DOI:10.13718/j.cnki.xsxb.2020.03.019

适用于自适应网络防御的联合云计算框架①

邹劲松[1], 唐 旭[2]

1. 重庆水利电力职业技术学院 普天大数据产业学院, 重庆 402160; 2. 重庆大学 科技处, 重庆 400044

摘要: 为了解决云计算中网络安全防御策略部署问题, 提出一种适用于自适应网络防御的联合云计算框架. 该框架由治理层和互操作层组成, 使用 LocalHub,StateHub 和 FederalHub 共 3 个集线器将独立的管理层连接起来, 能够根据云计算中不同事件来计算和部署网络防御策略, 满足部署网络防御解决方案和分布式计算所需的标准和复杂服务. 文中给出联合云计算系统模型及其构建单元, 以及所提模型的好处和实施带来的一些挑战. 该云计算联合框架解决了终端用户存在的问题. 实验表明: 当事件响应中涉及更高级别的联合框架时, 对应的延迟变高, 事件响应成功的概率增大. 在本文联合云计算框架中网络防御的性能优于其他 2 种云计算框架.

关 键 词: 云计算; 自适应网络安全; 联合云计算框架; 大数据分析

中图分类号: TP393 **文献标志码**: A **文章编号**: 1000-5471(2020)03-0121-06

云计算是未来分布式计算的新兴技术[1-4], 这是因为云计算具有大量强大的资源, 可以近乎实时地进行大数据处理, 并且对安全架构产生很大影响. 云计算已经得到很多应用, 如物联网[5]和政务大数据[6]等, 政府、学术界和工业界一直致力于开发云计算的不同架构[7-8].

文献[9]中提出了一种改进 Energy Hub 模型的移动云计算框架, 支持公用事业公司和智能能源集线器之间的实时双向通信, 并允许两端的智能基础设施来管理功耗, 使用博弈论来模拟智能能源中心之间的需求侧管理. 文献[10]中提出了云计算采用框架(Cloud Computing Adoption Framework, CCAF), 该框架经过定制以保护云数据. CCAF 多层安全框架可以实时保护数据, 它具有三层安全性: ①防火墙和访问控制; ②身份管理和入侵防御; ③融合加密. 文献[11]中提出一种云计算数据存储框架, 该框架能够有效存储大量物联网数据, 集成结构化和非结构化数据, 有效地处理大量非结构化文件. 该数据存储框架能够组合、扩展多个数据库和 Hadoop, 以存储和管理由传感器和 RFID(射频识别)读取器收集的各种类型的数据. 文献[12]提出一种基于安全云计算的智能电网大数据信息管理框架, 其主要思想是构建云计算中心的层次结构, 为信息管理和大数据分析提供不同类型的计算服务.

然而, 现有云计算框架对于基于上下文和分布式计算的自适应网络防御解决方案却是欠缺的. 针对以上问题, 本文提出一个联合云计算框架, 该框架结合联合和分布式计算成为一个混合模型, 用于根据云计算中不同事件来计算和部署策略. 如果将相关的高性能云基础设施汇集在一起, 这将使云服务更具可用性和灵活性, 从而增加吸引力且降低成本, 以满足部署网络防御解决方案和分布式计算所需的标准和复杂服务. 联合云计算架构基于统一的分层框架, 然后通过互连性、互操作性、可扩展性和信息交付应用于延迟, 服务质量和其他要求.

1 云计算模型

典型的云计算模型在架构的不同层运行, 由 3 个不同的层组成, 包括基础设施层, 平台层和软件应用

① 收稿日期: 2018-07-18

基金项目: 重庆市高等教育学会 2017—2018 年度高等教育科学研究重点课题(CQGJ17046A); 重庆市高等职业技术教育研究会重点课题(GY171002).

作者简介: 邹劲松(1975—), 男, 硕士, 副教授, 主要从事大数据挖掘与分析研究.

