云计算环境下用户安全研究

杨永强◎著

中国政法大学出版社

云计算

YUNJISUAN

环境下用户安全研究

HUANJINGXIA
YONGHUANQUAN
YANJIU

杨永强◎著

中国政法大学出版社

云计算环境下用户安全研究

杨永强　著

中国政法大学出版社
2018·北京

图书在版编目（CIP）数据

云计算环境下用户安全研究/杨永强著. —北京:中国政法大学出版社,2018.4

ISBN 978-7-5620-8221-7

Ⅰ.①云… Ⅱ.①杨… Ⅲ.①互联网络－安全技术－研究 Ⅳ.①TP393.408

中国版本图书馆CIP数据核字(2018)第079411号

出 版 者　中国政法大学出版社

地　　址　北京市海淀区西土城路25号

邮寄地址　北京100088信箱8034分箱　邮编100088

网　　址　http://www.cuplpress.com（网络实名：中国政法大学出版社）

电　　话　010-58908586(编辑部) 58908334(邮购部)

编辑邮箱　zhengfadch@126.com

承　　印　固安华明印业有限公司

开　　本　880mm×1230mm　1/32

印　　张　6.75

字　　数　205千字

版　　次　2018年4月第1版

印　　次　2018年4月第1次印刷

定　　价　39.00元

前言 PREFACE

随着大数据（Big Data）、云计算（Cloud Computing）、移动互联网、物联网技术的快速发展，云计算服务模式也出现了适应大数据、移动环境的新发展。然而，大规模数据、大规模用户和资源动态灵活管理等支撑技术在带来效率提升、服务便捷和成本降低的同时，也带来了一系列由于云平台的资源共享和逻辑边界不确定而导致的身份安全问题、数据安全问题。在大数据和混合云环境下，若干部署于不同机构的物理网络被统一虚拟网络所取代。这种计算资源共享模式实现了网络资源的高度整合与利用、网络流量的集中分发，但也带来了用户隐私泄露、密钥信息泄露、数据访问控制等安全问题。因此，如何克服虚拟网络不确定边界所带来的安全威胁挑战，进而确保云计算服务系统内的用户安全、数据安全成了当前信息安全领域亟待解决的重要问题。

密码技术的加密、签名、认证等技术为云平台中的用户安全、数据安全提供了新的思路。加密实现了数据的机密性，签名抵抗了身份伪装，认证确保了数据的授权访问；身份基密码消除了数字证书，属性基密码实现了数据的细粒度访问控制。但是，单一技术很难形成一个立体防护体系，难以同时保证身

份安全、数据安全和密钥安全。此外，云服务提供商（Cloud Service Provider，CSP）的用户身份保护与权限控制通过属性更新、密钥更新和访问控制树更新实现了密文数据的细粒度访问。在此基础上进一步研究用户权限升级与降级、密钥撤销以及身份属性保护，通过实现适合不同应用场景的动态管理用户的授权、隐私、密钥为云平台数据安全提供保障。

本书以确保用户安全为核心目标，针对云计算环境下身份管理与权限控制的通用性与可控性、密文访问与隐私保护的机密性与完整性问题，结合群和环的签名签密应用，分别研究单CSP和多CSP环境下的用户权限管理和隐私属性保护。

1. 研究单CSP环境下的用户权限升级与权限降级

单CSP环境下用户权限更新包括访问权限完全升级与部分升级、访问权限完全降级与部分降级，主要通过身份集更新、属性集更新、密钥更新实现。针对权限更新引发其它用户不能正常访问以及属性更新、密钥更新需要解决的身份安全、数据安全问题，本书提出了一种属性基群签名权限升级方案和广播CP-ABE（Ciphertext-Policy Attribute-Based Encryption，CP-ABE）权限降级方案。在权限升级方面，该方案利用群属性集的可重构特性，在用户申请签名密钥时，系统验证身份属性真实性以达到控制密钥分配；利用CP-ABE和撤销群的权限可控特性，系统验证用户签名以达到保护密文不被泄露。同时，在权限降级方面，该方案利用门限CP-ABE的属性分割特性，在用户申请撤销子用户权限时系统控制子用户私钥份额的分配以达到撤销子用户密文访问权限；利用广播的身份集管理优势，数据属主直接撤销一个部门用户的完全权限。该方案实现了用户权限升级与权限降级、规模撤销与立即撤销的双系统。

