

面向应用的天基嵌入式云服务安全技术研究

邵应昭¹, 丁跃利¹, 张建华¹, 张佳鹏¹, 杨鹏飞², 李剑桥¹

(1. 中国空间技术研究院 西安分院, 陕西 西安 710100;

2. 西安电子科技大学, 陕西 西安 710071)

摘要:地面云计算及其应用安全技术已发展成熟,天基信息基础设施虽经过多年发展且已形成一定规模,但由于其构建于资源受限的空间嵌入式环境,基于计算机系统的地面云及安全相关成熟技术无法直接应用于天基系统,导致目前多为一星一平台的独立系统,不具备网络化的共享服务能力。文中在对地面云计算及安全技术发展现状进行调研的基础上,结合天基信息云平台的高效能资源共享和应用服务安全建设需求,提出了由覆盖全球的多颗综合卫星体构成天基网络化嵌入式云服务平台的系统物理拓扑设想,并在此物理架构的基础上形成了天基分层式的云安全软件架构,最后在软件架构中提出了天基云系统应用安全服务体系的构建思路,可实现天基资源的安全共享,并保证广大用户的接入、检索和应用安全,为天基网络化嵌入式云服务安全平台构建提供参考。

关键词:云计算;云安全;天基云服务平台;嵌入式平台;高效能资源共享;天基应用安全

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2020)08-0109-06

doi:10.3969/j.issn.1673-629X.2020.08.018

Study on Cloud Service Security Technology of Space-based Embedded System Application

SHAO Ying-zhao¹, DING Yue-li¹, ZHANG Jian-hua¹, ZHANG Jia-peng¹,

YANG Peng-fei², LI Jian-qiao¹

(1. China Academy of Space Technology (Xi'an), Xi'an 710100, China;

2. Xidian University, Xi'an 710071, China)

Abstract: The ground cloud computing and its application security technology has been developed and mature. Although the space based information system has developed over a number of years and formed a certain scale, due to the construction of a space-constrained space embedded environment, the ground based cloud and security technologies based on computer systems cannot be directly applied to the space based system. As a result, it is mostly a standalone system with one platform for one satellite at present, without the ability of network shared services. Based on the investigation of the development of ground cloud computing and security technology, combined with the high efficiency resource sharing and application service security construction requirements of space based information cloud platform, the system physical topology of space based networked embedded cloud service platform is proposed, which is composed of several integrated satellite bodies covering the entire global region, and a space based hierarchical cloud security software architecture is formed on the basis of this physical architecture. Finally, construction guidelines of the application security service system of the space based cloud system are put forward in the software architecture, which can realize the secure sharing of space based resources and ensure the access, retrieval and application security of the majority of users. It provides a reference for the construction of space based embedded cloud service security platform.

Key words: cloud computing; cloud security; space based cloud service platform; embedded system; high performance resource sharing; space based application security

0 引言

随着信息技术和物联网技术的快速发展,未来信息服务基础设施将建设互联互通的天地一体化信息网

络系统,具备向众多用户群体提供网络化、差异化信息服务的能力。天基信息系统是国家信息化建设的重要基础性设施,它通过运行在外空间的星载资源实现信

收稿日期:2019-10-10

修回日期:2020-02-27

基金项目:国家自然科学基金(61572385,61972302,61702395)

作者简介:邵应昭(1983-),男,硕士,高级工程师,研究方向为星载嵌入式智能计算平台、星载云计算、云服务安全、微纳卫星载荷等。

息的获取、传输、处理及分发等功能,获取全球范围内近实时的态势感知情报^[1]。天基信息系统作为未来信息服务基础设施的重要组成部分,将基于嵌入式架构构建网络化云平台,以提高天基信息服务基础设施的整体服务效能^[2]。

安全防护保障为天地一体化信息网络可靠运行的关键支撑。有别于地面传统网络,天地一体化信息网络节点分布广泛、体系结构复杂、信道开放透明、拓扑动态变化、大尺度传输链路以及面向全球提供服务保障的网络特征,使其数据传输、信息服务等本身就更易受到来自外部的自然干扰和恶意攻击,这对各方面的安全运行能力提出了更高要求^[3-4]。

