文章编号：2096-1472(2016)-04-19-02

基于云计算的大数据安全保护研究

张玉琴
（常州建东职业技术学院电子与电气工程系，江苏 常州 213000）

摘　要：随着云计算的应用不断拓展，云计算自身也面临着巨大的挑战。本文针对数据访问隔离，提出了具有时态特性的多层次访问控制模型，保证信道中传输的静态数据以及用户下共同使用的数据，具有隔离性、正确性和完整性。

关键词：云计算；大数据；访问控制；安全性
中图分类号：TP393　　**文献标识码**：A

The Study of the Security and Protection of Big Data Base on Cloud Computing

ZHANG Yuqin
(*Department of Electric & Electronic Engineering,Jiandong Vocational Training College of Changzhou,Changzhou* 213000,*China*)

Abstract: Cloud computing is facing huge challenges itself with the enrichment and extension of cloud applications. This paper aims at the security of data and proposes a multi-level access control model with tense property.It ensures the security of static data transferred in the channel and data commonly used by users and is of great isolation, validity and integrity.

Keywords:cloud computing;big data;access control;security

1 引言(Introduction)

随着数据规模的不断增大以及互联网络的不断发展，云计算得到了越来越广泛的应用。云计算作为共享IT资源的一种方式，不仅能够满足人们对于高性能计算、大数据存储以及网络共享等功能的需求，同时使得软件作为一种服务而更加具有吸引力，并且改变了硬件设计和购买的模式。云计算在大数据处理以及资源共享方面具有极大的优势，可以为租户提供具有强大弹性扩展能力的计算资源和存储资源然而，随着云计算的应用不断拓展，云计算自身也面临着巨大的挑战，集中管理的数据资源出现了相应安全问题，由于现有的云计算系统部署相对分散，云计算系统之间的交互还没有统一的标准，关于数据流在SaaS、PaaS，以及IaaS层间仍存在一系列问题亟待解决。

2 国内外云计算大数据保护计算现状(The status at home and abroad of big data based on cloud computing)

2.1 云计算服务资源整合带来的安全性问题

在云环境层中，一般由众多独立的组件互相交互配合向上提供服务，对外表现为单一服务整体，对内表现为复杂的交互协议以及数量众多的交互接口和API。这些接口和API既面向租户，也面向内部组件，因此服务的整体安全性和可用性严重依赖于这些API和交互接口[1]。云计算环境一般存在复杂的资源共享架构，而底层的组件并不是为这些共享架构设计的，无法提供强有力的隔离保护，从而导致因组件交互复杂带来的数据隔离漏洞，对云平台安全性产生严重威胁。不安全的接口和API以及资源共享风险等成为云计算服务的重要威胁，由于云计算环境在设计时缺乏组件安全性、隐私性以及完整性的考虑，因此加强云计算环境内部组件之间的交互安全性、数据隐私性以及完整性的研究迫在眉睫。

2.2 数据的访问控制研究

访问控制能够通过对用户身份及其所属的预先定义的策略组限制其使用数据资源能力的手段，能够有效保证资源的保密性、完整性、可用性和合法使用性，是保证系统中不同角色能够安全交互、数据共享的关键策略之一。通过分析云环境中数据和信息的流向，以及各个实体的特点，然后对IaaS层各个实体采取不同访问控制策略，以提供分级的安全特性，能够为云环境的安全提供一种可行的控制策略[2]。但是当前的研究很少针对整个IaaS层组件进行细粒度的信息流和数据访问控制的研究，难以覆盖整个系统并提供相应的灵活的分层次安全策略，无法保证海量实体、组件间的交互安全。

3 数据保护技术(Data protection)

3.1 数据的访问控制技术

IaaS环境一般由众多独立的组件耦合形成，对外表现为单一服务整体，内部包含海量的交互协议以及交互接口，组件交互过程复杂性极大影响了IaaS环境的数据安全性，当前的研究主要是对云环境组件的交互工作从理论上进行论证分析

或者进行单个组件加强，无法从根本上改善云环境数据安全性不足的现状。由于数据资源的灵活性和共享性，安全数据流访问控制成为对外服务的最基本和最核心的要求。基于云环境数据流组件松耦合化，表现出适用于云环境具有时态特性的安全数据流控制模型，该模型结合已有访问控制模型，将数据管控模块作为组件交互的中转节点，对组件交互行为进行决策与放行，实现信息的可控管理；将数据访问主客体抽象成受控节点，实现耦合组件数据访问的动态授权，进而为IaaS层系统提供多层次灵活安全策略，最终提高云环境IaaS层的整体安全性[3]。同时建立组件数据交互状态验证系统，将验证属性与组件交互行为相结合。验证属性为组件信息流在控制策略的支持下完成相应组件交互的能力，提供相应的验证算法，对相应的策略进行输出，实现了对访问控制策略有效性的验证。从组件松耦合后访问控制的动态最小授权角度出发，实现细粒度模型下的信息流向管理，进而为IaaS层系统提供多层次的灵活安全策略，最终提高云环境IaaS层的整体安全性。如图1所示为云环境数据流管控模型。