2. 研究单 CSP 环境下的用户部分属性保护

单 CSP 环境下用户部分属性隐私保护包括防范属性集更新泄露与密钥关联属性泄露，主要通过代理认证、零知识证明、可信第三方和匿名签名实现。针对部分身份属性保护严重依赖第三方的密钥分配与属性更新授权，本书提出了一种密文策略属性基群签密部分属性保护方案。该方案利用群签密的无连接交互验证特性，在用户计算密钥因子时系统控制 CSP 获得密钥关联属性信息；利用无证书签密和密文策略签密的签名密钥与加密密钥相互独立特性，系统降低了用户签密所需要的最小身份属性集数量；利用身份基签密的不可伪造特性，系统抵制攻击者利用属性集更新伪造签名；本书系统以密钥服务为中心设计了群签密的身份属性验证机制以达到控制其它用户身份属性伪装。该方案实现了保护用户随机部分属性安全和消息隐私。

3. 研究多 CSP 环境下的用户密钥撤销

多 CSP 环境下用户密钥更新包括访密钥属性撤销、群密钥更新、证书属性撤销，主要通过设置证书和属性集生命周期、访问控制策略树更新实现。针对密钥共享属性撤销引发的属性泄露以及密钥重新生成引发的系统性能下降问题，本书提出了一种属性基环签名用户密钥撤销方案。该方案利用单调张成矩阵的映射特性，以用户属性集映射为矩阵行变量，系统控制 CSP 获得用户密钥关联属性；利用分布式属性基加密的多授权者独立特性，系统可以确保私钥属性安全；采用撤销环的非交互匿名撤销特性，系统控制 PKG（Private Key Generator，PKG）更新系统参数以达到共享属性撤销不影响其它用户访问；本书系统以密文访问为中心设计了环签名的身份属性验证机制以达到阻止用户共谋。该方案实现了密钥属性撤销、属性保护和密文验证访问。

4. 研究多 CSP 环境下的身份属性保护

多 CSP 环境下用户身份属性保护包括防范密钥关联属性泄露和属性集更新泄露，主要通过多方计算、属性分割与属性组合、源证书与认证证书实现。针对证书更新引发的关联属性泄露和密钥生成维护量增大、系统性能下降问题，本书提出了一种属性基盲环签密身份属性保护方案。该方案利用无证书签名的密钥分割特性，设计去中心化的用户密钥本地化生成以阻止 PKG 获得密钥关联整体身份属性；利用属性基环签密的签密验证特性，系统阻止 CSP 共谋获得签名关联的整体身份属性和用户身份属性伪装；采用盲签名的不可伪造特性，系统抵制伪造属性集、密文和保护消息隐私；本书系统以用户访问权限为中心设计盲环签密验证机制，保护身份属性的机密性和完整性。该方案实现了用户身份属性保护、消息隐私保护和密钥关联信息保护。

本书是笔者在云安全研究方面阶段成果的总结，并不是研究工作的结束，笔者将会继续深入研究大数据安全的理论、技术和应用。由于笔者学术水平有限，书中难免会有不妥和错误之处。对此，笔者恳请同行专家批评指正，并于此先致感谢之意。

目 录
CONTENTS

第一章 绪 论

CHAPTER I

第一节 研究背景和意义

云计算和大数据的广泛普及得到了越来越多的关注，成了国内外学术界、产业界倍受瞩目的热点研究领域。大家开始重视大数据的价值，探索大数据驱动的业务模式，在国内外掀起了一个空前的研究热潮。大数据通常用来形容一个公司创造的大量非结构化数据和半结构化数据，对这些数据进行分析时会耗费过多计算时间，实时性大数据处理需要 Hadoop/MapReduce 框架、实时流分析、分布式内存计算以及图计算框架等；大数据分析、存储与管理和云计算密切相关，云计算是大数据的基础平台与支撑技术，大数据是云计算的一个杀手级应用。本质上，云计算与大数据的关系是动与静的关系，云计算强调的是计算，是动的概念；大数据则是计算的对象，是静的概念。前者强调的是计算能力、存储能力，后者则需要处理大数据的强大计算能力。云计算资源分布广泛，是确保异构系统准确处理数据的有效方式。云计算为大数据提供了弹性扩展、相对便宜的存储空间和计算资源，中小企业可以通过云计算完成大数据查询、分析、处理和集成。随着物联网、社交网络的数据种类和规模以前所未有的速度增长，数据成了一种基础性资源，云