天基信息系统基于天基网络化云平台构建,云平台面向各类用户提供云计算、云存储和数据库检索等服务,但超大规模天基用户的共享资源应用、计算环境的动态复杂性、平台资源的开放性等特性,使得天基网络体系建设面临信息安全诸多方面的全新挑战。一方面,由于空间链路的开放性,怀有各种目的外部攻击者非法入侵天基网络系统来窃取或者破坏资源,一旦遭受攻击,将发生不可估量的损失。另一方面,由于天基嵌入式云平台资源高度共享,接入平台的内部好奇用户期望获取自身权限以外的隐私或保密数据,对用户的隐私数据安全也会带来一定的挑战。

因此,在构建天基网络体系云平台的同时,需构建安全服务体系,面向广大用户的应用服务需求,提供安全接入鉴权控制能力和分级权限安全控制能力,从信息安全角度屏蔽非法用户接入、限制内部好奇用户的越权行为,并保证数据的真实性、机密性、完整性和不可否认性。

1 云计算及安全技术发展概况

1.1 云计算技术发展概况

云计算是网格计算、并行计算、效用计算、网络存储、虚拟化、负载均衡等传统计算机技术和网络技术发展融合的产物^[5]。相对传统计算机系统,使用云计算具有以下优势^[6]:

(1)资源共享,低成本:云计算组件通过网络互联,向用户提供共享服务,降低成本。

(2)应用安全:多用户以受控方式独立运行在隔离的虚拟化环境下,可通过管控虚拟机的权限来提高应用安全性。

(3)资源可伸缩:提供弹性的计算与存储资源管理服务,以满足用户不同的资源需求。

(4)应用快速部署:支持应用动态部署,快速启动计算任务。

云计算相关技术已成熟,其发展历程大致如下^[7]:

20 世纪 60 年代,IBM 首先推出虚拟化技术并应用在其 7044 计算机系统,使得在同一台物理主机可以同时运行多个物理设备。之后 IBM 又开发了型号为 Model 67 的 System/360 主机进行虚拟化应用,通过虚拟机虚拟所有的硬件接口,直接运行在底层硬件,使得系统可同时运行多个虚拟设备。

1999 年,VMware 公司解决了 X86 硬件平台的完全虚拟化问题,推出了 X86 平台的虚拟机软件,支持 X86 平台上的所有客户操作系统,虚拟化技术开始走向普通用户。

2005 年~2006 年,Intel 和 AMD 推出支持虚拟化技术的处理器和芯片组,实现了硬件辅助虚拟化技术。Amazon 采用虚拟化技术提供云计算平台,取得了商业上的成功。

2012 年,美国风河公司提出嵌入式云计算概念。

嵌入式云计算概念的提出,为天基云平台构建提供了可能。类似于地面计算由本地单节点计算发展到云计算,用户计算机的配置要求大幅降低,整体系统计算效能大幅提高。空间计算体系由单星计算向云计算系统发展,将带来天基计算模式的应用转变,可降低卫星或终端用户的处理资源要求,解决当前卫星系统资源利用效率低、共享能力弱的问题。

1.2 云计算安全发展现状

云计算发展面临许多关键性问题,而安全问题首当其冲。并且随着云计算的不断普及,安全问题的重要性呈现逐步上升趋势,已成为制约其发展的重要因素。Gartner2009 年的调查结果就已显示,70% 以上受访企业的 CTO 认为近期不采用云计算的首要原因在于存在数据安全性与隐私性的忧虑^[8-10]。根据 Gartner 的调查报告,超过 85% 的用户对云计算的安全性表示关注,用户对安全性的关注程度超过系统可用性、系统性能等,安全性已成为用户最为关注的方面^[11-13]。

云计算系统不仅面临着传统信息系统(或软件系统等)的安全问题,还面临着由其运营特点所产生的一些新的安全威胁^[11]。云计算在安全方面必须解决好下列问题:多租户高效、安全的资源共享;租户角色信任关系保证;个性化、多层次的安全保障机制;以及效率、经济性与安全性兼顾的多属性服务系统^[14]。

