DOI:10.3969/j.issn.1000－1565.2018.04.014

基于动态信任评估的政务数据云服务平台设计

张彬[1],李继民[2],张寿华[2],陈学海[3]
(1.河北大学 信息技术中心,河北 保定 071002;2.河北大学 网络空间安全与计算机学院,河北 保定 071002;
3.保定人民广播电台 技术部,河北 保定 071000)

摘 要:基于动态信任评估的政务数据云服务平台通过统一的云服务接口和数据标准能够有效促进政府各部门之间的互连互通、业务协同,避免产生信息孤岛,同时有利于推动政府大数据开发与再利用.平台采用层次化的系统结构,在云服务安全管理中将宿主机的可信状态、虚拟机的可信度、云服务的安全级别、云用户的行为记录纳入动态可信评估范畴,对外提供政务云数据中心服务和政务云业务应用.在安全管理中将 TCM 可信服务引入到传统云服务中进行云服务可信化管理,把信任关系从可信根传递到云主机及政务数据云服务;采用 ANP 行为矩阵对云用户行为证据进行信任值度量,建立云用户行为动态信任评估安全机制,为政务数据提供安全可信的云服务.

关键词:可信计算;云服务;动态评估;云安全
中图分类号:TP311 **文献标志码**:A **文章编号** 1000-1565(2018)04-0432-05

A cloud service platform design based on dynamic trust evaluation

ZHANG Bin[1], LI Jimin[2], ZHANG Shouhua[2], CHEN Xuehai[3]
(1. Information Technology Center, Hebei University, Baoding 071002, China;
2. School of Cyber Seurity and Computer, Hebei University, Baoding 071002, China;
3. The Technical Department, Baoding People's Broadcasting Station, Baoding 071000, China)

Abstract: The government data cloud service platform is based on dynamic trust assessment. It can effectively promote inter connection and business collaboration between various departments of the government. It avoid the generation of information island through a unified cloud service interface and data standard. It helps to promote the development and reuse of the government's large data. The category of dynamic trusted evaluation include the trusted state of the host in the cloud service security management, the credibility of the virtual machine, the security level of the cloud service, and the behavior records of the cloud users. The government cloud data center and the application of government cloud business are provided to the outside world. In the security management, TCM trusted service is built into the traditional cloud service to manage cloud services. Trust relationship is transferred from trusted root to cloud host and government data cloud service. The trust value of cloud user behavior evidence is measured by ANP behavior matrix, and cloud user is established as a security mechanism for dynamic trust evaluation, and a secure and credible cloud service is provided for government data.

Key words: trusted computing; cloud service; dynamic evaluation; cloud security

收稿日期:2017-10-11
基金项目:教育部"云数融合 科教创新"基金资助项目(2017A20004);国家科技支撑计划项目(2013BAK07B04)
第一作者:张彬(1980—),男,河北涿州人,河北大学高级实验师,主要从事网络安全方向研究.E-mail: zb@hbu.edu.cn
通信作者:张寿华(1980—),男,河北广宗人,河北大学副教授,主要从事计算机系统方向研究.E-mail: zhangshouhua@hbu.edu.cn

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

政府部门在大数据时代对业务系统的高效快速部署要求越来越高,越来越多的传统政府数据业务迁移为云服务的方式提供对内对外服务.如何对政务数据云服务进行可信管理,采集分析云用户的访问行为进行动态监管,提供安全可信的云数据服务成为一个需要解决的重要问题.云服务平台的架构、云服务类型及业务提供方式复杂多样[1],通常采用层次分析法与网络分析法等应用在行为证据的评估方面,配合双滑动窗口的方法对行为证据的增量数据监控,能够有效地提高评估的准确性[2-3].政务云属于行业云的一种,通过统一的云服务接口和数据标准能够有效促进政府各部门之间的互连互通、业务协同,避免产生信息孤岛,同时有利于推动政府大数据开发与再利用.政务云的重要数据都存储在虚拟资源池中,云服务平台提供的数据服务的安全状况,云数据服务的访问授权的监管机制,云用户的行为异常分析成为提高云服务安全的重要保证[4].

本文基于动态可信评估技术,建立了一种政务数据云平台安全平台,在 TCM 的可信云基础架构上,通过用户行为动态信任评估等安全机制,提供安全可信的政务数据可信云服务.