计算服务模式得到了空前发展，其根本特征是“资源虚拟化、高可扩展性、按需租赁服务、泛在接入”，可以确保大数据高速迁移至云服务中心。

云计算利用云端的资源，如大型硬件平台、数据中心、应用服务中心等，向互联网用户提供资源租用、应用托管、服务外包等服务。此时，用户无需购买大量的硬件设备，也无需安装和配置软件环境以及对系统进行维护，从而改变了传统个人和企业对信息资源的处理、存储和交换的模式。目前，云计算提供三种基础服务，软件即服务（SaaS）、平台即服务（PaaS）以及基础设施即服务（IaaS）。企业用户和个人用户通过网络对这些服务进行使用，例如用户数据（博客、相册、网盘、邮件、文档等）的存储以及企业信息系统逐渐从终端向云端进行转移等，使得云端存储的用户数据和信息系统规模越来越大。用户数据和信息系统被集中存放在云端后，给用户使用和体验互联网业务带来极大的便利，同时也把安全问题从终端迁移到了云端。云计算的多租户模式会导致信息泄漏；恶意用户可以租用云服务，对云服务软件、架构、安全机制进行分析研究以及漏洞挖掘，为破袭云服务器提供强有力的支持；其平台上的用户资源会吸引各种恶意代码攻击和漏洞攻击，而且云计算平台本身也存在缺陷和漏洞。目前，云计算环境的安全加固和安全监控尚不足以抵御这些未知攻击。为此，提高云计算环境的安全性和可靠性成了目前研究的热点。

云计算平台在极大方便终端用户和企业使用计算资源和存储资源的同时，也在安全方面提出了更大的挑战。云服务意味着用户任务和用户数据被转移到了用户掌控范围外的云端，也就是云服务提供商（CSP）的手里。只要存在数据泄漏或者破坏的可能性，云计算服务就会被高安全等级的客户拒之门外。

从本质上讲，云计算的一个问题是确保用户的安全，另一个问题是确保 CSP 本身的可信和安全。如果云服务提供商无法抵挡恶意用户的 DDoS 攻击、基于漏洞的攻击以及各种恶意代码的攻击，则确保用户的安全将无从谈起。云服务提供商的管理员可能会偷窥用户数据，利用用户访问数据的日志感知用户的访问模式，而该访问模式是用户的隐私，需要保护。因此，云服务提供商是“半可信”的，需要采用密码学方法增强用户数据的安全性和隐私性。采用密钥规则的基于属性加密方案（KP-ABE）以及采用密文规则的基于属性加密方案（CP-ABE）都可以提供细粒度的访问控制。同时，采用秘密同态加密算法实现密文处理，以期减少密文处理时间，降低其暴露的次数。另外，云服务提供商在同一个硬件资源上同时服务于多个用户，简称多租户模式，该模式会导致信息泄漏。例如，在 IaaS 中，不同用户通过虚拟机共享同一个物理资源，恶意用户可以利用漏洞获取给非授权用户的数据；不同的企业、不同的应用可能共享相同的基础设施或者平台资源。

一、云计算环境的虚拟隔离和安全监控

虚拟化技术可以实现硬件资源的虚拟化和资源共享，为不同用户共享同一个物理资源以及同一用户利用不同物理资源提供基础支持。与传统的操作系统相比，虚拟化技术所需的代码量较小，传统的安全技术可以移植到虚拟机管理器（VMM）中。虚拟化技术能够隔离软件与硬件、应用软件与底层系统之间的直接依赖关系，能提供比操作系统更强的隔离性。同时，Hypervisor（VMM）可以监视、协调和控制客户操作系统和物理资源的访问，并实现数据保护、安全隔离和入侵检测。Elangop 等人提出了基于虚拟机的隔离执行环境。Raj 等人提出了通过缓