层，如图1所示.

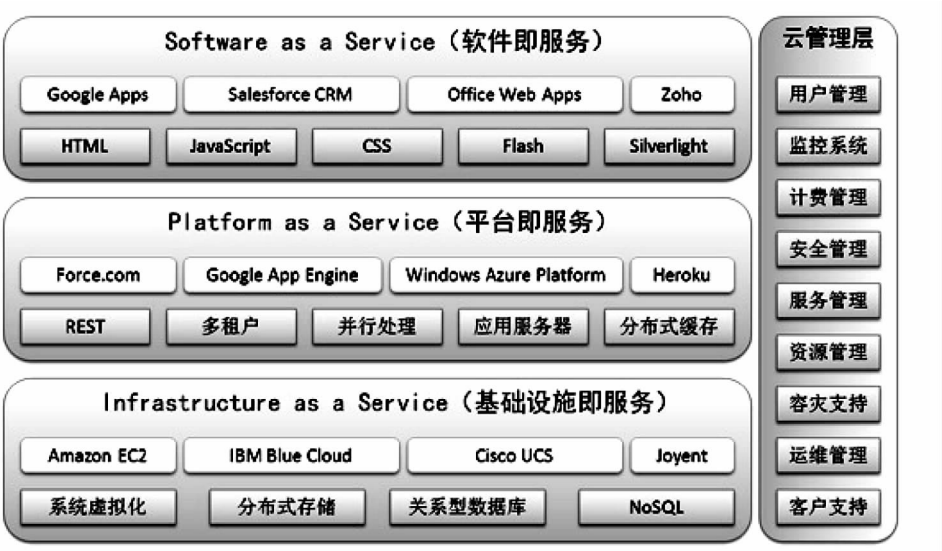

图1 云架构模型

基础设施层也称为虚拟化层，是云计算的核心或基础. 在该层中，存储和计算资源被合并，使得用户或企业按需部署服务需要，该层需要很好地理解负载平衡和所有其他虚拟化管理原则.

平台层位于虚拟化/基础架构层之上，由操作系统和平台应用程序组成，给云计算框架中部署存储、数据库和业务应用程序提供合适的平台.

层级顶部的应用层包括云应用程序，灵活地按需缩放和使用运营成本.

在基础设施层下还有一个硬件层，硬件层包括数据中心的硬件基础设施，计算机系统和相关组件，包括电源、冷却系统和安全系统，所有这些都协同工作，使数据中心能够可靠地运行并能够支持云计算环境.

美国国家标准与技术研究院(National Institute of Standards and Technology，NIST)定义了细分和区分云计算服务模型存在的几种服务. 部署与架构层相关的方式，例如基础架构层的按需存储空间，平台层适用于需要平台进行测试和部署的专有软件，还有用户与在线业务接口的应用层各种应用.

基础架构即服务(Infrastructure as a Service ，IaaS)：是提供所有其他服务所必要的基础平台服务. 按需基础架构资源提供云计算环境中从控制到管理环境资源、网络、虚拟机、处理和数据库服务所需的基本资源，这些资源将允许消费者控制存储分配、系统平台和软件消费者希望部署的应用程序. 平台即服务(Platform as a Service，PaaS)：是为消费者提供开发或获取部署软件应用程序的平台模型. 提供商提供具有所有资源功能的环境，允许消费者测试、运行、管理和控制应用程序的开发或获取. 软件即服务(Software as a Service，SaaS)：是最终用户云计算需求按需提供的地方. 提供商确保应用程序正在运行并且可供最终用户计算设备访问，消费者可能具有用户特定的对应用程序配置的控制，但是无法控制底层云计算基础架构.

云部署模型决定了云托管的类型，以及组织根据自身对云计算环境的要求而做出模型选择，这些模型可以为其独特的业务使命提供强有力的支持，从而最大程度地满足其需求、访问权限和规模，并获得高回报投资和降低间接费用. 因此，组织要选择满足其所有业务目的的正确模型.