1　政务数据可信云服务平台总体结构设计

政务数据可信云服务平台设计主要集中于基础设施服务和平台控制服务 2 大核心业务层.内置 TCM 的可信服务器、虚拟化服务器集群和云平台管理系统是平台的重要组成部分.可信服务云平台的基础设施层(Infrastructure as a Service,IaaS)、平台服务层(Platform as a Service,PaaS)、应用服务层(Software as a Service)进行对接,采用主流 PCServer 计算节点提供计算服务.在云服务安全管理中将宿主机的可信状态、虚拟机的可信度、云服务的安全级别、云用户的行为记录纳入动态可信评估范畴,对外提供政务云数据中心服务和政务云业务应用[5],系统结构如图 1 所示.

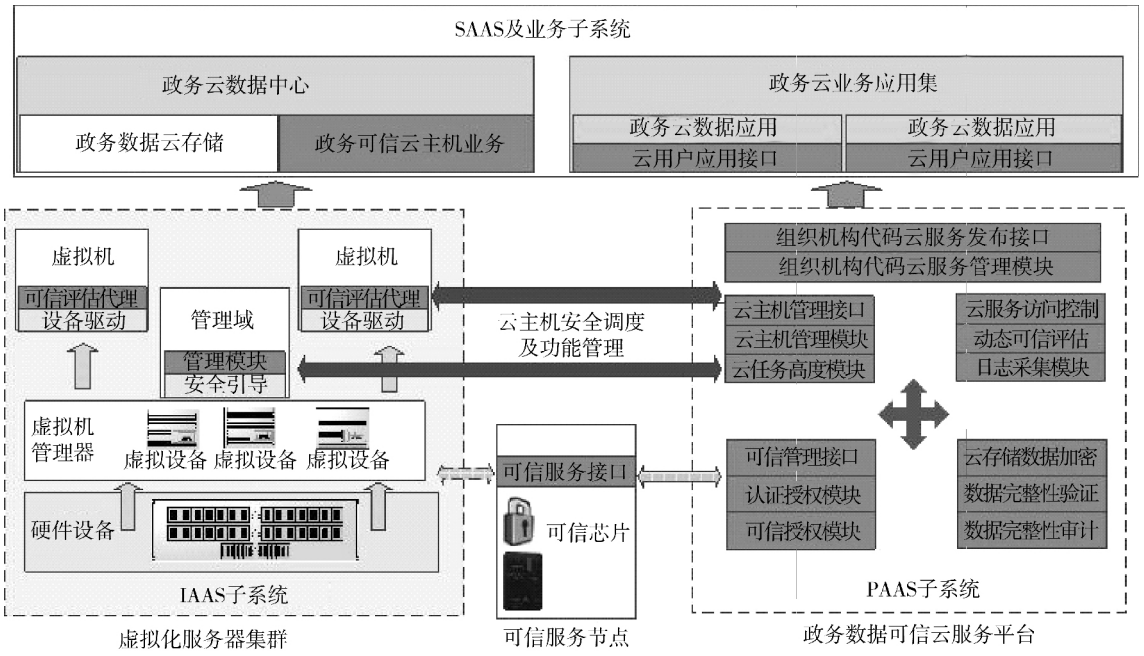

图 1　政务数据可信云服务平台系统结构

Fig.1　System structure of trusted cloud service platform for government data

政务数据可信云服务平台采用层次化的系统结构,可信服务模块(Trusted as Service Module)使用云服务的方式把可信模块功能纳入平台统一管理,通过可信服务接口调度管理虚拟化系统,从而将信任关系从可信根传递到云主机及政务数据云应用.

可信服务器内置 TCM 安全芯片,提供政务数据可信云服务平台的信任根服务.从信任根开始,建立一条信任链,按照系统启动的顺序,依次逐级验证 BIOS、自举程序、操作系统和可信根服务程序;通过可信根服务接口将信任链依次传递到云平台系统、云服务管理系统;信任链通过可信评估代理的验证服务,会依次

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

传递到云主机和云服务[6].

虚拟服务器集群采用常规物理服务器,通过虚拟化系统提供硬件虚拟化服务.管理域(Domain0)通过政务数据可信云服务平台与可信服务器对接,实现安全控制相关功能.

2 基础设施服务设计

本系统的IaaS层基于开源虚拟化系统实现,提供物理服务器的底层虚拟化,管理域通过可信云主机管理平台与可信服务器节点对接,对虚拟机底层硬件进行可信验证.