存层次可感知的核心分配，以及给缓存划分的页染色的两种资源管理方法实现性能与安全隔离。Wei 等人分析了虚拟机文件对应的每一个客户应用，它们必须具有高度完整性，且需要可以安全共享的机制，其映像文件管理系统实现了映像文件的访问控制、来源追踪等，可以检测和修复安全性违背问题。

云计算平台的完整性包括文件完整性、内核代码完整性和虚拟机管理器代码完整性。将可信计算技术融入云计算环境是一种常用的安全加固方法。Santos 等提出了一种可信云计算平台 TCCP，IaaS 服务商可以向用户提供一个密封的箱式执行环境，保证虚拟机运行的机密性。Sadeghi 等基于可信计算技术（TPM），设计了一种可信软件令牌，将其与一个安全功能验证模块相互绑定，以求在不泄漏任何信息的前提条件下，对外包的敏感（加密）数据执行各项功能操作。Quynh 等人提出基于 Xen 虚拟机来实时监控文件系统的完整性，并将文件操作的记录通过共享内存的方式保存在单独的虚拟机中。但是，文件监控器可能被屏蔽，且对监控系统不透明。RFIM 系统通过在虚拟机管理器层截获虚拟机中的系统调用，实现文件操作的语义恢复和文件的完整性度量。Sec Visor 通过修改 Linux 来创建一个轻量级虚拟机，从而保护主机操作系统的完整性；KOP 则是通过映射动态的内核数据来保证内核完整性。此外，HUKO 是基于虚拟化的完整性保护系统，从而避免对操作系统内核进行不可信的扩展。Hypersafe 采用不可绕过的内存锁和受限制的指针索引保证了虚拟机管理器代码的完整性。Hyper Sentry 和 Hyper Check 通过系统管理模式（System Management Mode，SMM）来保护代码和关键数据。前者引入与虚拟机管理器隔离的软件组件实现度量；后者仅依赖于 BIOS 实现度量。

虚拟机的安全监控是保障虚拟机安全运行的基础，有内部

监控和外部监控两种体系结构。在内部监控中，信息收集组件部署在目标虚拟机中，负责收集和拦截某些事件。当 VMM 捕获到特定的事件时，VMM 会通知安全域中安全组件实施事件的安全审查和入侵检测。内部监控可以直接获取事件的高级语义，会遭受恶意攻击者对信息收集组件的直接攻击。在外部监控中，信息收集组件部署在 VMM 中，拦截目标虚拟机中的事件，重构该事件的高级语义并传递给安全域中的安全组件。外部监控的所有部件独立于目标虚拟机，对攻击者是不可见的，但其捕获的事件缺少操作系统的语义，存在从低级语义重构高级语义的困难。Cloud Visor 将虚拟机监视器资源管理功能与安全保护功能分离，给出了一种基于嵌套虚拟化的解决方案，其安全工具进一步深入虚拟机监视器的下层。即使虚拟机监视器和虚拟机都已被恶意行为入侵，也能够保证用户数据的隐私和虚拟机的一致性。通过修改 VMware Workstation，Livewire 利用 VMM 监控到的信息检测入侵。被监控系统封装在虚拟机中，同时从外部监控其中的系统调用序列，根据调用序列判断进程行为是否异常。

云计算环境承载多种操作系统、中间件和服务软件。用户开启大量的服务实例，这些实例产生软件或者平台的同构性。一旦这些系统或软件存在漏洞缺陷并被利用，则很可能导致大量服务被破坏或者控制。而且，攻击是普遍存在的。例如，VM 逃逸（Escape）攻击可以让攻击者访问宿主 OS 和其他所有的 VM。2009 年 5 月，VMware 虚拟化软件的 Mac 版本存在一个严重的安全漏洞，别有用心的人可以利用该漏洞通过 Windows 虚拟机在 Mac 主机上执行恶意代码。2012 年，仅 Xen Hypervisor 4.1.4 版本就修复了 18 个关键漏洞，其中 Hypervisor 的缺陷会导致攻击者获得对虚拟平台的控制。因此，由漏洞引发的攻击是无法避免的。

