软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(6):1325−1327 [doi: 10.13328/j.cnki.jos.005010]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

云计算安全研究专刊前言*

薛 锐[1], 任 奎[2], 张玉清[3], 李 晖[4], 刘吉强[5], 赵 波[6], 祝烈煌[7]

[1](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

[2](Department of Computer Science and Engineering, State University of New York at Buffalo, USA)

[3](中国科学院大学 计算机与控制学院,北京 100049)

[4](西安电子大学 网络与信息安全学院,陕西 西安 710071)

[5](北京交通大学 计算机与信息技术学院,北京 100044)

[6](武汉大学 计算机学院,湖北 武汉 430072)

[7](北京理工大学 计算机学院,北京 100081)

通讯作者: 薛锐, E-mail: xuerui@iie.ac.cn

中文引用格式: 薛锐,任奎,张玉清,李晖,刘吉强,赵波,祝烈煌.云计算安全研究专刊前言.软件学报,2016,27(6):1325−1327. http://www.jos.org.cn/1000-9825/5010.htm

云计算作为推动信息技术实现按需供给、促进信息技术和数据资源充分利用的全新业态,已成为信息化发展过程中的重大变革和信息技术发展的必然趋势.然而,正是由于云计算模式所具有的一些特性,如云计算平台的服务外包和基础设施公有化特征、超大规模多租户资源共享特征、云计算环境的动态复杂性、云平台资源的高度集中性、云平台的开放性等,使得人们在享受云计算所提供的应用便利和成本低廉的同时,也逐渐意识到了其在诸多安全方面的全新挑战.新的计算模式需要新的安全保障技术、理论和方法来应对安全挑战,如在外包环境下如何实现用户数据安全防护、如何实现虚拟化技术的安全性、如何设计适合云计算环境的安全协议、如何构建一个安全可靠的云计算平台以及如何测试和评价云计算平台的安全性等.本专刊选题——云计算安全研究,力图反映我国学者在云计算安全领域的近期研究成果.

专刊公开征文仅限一轮,共征得投稿37篇.稿件来自国家211大学以及中国科学院相关研究单位,质量相对较高.稿件涉及云计算安全理论、算法以及应用等诸多方面的研究内容.对于云计算环境、云数据以及云计算应用等方面的安全问题进行了深入的探讨,反映了我国学者近期对于云计算安全关注的主要研究方向.特约编辑先后邀请了40余位云计算安全及相关领域的专家参与审稿工作,每篇投稿邀请2位专家进行评审.稿件评审时间历经3个月,经初审、复审、云计算安全专题研讨会宣读和终审各个阶段,最终由《软件学报》编委会批准,决定19篇论文入选本专刊.纵观所收录的论文,它们的研究范围和内容可分为如下3部分:

首先是对云计算环境安全、云平台可信性分析、移动终端安全接入与虚拟化技术安全的相关研究对建立云计算安全体系安全架构的各个层次进行研究.

《云计算环境安全综述》从云虚拟化安全、云数据安全以及云应用安全这 3 个层面对云计算环境安全领域的相关工作进展、未来发展趋势以及后续研究方向进行了综述.

《一种云平台可信性分析模型建立方法》针对目前云平台可信性评价机制不完善的现状,在明确了云平台可信性的定义、子属性及具体分析内容的基础上,提出了有效的模型建立方法.

《基于 TrustZone 的可信移动终端云服务安全接入方案》针对目前移动终端安全接入云服务的研究空白,基于硬件隔离、物理不可克隆函数和可信计算等技术,设计提出了相关机制与协议,并给出了应用实例.

《虚拟机自省技术研究与应用进展》基于语义重构方式的不同对现有 4 类虚拟机自省技术从安全性、性

* 收稿时间: 2016-01-11; jos 在线出版时间: 2016-01-21
CNKI 网络优先出版: 2016-01-22 10:14:52, http://www.cnki.net/kcms/detail/11.2560.TP.20160122.1014.009.html

能及可获取的高层语义信息量等方面进行比较分析,综述了虚拟机自省技术的应用情况,指出未来研究方向.

《KVM 虚拟化动态迁移技术的安全防护模型》针对虚拟机动态迁移的安全问题,在虚拟化机制和虚拟化操作系统源代码的研究基础上,提出了一种新的基于混合随机变换编码方式的安全防护模型.

第 2 部分是云计算数据安全、云安全存储相关安全技术及机制的研究.对云计算安全的具体实施提供了有益的探讨.

《云存储中支持数据去重的群组数据持有性证明》考察了群组应用中的数据去重问题,基于矩阵计算和伪随机函数,提出了一种支持数据去重的群组 PDP 方案(GPDP),经理论验证和实际应用测试,效果良好.