现有的云计算安全架构^[15]主要分为三类:基于可信根的云计算安全架构试图通过可信计算的成果从根本上解决云计算的安全问题,但不利于对现有资源的继承与利用。基于隔离的云计算安全架构旨在针对所有的租户构建封闭且安全的运行环境,从而保证其定制服务的安全性,但其势必增加租户间协作的难度,引起管理成本的提高。安全即服务的架构充分考虑到了

一个循序渐进、不断完善的过程,系统框架、机制的设计不仅需要兼容现有天基分立系统和后续部署系统的资源异构性,同时需要支持不同用户的安全差异性和陆、海、空、天的多源异质数据安全接入。

天基网络化嵌入式云服务平台与用户的交互及使用流程具体如下:

- (1) 用户通过星地接入控制链路访问天基云系统;
- (2) 天基云系统门户对用户进行身份认证;
- (3) 用户根据自身需求向云系统门户提交计算、存储、网络资源申请;
- (4) 天基云系统门户根据用户权限等级和资源调

配情况,为用户分配资源;

- (5) 用户完成计算任务,向门户提交资源释放申请;
- (6) 门户释放资源,将其整合到可用资源池中。

2.2 天基分层式云安全软件架构

针对天基嵌入式云服务体系需要具备多用户身份认证、大数据安全接入控制、天基安全加密云存储及安全检索、计算权限安全控制等能力需求,在充分调研、研究地面通用云计算软件层次架构的基础上,结合天基云系统与地面系统的差异,提出了如图 3 所示的天基分层式云安全软件架构。

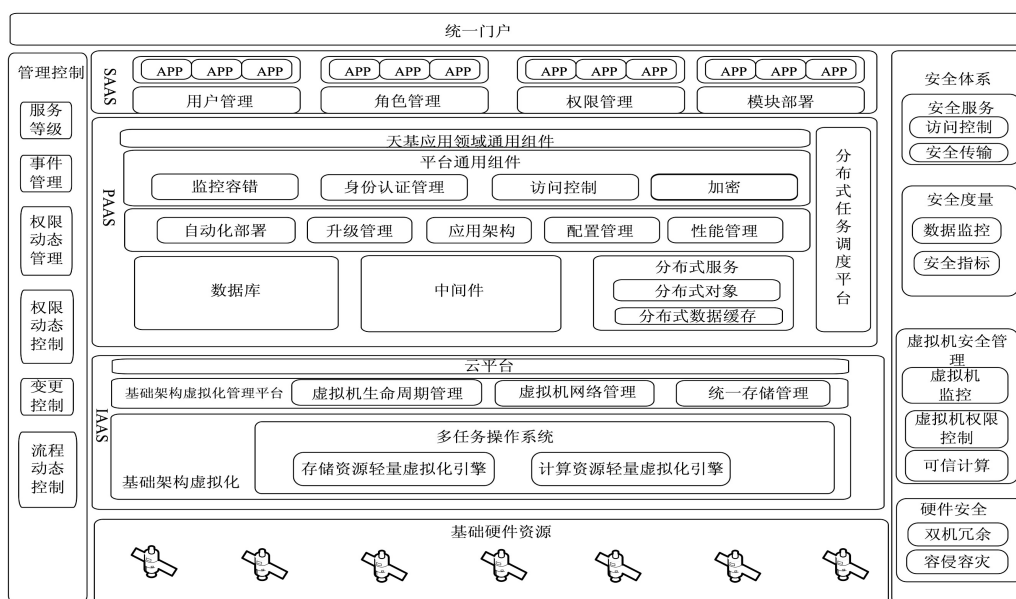


图 3 天基分层式云安全软件架构

可管、可控、可度量云计算的安全架构基于地面云计算安全架构的理论和研究成果,提出了结合当前主流三类安全架构优势的综合架构,可为各类云计算安全系统构建提供参考。

天基分层式云安全软件架构面向天基云系统的应用场景和特殊环境安全需求,借鉴可管、可控、可度量的架构思路,其构建的天基安全服务框架针对天基特殊环境及应用场景下的 SaaS、PaaS、IaaS 三层具体云服务组件进行设计。安全度量部分可实现天基分布式平台数据和用户数据的安全监控,并进行安全指标和能力的量化分析,提供给天基用户,可支持不同用户选择适合自身应用场景的安全策略,最终实现天基云系统安全“可度量”。安全架构支持对用户、权限、时间、流程、系统变更等不同方面的动态安全管理和控制,可实现天基云系统安全“可管”、“可控”。