2.1 IaaS层设计要点

云主机管理系统和云服务管理系统独立模块化设计,通过API接口对接.2个系统既可以联动使用提供高安全性的可信服务,也可以独立运行提供云主机业务和云服务安全管理功能.

虚拟化平台采用开源的虚拟化系统,宿主机不直接架设于专用的可信物理服务器,而是采用常规的物理服务器,通过云服务器平台与可信服务器对接,减少可信物理主机的部署成本.使用独立的安全域和物理隔离机制对不同信任级别的网络通信进行访问控制,集群管理网络与业务网络分离,通过与动态信任评估联动策略控制不可信网络与可信网络间的互通,大大提高了可信云服务的安全性[7].

可信评估代理组件安装于云主机,实时采集虚拟机的虚拟硬件信息,提交到可信云服务系统进行主机行为特征采集.结合宿主机的硬件表示,根据云主机的虚拟硬件信息生成云主机特征码,如可信评估代理检测到虚拟硬件发生篡改或异常变动,云服务平台会动态计算评估云主机信任度评分和安全级别,云服务控制模块联动进行告警、阻拦、审计或停止相关云服务[8].

2.2 虚拟资源的可信管理

政务数据云系统通过API方式对计算节点的特权域直接控制,实现对虚拟机的虚拟硬件校验及虚拟机控制.计算节点采用传统的高性能服务器,通过可信服务认证后在政务数据云服务平台中提供计算服务,云平台通过特权域方式对普通的计算节点进行授信管理.

特权域在虚拟化系统中提供管理及可信服务对接功能,虚拟化系统采用混合模式,授权一个特权的虚拟机协助虚拟机管理器参与其他虚拟机的管理.在虚拟化系统中对虚拟化机制进行实现,而在授权的虚拟机中去设计和指定每个客户系统具体的实现策略.特权域在随着虚拟化系统的启动而建立,根据云主机的虚拟硬件、CPU标识、硬盘、网络地址、特征文件等信息生成云主机虚拟意见摘要,通过底层API接口与可信服务器进行硬件比对.

3 平台控制服务设计

3.1 PaaS层设计要点

平台即服务层以IaaS层服务为基础,将组织机构代码的基础数据进行整合,进行合理的资源配置和管理,提供资源统一服务入口,有效实现信息资源的整合、互换与共享.PaaS层以数据资源为核心,提供资源共享与协同调度功能,为SaaS层和其他应用提供数据访问服务[9].另外,PaaS层采用统一安全认证及授权控制机制,支持云主机注册、可信评估代理注册、云用户认证、云服务授权等功能.

系统的平台服务控制具有以下特点:

1)提供云主机平台资源管理、云主机控制、云主机管理等IaaS管理系统相关的所有操作功能,并提供API接口操作.

2)提供云平台的跨区域的分布式弹性云管理模式,完成对计算资源池、网络资源池、存储资源池的集中分配,支持对CPU、内存、存储、网卡、网络速率以及用户资源调配,并提供API接口操作.

3)支持通过用户名、密钥、IP等条件的云主机控制和云服务安全管理.

4)通过接口交互方式,与可信服务器、云主机平台、云服务平台进行对接,从信任根开始,建立一条信任链,通过可信根服务接口将信任链依次传递到云平台系统、云服务管理系统、云主机和云服务.

云平台的信任控制主要通过可信评估代理采集云主机原始信息,可信评估代理采集虚拟硬件信息摘要与云平台下发的虚拟硬件信息进行登记注册及动态比对,完成对虚拟硬件的安全校验;可信评估代理组件采

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

集云存储文件摘要信息进行初始登机和随机验证，同时进行云存储数据的完整性校验和篡改识别.平台控制层同时提供密钥产生和维护[10]、可信存储[11]、和安全数字签名[12]等安全功能.

3.2　云用户行为评估

系统采用 ANP 矩阵计算政务数据云用户的评估信任值[13]，通过采集各层次云用户行为，将收集到的行为证据按属性分为安全属性 A1 和开销属性 A2 2 类，并定义相应的评估准则，将采集的行为证据归类到相应的准则中，得到 ANP 加权矩阵[14].

$$\boldsymbol{A}=\begin{pmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \vdots & \vdots \\ a_{N1} & \cdots & a_{NN} \end{pmatrix}.$$

通过向量计算得到矩阵的归一化权重向量 w，运用的各个元素中，构成判断矩阵

$$\boldsymbol{w}_{ij}=\begin{pmatrix} w_{i1}^{(j1)} & \cdots & w_{i}^{(jn_j)}1 \\ \vdots & \vdots & \vdots \\ w_{in_i}^{(j1)} & \cdots & w_{in_i}^{(jn_j)} \end{pmatrix}.$$