《支持策略隐藏的加密云存储访问控制机制》针对在使用选择加密过程中的支持策略泄漏问题,提出了一种新的访问控制策略隐藏机制,能够在确保细粒度访问控制和高效密钥分发的同时,隐藏访问控制策略信息.

《具有私钥可恢复能力的云存储完整性检测方案》考察了共享数据云存储完整性检测中私钥不可用的问题,提出了具有私钥可恢复能力的检测方案,通过理论和实验证明了方案的安全高效性.

《融合门限公钥加密和纠删码的安全云存储模型》针对当前云存储系统中不能兼顾机密性和容错性的问题,基于门限公钥加密与指数纠删码技术,提出了能够同时满足二者要求的安全云存储模型,代价优势较好.

《基于二叉树存储的多用户 ORAM 方案》针对现有多用户 ORAM 方案中混淆过程计算复杂度高的问题,在基于二叉树 ORAM 方案的基础上构造了一个通过代理加密实现的多用户 ORAM 方案,具有良好的计算优势.

第 3 部分是关于云计算应用安全的研究.加密、认证机制及安全外包计算的相关研究对促进云计算安全的实用化发展起到了积极的推动作用.

《利用特征向量构造基于身份的全同态加密体制》针对现有全同态加密体制的计算低效问题,基于任意次数分圆环代数结构提出了一种新的全同态加密体制和一种机制转换方法,可实现良好的计算和存储效率.

《一种实现一般电路的密钥策略的属性加密方案》针对现有属性加密方案中的电路受限问题,基于电路等价转换思想并引入转换密钥,提出了一种可实现节点跨层输入的新方案,其选择安全性得到了理论上的证明.

《标准模型下隐私保护的多因素密钥交换协议》以两方口令认证密钥交换协议、鲁棒的模糊提取器以及签名方案为基本组件提出了一个标准模型下可证明安全的多因素协议,具有良好的计算和通信效率.

《云环境下基于 PTPM 和无证书公钥的身份认证方案》针对目前云环境下身份认证过程中的安全问题,首次将 PTPM 和无证书公钥密码体制应用于云环境,提出的方案在理论证明和性能分析中具有良好的计算效率.

《一种透明的可信云租户隔离机制研究》针对云租户隔离问题,对隔离机制进行定义,制定了云计算平台中的域间信息流策略控制方式,基于信息流无干扰理论证明了所定义的云租户隔离机制在安全方面的有效性.

《云环境下集合隐私计算》针对多方集合隐私计算问题,基于新的编码方案和同态加密算法构造了一个具有普遍适用性且抗合谋的保密计算集合并集问题解决方案,具有良好的可扩展性.

《基于相似查询树的快速密文检索方法》针对现有方案中对大数据量的密文检索低效问题,基于相似查询树的聚类思想,提出了一种快速密文检索方法,并通过实验验证了该方法的计算效率显著高于传统检索方法.

《对加密电子医疗记录有效的连接关键词的搜索》考察在医疗场景下如何高效检索密文的问题,构造提出了一个多域连接关键词搜索的初步方案及后续的提高方案,在理论上被证明可抵抗已知明文攻击.

《同态公钥加密系统的图像可逆信息隐藏算法》针对加密图像的有效管理及安全保护问题,基于差分扩展和同态加密技术,提出了一种图像可逆信息隐藏算法,并通过实验验证了该算法的计算效率优势.

本专刊主要面向云计算安全相关领域的研究人员,反映了我国学者在云计算安全领域的最新研究进展.在此,我们要特别感谢《软件学报》编委会对专刊工作的指导和帮助,感谢编辑部各位老师从征稿启示发布、审稿专家邀请至评审意见汇总、论文定稿、修改及出版所付出的辛勤工作和汗水,感谢专刊评审专家及时、耐心、细致的评审工作.此外,我们还要感谢向本专刊踊跃投稿的作者对《软件学报》的信任.

最后,感谢专刊的读者们,希望本专刊能够促进相关领域的研究工作.

薛锐(1963－),男,博士,研究员,博士生导师,主要研究领域为公钥密码学,安全协议以及相关理论基础和应用研究.

任奎(1978－),男,博士,副教授,主要研究领域为云计算安全,物联网,无线网络安全.

张玉清(1966－),男,博士,教授,博士生导师,主要研究领域为网络与系统安全,安全协议与云安全,移动互联网安全.

李晖(1968－),男,博士,教授,博士生导师,主要研究领域为密码信息安全,信息论,编码理论.

刘吉强(1973－),男,博士,教授,CCF 会员,主要研究领域为可信计算,隐私保护.

赵波(1972－),男,博士,教授,博士生导师,主要研究领域为密码学应用,信息系统安全,可信计算,嵌入式系统,云计算安全,网络安全技术.

祝烈煌(1973－),男,博士,教授,博士生导师,主要研究领域为密码协议及应用,云计算安全,物联网安全.