私有云：对于拥有可靠资源来专门管理云基础架构的组织，此模型是正确的选择. 私有云是一个需要高数据输入和输出组织的正确部署模型，并且网络延迟很低. 公共云：云基础设施是供公众开放使用的，可以由商业、学术或政府组织或者它们的某种组合拥有、管理和运营. 这种云基础设施向公众提供服务免费，或者某些提供商通过许可协议收费或订阅，此模型下的常见服务是SaaS. 社区云：云基础架构是供具有共同关注点组织的特定消费者社区专用的，但是社区资源控制和管理只能通过治理和合规领域具有专业纪律的成员来加强，该部署将为政府机构、研究机构和金融部门提供服务. 混合云：云基础架构由两个或多个不同的云基础架构(私有、社区或公共)组成，这些基础架构仍然是独特的实体，但通过标准化或专有

技术绑定在一起，从而实现数据和应用程序的可移植性，混合云的一个主要问题是由于对公共云的控制有限，管理稍显复杂.

2　联合云计算框架

在联合云计算中，最终用户将拥有通过 API(应用程序接口)访问云的机制，这些资源来自于各种基础架构组件的合并，后端详细信息对服务的用户或使用者是不可见的. 云联合可以分为两部分：云服务(提供组合的底层基础架构平台，允许来自多个提供商的云计算服务)和配置云服务. 因此，联合云是一种云间部署模型，通过聚集其资源能力形成一个统一的单元来连接云基础设施提供商，包括公共云、私有云和混合云，创建一个平台允许提供云服务，以便联盟内的多个提供商进行操作. 联合的概念保持不变，仅仅因为其是一个云环境，由一组云组成，可以与联盟内的其他云互操作，但独立于内部控制和管理. 联合云计算框架的一个优点是在云计算上有竞争优势，这为中小企业开辟了云服务提供商的竞争市场.

2.1　联合云架构

本文提出的安全敏捷和自适应联合云架构由治理层和互操作层组成，如图 2 所示. 由 3 个主要的 Hub(分别是 LocalHub，StateHub 和 Federal-Hub)将独立的云管理层连接起来. 虽然子系统中的每个云都是自治的，并且有自己独立的权力来决定内部控制和管理，但是父层构成了云治理的一部分，包括集中、分布式和共享的职责，以确保真正联合的平滑互操作性. 此外，每个层都为整个云联盟提供云服务和安全网络的结构.

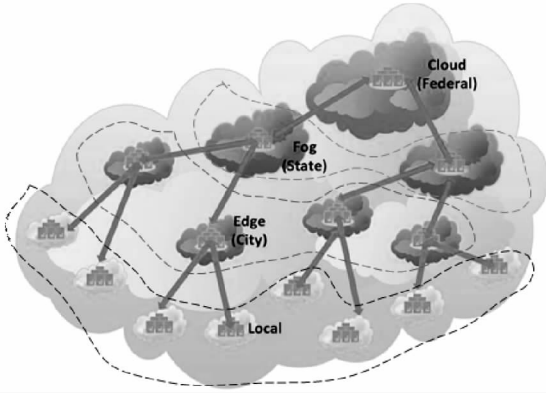

图 2　网络防御与边缘计算联合云计算体系结构

FederalHub(云级别)提供集中的领导和治理，联盟内的每个云都受益于集线器的参与并提供主动安全和健康的环境. 该中心制定并实施必要的策略，以促进和支持联合的核心价值.

StateHub(雾级)通过帮助确保从顶部的联合视觉通过 localhub 传播到联合中的云，在联合中的云协作中起主要作用. 该中心具有合作伙伴关系的优势，可以克服可能与之相关的云管辖权差异地理位置，负责对其领域下的云进行高级别的战略审查、监控和绩效评估.