天基分层式云安全软件架构基于天基环状网络物理实体实现部署运行,将天基分布式基础网络、计算、存储资源通过标准万兆网协议实现网络化互联,并实

现资源的虚拟化和动态管理控制,面向用户应用需求,实现天基基础硬件资源的动态管理和硬件架构重构。在满足用户资源使用、资源共享和应用服务的同时,结合架构中的安全管理、安全控制、和安全度量等安全策略,保障用户过程安全和数据安全。

软件架构基于底层硬件资源可以分为基础服务层(IaaS)、应用支撑层(PaaS)和统一门户层(SaaS)。在对地面云系统软件架构进行裁剪的基础上,增加三大部分组件,添加面向嵌入式硬件资源的轻量虚拟化引擎;添加安全服务、虚拟化安全管理、硬件安全三个层面构建的安全服务体系;添加在轨处理、多源检索、用户权限管理等天基应用相关组件。最终构建的天基云系统软件架构向用户提供 SaaS 和 PaaS 两层服务,IaaS 不对用户开放,为用户应用提供虚拟化资源;每一层均涉及安全服务。IaaS 基础层分为虚拟化层和虚拟化管理平台,虚拟化层运行在操作系统之上,主要对异构资源虚拟化,屏蔽底层差异性,构建天基云系统的计算、存储、网络资源池,资源池逻辑统一,向上层提供服务。

天基云系统软件架构以 TPM 可信平台模块为可信根,可信虚拟机负责密钥管理和分发任务,最大程度满足可信计算关于防旁路、防篡改等基础要求,为系统提供高级别安全保障。

应用支撑层包括平台通用应用组件和领域通用组件两个部分,平台通用应用组件包括身份认证管理、权限控制、自动化部署、加解密操作、监控容错,身份认证管理采用双向用户身份认证,将授权合法用户接入,屏蔽非法、无效用户屏蔽;权限控制采用细粒度控制策略,将云平台的资源和对资源访问的权限细分,划分不同的用户组;自动化部署为用户的应用提供运行环境,支撑用户的应用动态部署,用户采用多种开发语言的应用上传到云平台后,将会在底层启动相应的虚拟机,虚拟机内自动安装应用所需的执行运行环境,应用执行完后,相应虚拟机回收释放资源。加解密操作一方面作为在进行用户增加等系统操作时产生所需的非对称密钥,为大数据的流加密提供对称密钥等,同时也提供给用户使用,用户可以自主调用加解密模块在应用内实现相应的加解密操作。

3 天基云系统应用安全服务体系构建

天基云系统应用安全服务体系在天基分层式云安全软件架构中实现,作为操作系统的标准安全控制组件在天基云软件上部署运行,在嵌入式安全服务总体架构下,基于虚拟化安全隔离等关键技术,实现天基资源的安全共享,并保证广大用户的接入、检索和应用安全。