利用规范后的行为证据，组成行为证据向量 $\boldsymbol{B}$ 并进行向量加权，得出 ANP 行为证据评估值公式

$$V_{\mathrm{ANP}}=W_F\boldsymbol{B}=[w_{f1},w_{f2},\cdots,w_{fN}][b_1,b_2,\cdots,b_N]^{\mathrm{T}}.$$

3.3　可信服务重发布

云服务提供者将云服务在平台注册并进行可信认证，云服务平台采用 ANP 行为证据评估方式对提供的云服务进行可信评估和重发布.政务数据云服务管理平台提供对云服务的注册、可信评估、认证授权、访问控制和行为分析功能.针对每个云服务，平台提供独立的访问权限控制和授权管理；最终服务以统一的接口进行重新发布，云用户可以通过该接口进行 API 访问，并集成到云业务应用.在云用户和云服务交互过程中，云服务管理平台提供认证授权、行为分析和可信评估功能.云服务发布模式如图 2 所示.

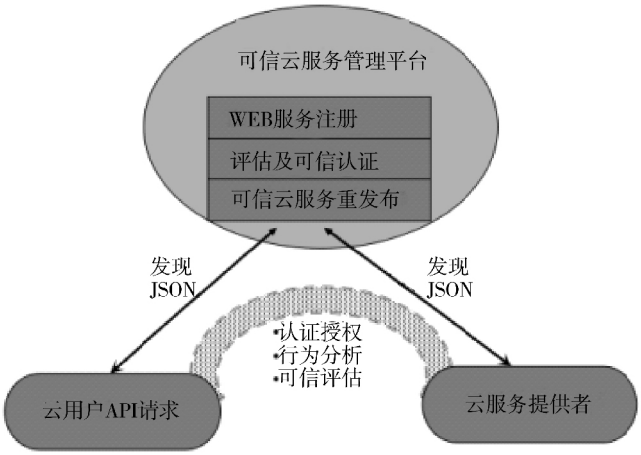

图 2　云服务发布模式

Fig.2　Publishing model of cloud service

平台中的云服务统一以 JSON 的接口标准进行注册发布，注册过程需将云服务的名称、业务代码、业务类型、服务源 URL、输入参数、输入参数进行统一管理.政务数据云平台对不同部署模式的云服务从低到高共划分为 3 种安全级别：

1）第三方云服务：架设在第三方云平台或服务器主机的政务数据云服务.作为第三方云服务注册后，以统一云服务接口，将云服务原始地址放置于云平台后端，提供安全防护作用.云平台提供认证授权、行为分析和访问控制功能.

2）认证的云服务：在第三方云服务运行的主机上安装可信评估代理，平台可以采集云服务主机的硬件信息和关键文件的完整性校验功能.云平台在第三方云服务的基础上提供了快照模式的硬件校验和文件校验功能，同时具备认证授权、行为分析和访问控制功能.此级别支持部署于常规物理服务器和第三方云服务器.

3）可信的云服务：架设于可信云主机平台且通过可信认证的政务数据云服务.云平台提供通过可信评估代理采集并校验云主机硬件信息和关键文件的完整性校验功能.云平台在第三方云服务的基础上提供了权威的硬件校验和文件校验功能，同时具备认证授权、行为分析和访问控制功能.仅部署于可信云主机平台，才能提供此级别可信的云服务.

4　结束语

设计了一种基于动态信用评估的政务数据云服务平台，该平台能够充分利用政务云数据中心的计算资源、存储资源、网络资源和数据资源进行规范化管理和整合.在充分利用原有云基础设施的前提下，通过可信

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

计算与动态信任评估机制集成构建政务数据可信服务,实现了政务数据云服务的安全发布及动态可信评估,可以有效地提升政务云相关信息服务的综合能力,为政务大数据提供安全的数据平台支撑.

参 考 文 献:

[1] 章谦骅,章坚武.基于云安全技术的智慧政务云解决方案[J].电信科学,2017,33(3):107-111.DOI: 10.11959/j.issn.1000-0801.2017063.
ZHANG Q H, ZHANG J W. System structure of trusted cloud service platform for government data.[J].Telecommunications Science,2017,33(3):107-111.DOI: 10.11959/j.issn.1000-0801.2017063.