LocalHub(边缘级别)最接近用户或者设备，并为其提供服务. 对于保持每个云的独特性，以及提升在其领域内工作的服务质量能力至关重要，这些服务包括最佳服务于前端用户的规划、分发和资源分配，其他服务包括保护和时间计算以及设施支持.

2.2　联合云框架的自适应连接模型

针对网络防御和分布式计算的自适应联合云的假设模型基于几个因素，这些因素决定了联合云内的最佳可用性，并且可以为任何用户/消费者请求服务提供最佳服务质量. 需要 3 个重要的程序步骤：

(1) 设备与边缘/云的接近度

该模型允许基于边缘的地理分布及其与设备的位置接近度来分配资源. 第一步是通过识别最接近设备接近度的云来简化资源分配过程，然后应用某些指标来确定它们为设备 / 用户提供服务的可用性. 为了生成设备到云中心的距离列表 DC_{dist}，通过使用全球定位系统估计设备位置(x_1，y_1)和云中心位置(x_2，y_2)来计算欧几里德距离，因此假设设备 D_{evice} 想要使用云中心 C_{cloud}，设备和云边缘之间的欧几里德距离是

$$d_1 = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{1}$$

对于 N 个云中心，用户 / 设备的距离 DC_{dist} 由式(1) 生成为$\{d_1, d_2, \cdots, d_N\}$，设备可以根据计算的距离选择最接近的设备.

(2) 云中心可用性状态

基于强大的竞争优势，可快速评估 N 个云中心的每个中心，以确定其可用状态 $C_{availstate}$. 有助于减少列表的两个关键变量是云中心审计状态 C_{audit} 和存储资源容量 $C_{storage}$，两者都返回 TRUE 状态，这意味着

$$C_{availstate} = \{C_{audit} = \text{“TRUE”} \ \& \ C_{storage} = \text{“TRUE”}\} \tag{2}$$

$C_{availstate}$ 可以使用马尔可夫模型确定，马尔可夫模型用于决定 C_{audit} 和 $C_{storage}$ 的结果. C_{audit} 是联合框架内每个云中心的风险状态，可以从高风险转变为低风险，反之亦然. C_{audit} 由一系列值(低 < 设定值 < 高) 确定. 所考虑的风险影响矩阵是云中心受到攻击、威胁级别、攻击次数和攻击历史组成的. 审计状态是由层中心(federalHub，stateHub 和 localHub) 监视的连续后台持续进程，目标是通过潜在地减少或完全消除风险来平衡风险. 因此

$$C_{audit} = \{\text{高风险} = \text{“FALSE”}, \text{低风险} = \text{“TRUE”}\} \tag{3}$$

$C_{storage}$ 是可量化的，如果没有可用的存储资源 / 容量来满足所需的工作容量 R_{job}，一个云中心 C_{cloud} 显然将无法为设备 / 用户提供服务. 所以，假设一个 C_{cloud} 有几个服务器 S_n，$n \geqslant 1$，每个服务器可能有多个虚拟机 VM_n，这意味着服务器上的总容量是 $S_n = VM_1 + VM_2 + \cdots + VM_n$，服务器上使用的存储容量 $U_n = U_{VM_1} + U_{VM_2} + \cdots + U_{VM_n}$，其中 U_{VM} 用于每个虚拟机上的存储容量，则服务器上的可用存储容量是 $A_n = S_n - U_n$，因此 $C_{storage} = !(R_{job} \geqslant A_n)$.