3.1 天基应用安全服务体系架构

天基云系统应用安全架构如图4所示,采用层次化的云安全策略,可为云系统用户提供云数据安全存储、隐私保护、可信云计算的服务。

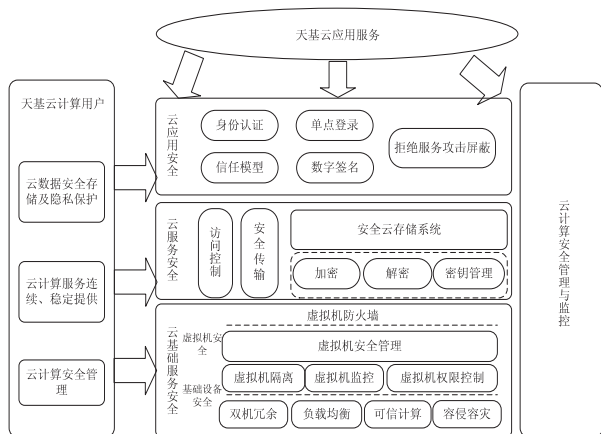


图4 天基安全服务体系架构

云系统安全架构可以分为云应用、云服务和云基础服务安全层,不同层引入了相应的安全策略,在云基础服务层包括基础设备安全和虚拟机安全,基础设备

安全包括双机冗余、负载均衡、可信技术和容侵容灾四个部分,体现在硬件平台采用了双主控板的方式协同处理大数据的接入,监控系统监控到单主控失效后,在秒级单位内将大数据接入任务切换到备份主控,提供不间断服务;在计算单元内具有 TPM 可信平台模块,包括随机数生成、SHA-1 引擎、RSA 引擎、非易失性存储器等,以此为可信计算的信任根,负责保存具有访问系统权限的用户和系统自身的公钥和私钥,生成对象加密密钥等;同时硬件层之上的操作系统的内核和应用也进行了裁剪,去除不相关的模块,降低底层因为软件漏洞等因素被入侵的概率。对虚拟机的安全采用了一系列的安全措施,首先限制虚拟机与外面的通信,对虚拟机设置防火墙,限制可以访问虚拟机的端口和用户,同时虚拟机间进行隔离和监控,实时监控虚拟机的运行状态,防止虚拟机内运行的应用恶意攻击系统和其他正常虚拟机,最小化虚拟机内应用崩溃等对其他正常应用的影响。同时通过权限控制策略限制不同虚拟机的可访问资源,保护敏感数据不受非法操作。

在云服务层包括访问控制、安全传输和安全云存储三个部分,访问控制主要针对用户,细粒度划分系统的资源访问控制权限,将用户划分不同安全级别进行资源的使用。安全传输包括采用流加密方式将百 Gbps 数据加密传输,其他用户数据的传输采用非对称加密传输,安全云存储系统可以根据数据的安全等级采用不同加密算法对数据加密,同时利用 TPM 模块将加密文件的密钥存储在本地磁盘。

云应用层包括身份认证、拒绝服务攻击屏蔽等,卫星接入天基云系统需要进行身份认证,认证完成后即以单点登录的方式登录系统,随后可以访问系统内所有授权的资源,同时用户数据传输时采用数字签名的方式防止未授权卫星等发送伪造数据攻击系统,采用了双端口的方式屏蔽拒绝服务攻击,用户通过非受控端口与云系统进行双向身份认证,在完成身份认证后,计算平台为成功认证后的数据源分配一个特定的受控端口;之后,数据源可通过云系统的特定受控端口实现到云系统的安全接入。

3.2 面向应用安全的天基嵌入式安全服务策略

天基网络化嵌入式安全云服务体系的安全服务策略基于图4所示的安全服务体系架构,均在图3所示的天基分层式云安全软件应用层实现,安全服务策略覆盖用户与天基云平台的交互和操作全流程,针对不同的安全威胁,采用不同的安全服务策略。安全服务策略主要包含防护、检测、响应和恢复四种安全机制,又可细分为七类安全措施,为各类用户提供接入安全、应用安全、计算安全、系统安全等安全服务。图5所示为基于 PDRR (protect、detect、response、recover) 安全模