二、内存错误攻击

当访问的对象不同于期望的对象时，会发生内存错误，例如对象指针越界、对象未初始化、对象指向非指针数据或不存在对象等。自20世纪70年代以来，内存错误一直是软件的重要漏洞之一，在CERT和CVE漏洞列表中占据前列，如栈溢出、堆溢出、格式化字符串漏洞、NULL指针漏洞、整数溢出、释放后引用漏洞等。内存错误漏洞可能会导致拒绝服务攻击、信息泄漏和控制劫持。软件的控制流劫持使得软件转向攻击者设计的代码（简称外部代码，Shellcode）。其可以劫持系统程序的软件执行，也可以劫持用户程序的软件执行，从而违背期望的执行语义，导致云计算环境被劫持或者信息泄漏。为了检测源于内存错误引发的外部代码，可以检测用户数据是否含有外部代码，禁止外部代码的执行。

检测可疑外部代码的方法之一是检测用户数据，特别是网络输入数据是否存在可执行代码的签名，如NOP-Sled、特权指令或控制流/数据流结构等。Toth对网络流数据进行反汇编，识别Shellcode前面的NOP-Sled。但这种静态分析技术对混淆技术敏感，Polychronakis给出了基于仿真的检测方法对抗混淆技术，可以处理自加密的Shellcode。Zhang从数据流角度识别GetPC代码。Polychronakis利用Shellcode需要解析kernel32.dll地址、扫描SEH地址或System call指令等启发式知识去检测Shellcode。Gu采用进程内存的快照信息提高Shellcode检测的精度，解决Shellcode检测中缺少进程上下文的问题。Shellzer利用PyDbg和API函数仿真动态获取Shellcode的API序列以及外部URL资源，从而可以解决Shellcode分析中的缺少上下文和效率低下的问题。ShellOS采用虚拟化技术（如KVM或Intel VT）分析Buffer数据，

利用 Polychronakis 中的启发性知识检测 Shellcode，该方法可以减少检测时间，同时提高检测的准确性。

Heap Spraying 攻击 Sotirov 是通过分配大量的 Heap 对象达到溢出的目的。该攻击可以绕过地址随机化技术，增加攻击成功的概率。Egele 通过检查 Java Script 的字符串对象检测其中的 Shellcode。Nozzle 反汇编 Heap 对象，从汇编代码的控制流中计算其攻击面特征 SA，并利用此 SA 的值识别该攻击。Ding 利用内存对齐特性，大量减少其攻击代码中的 Nop-Sled，该攻击可以逃避已有的检测，并给出其对抗的解决办法。

不管是一般的 Shellcode，还是 Heap Spraying 攻击的 Shellcode，我们都假设其 Shellcode 含有可执行的特定代码；如果 Shellcode 不含任何代码，则以上检测 Shellcode 的方法都将失效。另外，随着操作系统内存保护机制的增强，常用的代码注入方式将不再有效。对此，人们提出和应用代码复用攻击（ROP/JOP），其攻击数据没有任何可执行指令，只含有各种参数和控制 ESP 的数据。最早的代码复用攻击 Return-to-libc 复用动态库中的函数。随后出现的 ROP 和 JOP 复用动态库或者应用程序的指令序列（该序列简称为 Gadget），扩大了攻击面，使得其检测比较困难。DROP 检测以 RET 指令结束的短指令序列识别 ROP 攻击。Ropdefender 利用隔离的影子栈检测返回地址是否被修改识别 ROP 攻击。Li 通过消除程序中的返回指令减少代码被复用的可能性，但需要编译内核。G-free 通过消除程序中的 Gadget 达到抑制 ROP 攻击的目的。Tyler 采用控制流锁检测 ROP 攻击。ROP 可以逃逸基于代码分析的 Shellcode 检测技术和 DEP 技术，但 ASLR 可以增加 ROP 攻击的难度。

禁止外部代码的执行包括禁止数据页执行，对保护对象实施完整性或签名校验等技术。外部代码注入合法程序的缓冲区，