(3) 基于服务质量的云中心选择

这是模型的过滤部分，其中每个云中心分析将产生优质服务的性能，并且更新向上传递到 localhub. 由于目标是通过确保设备连接到具有可以有效响应服务需求的最佳资源能力的云中心来为设备提供最佳服务质量(Quality of Service，QoS)，因此存在与资源一起检查和计算的性能因素，用在每个已清除的云中心 C_{cloud} 上可用的服务器 C_iS_i 的资源得分(resource score，RS) 来检查和计算. 性能因素为 S_{CPU}，S_{mem}，S_{kb}(kb = 千字节)，S_{pr}(pr = Packet Rate)，S_{vsc}(vsc = VS 容量)，S_{acts}(acts = active session)，S_{dlay}(dlay = 延迟)，S_{vss}(vss = 虚拟服务器得分 virtual Server Score)，S_{dist}(dist = DC_{dist})，S_{cap}(cap = $C_{storage}$ 中的 A_n). 将这些因子中的每一个乘以一个权重系数以计算得分(例如，S_{CPU} = 性能因子 × 权重系数). 权重是基于优先级的，是定性确定的一些因素. C_iS_i 的最终选择将以最高的分数为基础.

使用联合云框架时，延迟 t_d 可写为

$$t_d = t_{det} + t_{act} + 2\ t_{edge} + 2\ t_{fog} + 2\ t_{fed} + t_{edge-act} + t_{fog-act} + t_{fed-act} \tag{4}$$

其中 t_{det} 是检测攻击的时间，t_{act} 是设备本地操作的时间，t_{edge} 是设备到边缘之间的传播延迟，t_{fog} 是设备和雾之间的传播延迟，t_{fed} 是传播时间，$t_{edge\text{-}act}$ 是边缘对事件采取行动所花费的时间，$t_{fog\text{-}act}$ 是雾对事件采取行动的时间，$t_{fed\text{-}act}$ 是联邦级别云计算事件所需的时间. 当设备本地检测到并且对事件响应起作用时，$t_d = t_{det} + t_{act}$，式(4) 中其他项将为零.

2.3 联合云框架的好处和挑战

使用联合云框架而不使用单个自治独立的实体有几个好处，其一，该模型提供了一个更强大、可识别且可销售的服务品牌，具有规模经济和更强大的计算能力；其二，它提供了丰富的管理经验以解决故障和防止攻击，从而确保在整个企业范围内满足消费者需求的可扩展集成服务. 集成联合云计算框架的其他好处包括：节省成本和提高效率、服务提升和改善治理.

节省成本和提高效率：因为共享云基础架构、攻击历史、知识、网络和计算资源，能够节省云设施和运营的整体运行成本. 在联合云系统中，根据共享资源，一旦出现漏洞，网络防御机制之间的信息共享就可以防止联盟内部的攻击扩散. 消费者不会注意到受影响中心可能遇到的停机时间，性能水平也不会下降.

服务提升：联盟提供了以分层方式共享历史和攻击知识的灵活性，从而以更高的效率为更多设备提供服务. 对于用户而言，可以通过联合平台上更广泛的云网络享受更多服务和更高质量的服务，这些网络是可用的、可访问的和安全的.

改善治理：较低的中心(localhub 和 statehub)在确保存在问责制方面发挥重要作用，即使每个云都负责其内部控制和管理，必须保护核心原则以实现共同的目标.

另外集成联合云计算框架也带来一些挑战，体现在防御安全策略和治理和控制方面.

防御安全策略：使用分布式策略，以便在遍布整个联盟之前检测并准备好防止攻击. 需要集中和分布机制来准确有效地检测任何可能的利用并在失控之前对其进行管理.

治理和控制：信任和承诺对联合云框架非常重要，需要确保适当的控制措施，以确保跨联盟(包括云租

户)之间的数据隐私和安全性.

3　框架评估结果

为了对本文框架的可行性进行验证，在 60 台电脑组成计算云环境进行实验，每台计算机 CPU 为 2.1 GHz，运行内存为 8 G，内存为 500 G，网络环境为 200 Mb/s. 图 3 和图 4 中给出了对联合云框架的性能分析. 首先评估了当联合框架部署的攻击检测和网络防御解决方案保护设备时，不同级别的联合云框架引入的延迟，如图 3 所示.

