1-4.
[10] 李红海，李英德，王传奎 . 分子和金表面相互作用的第一性原理研究 [J]. 物理学报，2002，51（6）：1239-1243.
[11] 章永凡，林伟，王文峰，等 .3d 过渡金属碳化物相稳定性和化学键的第一性原理研究 [J]. 化学学报，2004，62（11）：1041-1048.
[12] 文玉华，朱如曾，周富信，等 . 分子动力学模拟的主要技术 [J]. 力学进展，2003，33（1）：65-73.
[13] Moelans N，Blanpain B，Wollants P. An introduction to phase-field modeling of microstructure evolution[J]. Calphad，2008，32（2）：0-294.
[14] Koslowski M，Cuitiño A M，Ortiz M . A phase-field theory of dislocation dynamics，strain hardening and hysteresis in ductile single crystals[J]. Journal of the Mechanics and Physics of Solids，2002，50（12）：2597-2635.
[15] Chen L Q. Phase-field models for microstructure evolution[J]. Annual Review of Materials Research，2002，32（1）：113-140.