[2] SHIN D H. User centric cloud service model in public sectors:policy implications of cloud services[J]. Government Information Quarterly, 2014, 30(2): 194-203.DOI:10.1016/j.giq.2012.06.012.

[3] MARSTON S, LI Z,BANDYOPADHYAY S. Cloud computing-the business perspective[J]. Decision Support Systems, 2011, 51(1):176-189.DOI:10.1109/HICSS.2011.102.

[4] DISHA M, PAREKH H. An analysis of security challenges in cloud computing[J]. International Journal of Advanced Computer Sciences and Applications, 2013, 4(1): 39-46. DOI:10.14569/IJACSA.2013.040106.

[5] TAMARA A, YOUSEF K. Cloud computing of e-government[J]. Communications and Network, 2016,01(8):1-8. DOI: 10.4236/cn.2016.81001

[6] 翟翔,贺也平. 基于可信计算的使用控制实施方案[J]. 计算机科学与探索, 2015,9(8):954-962. DOI: 10.3778/j.issn.1673-9418.1409077.
ZHAI X,HE Y P. Approach of usage control enforcement based on trusted computing[J]. Journal of Frontiers of Computer Science and Technology, 2015,9(8):954-962. DOI: 10.3778/j.issn.1673-9418.1409077.

[7] GONZALES D, KAPLAN J, SALTZMAN E, et al. Cloud-trust a security assessment model for infrastructure as a service (IaaS) clouds[J]. IEEE Transactions on Cloud Computing, 2017, 5(3):523-536. DOI: 10.1109/TCC.2015.2415794.

[8] MADNI S H H, LATIFF M S A, COULIBALY Y, et al. Resource scheduling for infrastructure as a service (IaaS) in cloud computing:challenges and opportunities[J]. Journal of Network & Computer Applications, 2016, 68:173-200. DOI:10.1016/j.jnca.2016.04.016.

[9] HAO W, RUI Z S, RUI Z, et al. Application feature based elastic resource management mechanism on paaS[J]. Chinese journal of computers, 2016(2):223-236. DOI:10.11879/SP.J.1016.2016.00223.

[10] 成茂才, 徐开勇. 基于可信计算平台的审计日志安全存储系统[J]. 计算机科学, 2016,43(6):146-151. DOI:10.11896.j.issn.1002-137X.2016.6.030.
CHENG M C, XU K Y. Audit log secure storage system based on trusted computing platform[J]. Computer Science, 2016,43(6):146-151. DOI:10.11896.j.issn.1002-137X.2016.6.030.

[11] 刘振鹏, 蔺志贤, 胡倩茹,等. 改进的基于身份的数据完整性验证方案[J]. 河北大学学报(自然科学版), 2017, 37(1): 86-91. DOI:1000-1565(2017)01-0086-06.
LIU Z P, MAN Z X, HU Q R, et al. Improved identity-based data integrity verification scheme[J]. Journal of Hebei University(Natural Science Edition), 2017, 37(1):86-91. DOI:1000-1565(2017)01-0086-06.

[12] 程思嘉, 张昌宏, 潘帅卿. 基于CP-ABE算法的云存储数据访问控制方案设计[J]. 信息网络安全, 2016(2):1-6. DOI: 10.3969/j.issn.1671-1122.2016.02.001.
CHENG S J,ZHANG C H,PAN S Q.Design on data access control scheme for cloud storage based on CP-ABE Algorithm[J].Netinfo Security,2016(2):1-6.DOI:10.3969/j.issn.1671-1122.2016.02.001.

[13] 王佳慧, 刘川意, 王国峰,等. 基于可验证计算的可信云计算研究[J]. 计算机学报, 2016, 39(2):286-304. DOI:10.11897/SP.J.1016.2016.00286.
WANG J H, LIU C Y, WANG G F, et al. Review of trusted cloud computing based on proof-based verifiable computation[J]. Chinese Journal of Computers, 2016, 39(2):286-304. DOI:10.11897/SP.J.1016.2016.00286.

[14] 田俊峰, 曹迅. 基于多部图的云用户行为认定模型[J]. 计算机研究与发展, 2014,51(10): 2308-2317. DOI:10.7544/issn1000-1239.2014.20130619.
TIAN J F, CAO X. A cloud user behavior authentication model based on Multi-Partite graphs[J]. Journal of Computer Research and Development, 2014,51(10): 2308-2317. DOI:10.7544/issn1000-1239.2014.20130619.

(责任编辑:孟素兰)

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net