由图 3 可知，当设备检测到网络攻击并实施对策时延迟最小，并且在最高云级别操作(Federal Level)时延迟最高. 当类似的攻击重复发生时，响应时间会减少. 类似地，当云单元的更高级别涉及到网络攻击的检测时，与设备级响应相比，设备和系统具有更好的对策和事件响应，具有更高的概率(较低的不确定性)，如图 4 所示.

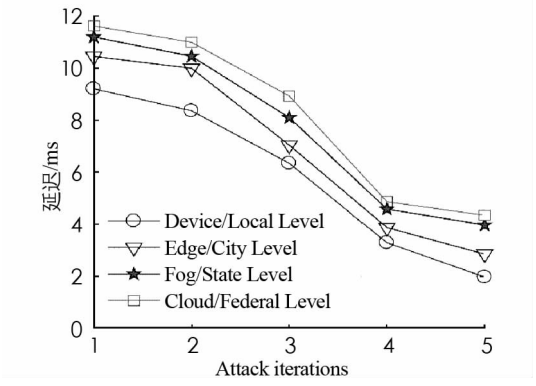

图 3　针对不同的攻击迭代时联合云框架的延迟

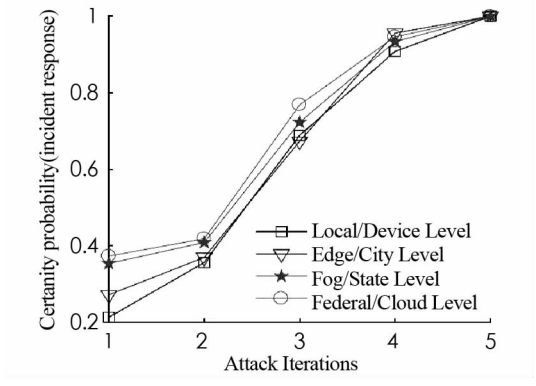

图 4　针对不同攻击迭代的联合云框架中事件响应的确定性

为了本文框架的有效性，将本文联合云计算框架与文献[10]中单层云计算框架 SLF 及多层云计算框架 CCAF 进行比较. 比较本文联合框架、CCAF 多层框架和 SLF 单层框架中进行网络防御杀死的病毒或木马数量，如图 5 所示.

从图 5 中可以看出，网络防御在本文框架中能发挥更好的性能，能够杀死更多的病毒或木马，性能比 CCAF 提高了 37.7%，说明本文框架对于网络防御的适用性能优于其他两种云计算框架. 实验结果表明，本文联合云计算框架能够为数据中心提供更好的网络防御服务，说明了本文框架的有效性和优越性.

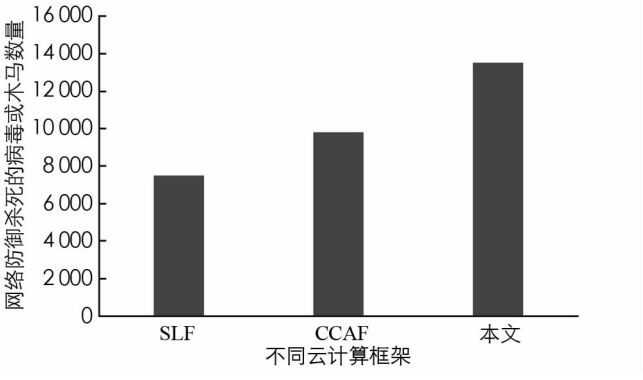

图 5　不同云计算框架下网络防御性能比较

4　结　　论

本文提出一种用于自适应网络防御和分布式计算的联合云计算框架，该框架的解决为终端设备或用户带来了显著的好处，有助于提高事件响应的确定性. 当用户或者设备使用云计算时，该架构为其运行参数提供了很大优势，参数包括：不同级别的计算能力、最终设备位置、服务质量和边缘的安全级别等. 实验结果表明，当事件响应中涉及更高级别的联合框架时，可能会有稍微更高的延迟，但事件响应成功的概率会增加. 另外，将本文框架与其他框架进行比较，本文联合云计算框架比其他两种框架更适用于网络防御，说明本文框架的有效性. 未来的工作将集中在所提联合框架的安全方面.