型实现的天基云平台安全服务策略。

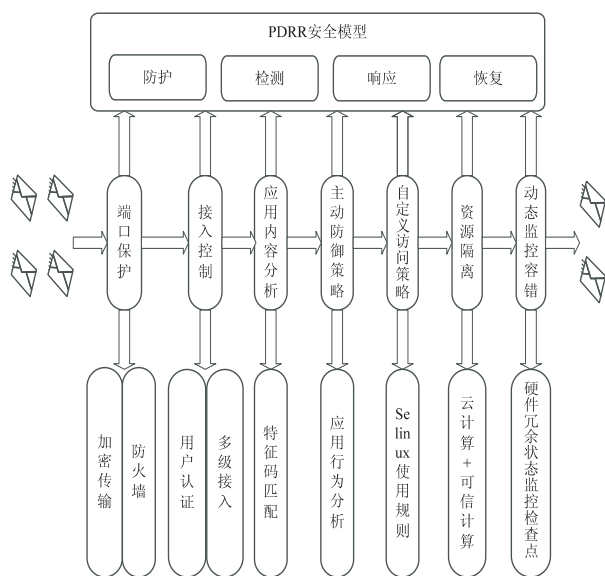


图5 天基嵌入式安全服务策略

安全服务体系参考 PDRR 标准安全体系模型,包含防护、检测、响应、恢复四部分,共七个层次。端口保护以防火墙为主,加密传输为辅,屏蔽非法请求;接入控制通过多级安全服务策略实现用户安全接入认证;检测部分采用动静结合策略,首先提取应用执行体特征码,与已知恶意程序匹配,清除恶意程序,并通过监控程序发送警报,随后在虚拟环境下观察应用调用系统 API 接口的动态,判断应用合法性;响应部分采用自定义访问策略和资源隔离的手段,基于 SELinux 安全模块定义适用于天基云平台的安全策略,实时限制非法操作,同时利用虚拟化技术实现应用间的逻辑隔离,切断非法操作;最后的恢复部分采用动态监控容错技术,具体为硬件冗余、系统状态监控和软件检查点策略,提高系统遭受攻击时的顽存性。

4 结束语

在充分调研云计算及安全系统发展历程及相关关键技术发展的基础上,结合天地一体化信息网络系统对天基信息基础设施提出的云计算及安全服务体系需求,提出了天基网络化嵌入式云服务平台构建思路,以及基于嵌入式云服务体系的天基云系统应用安全架构,可提高天基云平台资源利用效率,实现天基资源高效能共享,并有效解决海量多用户接入、计算、存储安全等问题,可为天基嵌入式云计算及安全服务体系构建提供有效参考和借鉴。

参考文献:

- [1] 李 斌,刘乘源,章宇兵,等. 天基信息港及其多源信息融合应用[J]. 中国电子科学研究院学报,2017,12(3):251-256.
- [2] 王 磊,梁 俊,刘淑芬. 小卫星智能自组织云计算体系研究[C]//2015 年小卫星技术交流会论文集. 北京:中国宇航学会,2015:322-327.
- [3] 李凤华,殷丽华,吴 巍,等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报,2016,37(11):156-168.
- [4] 季新生,梁 浩,扈红超. 天地一体化信息网络安全防护技术的新思考[J]. 电信科学,2017,33(12):24-35.
- [5] 朱 兵,叶 飞,王 阳. 服务器虚拟化技术初探[R]. 北京:中国电力企业,2011.
- [6] 范 焱,庞芳梅,邵 刚. 云计算和云数据管理技术[J]. 硅谷,2013(24):47.
- [7] 张建勋,古志民,郑 超,等. 云计算研究进展综述[J]. 计算机应用研究,2010,27(2):429-433.
- [8] 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.
- [9] 赵鑫龙. 云计算安全动态检测与静态评测技术研究[D]. 大连:大连海事大学,2017.
- [10] CHEN Y, PAXSON V, KATZ R H. What's new about cloud computing security[R]. California: University of California, 2010.
- [11] ALI M, KHAN S U, VASILAKOS A V. Security in cloud computing: opportunities and challenges[J]. Information Sciences, 2015, 305:357-383.
- [12] GUILIO D C, SPRABERY R, KAMHOUA C, et al. Cloud standards in comparison: are new security frameworks improving cloud security? [C]//2017 IEEE 10th international conference on cloud computing (CLOUD). Honolulu: IEEE, 2017.
- [13] SHEN Zhidong, LI Li, YAN Fei, et al. Cloud computing system based on trusted computing platform[C]//International conference on intelligent computation technology and automation. Changsha: IEEE, 2010.
- [14] MAHALLE S, JAISWAL R. Cloud computing security: a survey[J]. International Journal of Computer Applications, 2015, 115(6):21-25.
- [15] 林 闯,苏文博,孟 坤,等. 云计算安全:架构、机制与模型评价[J]. 计算机学报,2013,36(9):1765-1784.