参考文献:

[1] HASHEM I A T, YAQOOB I, ANUAR N B, et al. The Rise of "Big Data" on Cloud Computing: Review and Open Research Issues [J]. Information Systems, 2015, 47: 98-115.

[2] KRISHNAN Y N, BHAGWAT C N, UTPAT A P. Fog Computing-Network Based Cloud Computing [C]//2015 2nd International Conference on Electronics and Communication Systems (ICECS). Coimbatore: IEEE, 2015.

[3] 薛 涛, 刘 龙. 云计算中虚拟机资源自动配置技术的研究 [J]. 计算机应用研究, 2016, 33(3): 759-764.

[4] ALI M, KHAN S U, VASILAKOS A V. Security in Cloud Computing: Opportunities and Challenges [J]. Information Sciences, 2015, 305: 357-383.

[5] 陈 亮, 仇 晶, 朱有产, 等. 面向家庭物联网的云计算架构 [J]. 计算机应用研究, 2013, 30(12): 3686-3689.

[6] 李吉凯. 基于税务大数据的云计算融合处理平台架构设计 [J]. 工业控制计算机, 2016, 29(8): 36-37.

[7] YAN Q, YU F R, GONG Q X, et al. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: a Survey, some Research Issues, and Challenges [J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 602-622.

[8] 张 晓, 秦志光, 罗亚东, 等. 一种低代价的云计算存储权限管理机制 [J]. 西南师范大学学报(自然科学版), 2015, 40(7): 33-40.

[9] SHEIKHI A, RAYATI M, BAHRAMI S, et al. A Cloud Computing Framework on Demand Side Management Game in Smart Energy Hubs [J]. International Journal of Electrical Power & Energy Systems, 2015, 64: 1007-1016.

[10] CHANG V, RAMACHANDRAN M. Towards Achieving Data Security with the Cloud Computing Adoption Framework [J]. IEEE Transactions on Services Computing, 2016, 9(1): 138-151.

[11] JIANG L H, XU L D, CAI H M, et al. An IoT-Oriented Data Storage Framework in Cloud Computing Platform [J]. IEEE Transactions on Industrial Informatics, 2014, 10(2): 1443-1451.

[12] BAEK J, VU Q H, LIU J K, et al. A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid [J]. IEEE Transactions on Cloud Computing, 2015, 3(2): 233-244.

A Federated Cloud Computing Framework for Adaptive Network Defense

ZOU Jin-song[1], TANG Xu[2]

1. *Putian Big Data Industrial, Chongqing College of Water Resources and Electric Engineering College, Chongqing 402160, China;*
2. *Scientific And Technical Department, Chongqing University, Chongqing 400044, China*

Abstract: In order to solve the problem of network security defense strategy deployment in cloud computing, an integrated cloud computing framework for adaptive network defense has been proposed. The framework consists of the governance layer and the interoperability layer, using the LocalHub, StateHub, and FederalHub three hubs to connect the independent management layer to compute and to deploy network defense strategies based on different events in cloud computing, which meet the needs and complex services needed for deploying network defense solutions and distributed computing. In this paper, the integrated cloud computing system model and its building blocks have been presented, as well as the benefits and implementation challenges of the proposed model. With the cloud computing integrated framework, the problems of end users have been solved. Experiments show that when a higher-level joint framework is involved in the event response, the corresponding delay becomes higher and the probability of successful event response increases. Besides, in the federated cloud computing framework, the performance of network defense is better than that of the other two cloud computing frameworks.

Key words: cloud computing; Adaptive Network Security; Integrated Cloud Computing Framework; Big Data Analysis

责任编辑 夏 娟