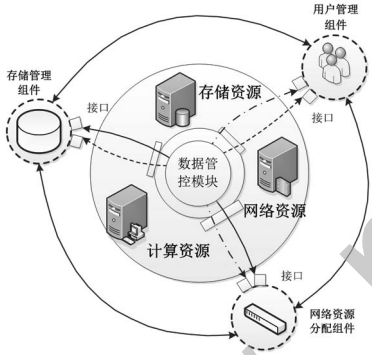

图1 云环境数据流管控模型

Fig.1 The model of data flow control based on cloud computing

3.1.1 具有时态特性的安全数据流控制模型

IaaS云平台外部包括数量庞大的用户，内部包含海量的控制、计算与存储实体，这些实体之间彼此互相关联，依存度极高。实体访问组件之间信息流的复杂程度取决于软件内部结构各子系统之间的组件耦合与信息控制流的复杂程度，它包括算法复杂度和结构复杂度[4]。本研究将以组件交互上下文为基础，把IaaS环境组件抽象成受控节点，将访问组件之间的依赖关系抽象成数据流在组件间的流向关系，从而建立松耦合下的细粒度访问控制。在松散耦合基础上从信息流上下文、组件访问依赖集合和组件访问有效期三个方面，提出具有时态特性基于信息流和组件角色的安全访问控制模型，解决组件安全交互控制问题。

3.1.2 多层次安全数据访问控制模型设计

首先对现有IaaS环境的访问数据流控制策略进行分析，针对Iaas安全访问约束规则形式化的描述，结合租户对IaaS组件安全访问的目标查找现有访问控制策略的缺陷。分析松耦合下IaaS环境在信息流控制方面存在以下问题：Iaas内部约束组件集合的动态变迁造成其安全访问管理复杂，受限客体访问主体的流动性较大，访问权限的定义模糊，无法满足最小授权原则以及访问权限的动态变更。分析完成后，本研究采用基于迭代的设计方法和基于组合的设计方法对松耦合IaaS安全访问控制模型进行设计和验证。

3.2 基于安全隔离架构的数据流控制模型

为构造安全的IaaS云环境，实现对数据的细粒度隔离，保证共享数据的细粒度管控，本研究基于安全隔离架构，依据组件监控模块的行为安全评估结果，根据当前环境构造的控制策略，设计数据流控制模型，实现组件数据交互安全可控。

由于一个可靠的数据流控制模型必须保证安全属性配置和交互端口改动尽可能适应系统运行的动态需求，本研究借鉴进程构造的方法，建立具有时态逻辑的数据访问传递机制，将数据管控模块作为连接隔离组件端口和访问基础设施服务资源的中转接点，对访问主体与客体的交互数据进行安全属性分析，划分数据安全等级，依据数据流安全控制策略，匹配组件访问的约束规则；对访问系统资源的请求进行内容过滤，保证访问系统数据的安全，并根据安全策略设计算法进行验证分析，实现对组件间数据流的统一管控，确保数据流向的安全。同时，为了精简模块规模，提高系统的灵活性和性能。本研究集成了数据管控仲裁模块和数据管控执行模块，实现任务并行操作，提高系统效率，如图2所示。

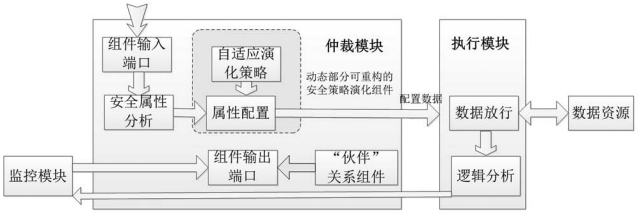

图2 动态自演化数据流管控

Fig.2 The dynamic and self-evolution data flow control

构建具备安全隔离环境的云IaaS层实验验证系统。综合上述方法，构建举报IaaS层安全环境方法的实验验证系统[5]。以现有IaaS层面的安全威胁为威胁模型，以现有代表性IaaS层系统为平台，首先为其进行安全架构改进，在此基础上，部署主动安全防护方法，从而构建IaaS底层安全环境的实验验证

系统，并通过实际使用和攻击测试，验证其安全隔离能力。

4 结论(Conclusion)

本文立足于松散耦合架构，借鉴进程构造的方法，引入组件行为状态变迁机制，将组件包实时划分成授权组件依赖集，集成IaaS环境组件访问集合，提高IaaS环境构件信息流控制的抽象级别和粒度；根据组件交互依赖闭包的形式规约，给出复合访问集合和复合访问接口的约束规则[6]；根据约束规则，实现组件交互时权限匹配仲裁，指导和规范IaaS环境组件安全访问控制；最终根据访问控制安全属性，提出具有时态特性基于信息流和组件角色的安全访问控制模型，解决组件安全交互控制问题。

参考文献(References)

[1] 李彤.论大数据时代网络隐私权的保护[D].河北大学,2014.

[2] 卜浩然.云环境下教育大数据安全策略研究[D].首都师范大学,2014.

[3] 刘玲.支持隐私保护的角色访问控制模型研究[D].湖南大学,2011.

[4] 于欣.云计算中的访问控制技术研究[D].西安电子科技大学,2013.

[5] 李阳.云计算中数据访问控制方法的研究[D].南京邮电大学,2013.

[6] 李文雪.云计算平台的访问控制评测技术研究[D].哈尔滨工业大学,2013.

作者简介：

张玉琴(1980−)，女，硕士，讲师.研究领域：计算机科学与技术.

(上接第26页)

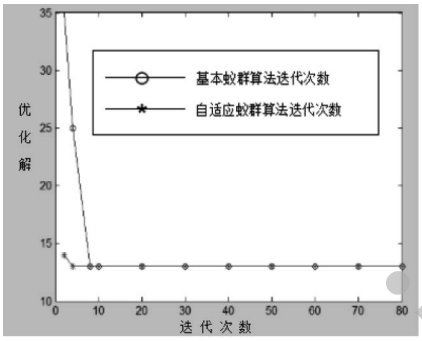

图4 自适应蚁群算法和基本蚁群算法迭代次数的对比

Fig.4 The number of iterations from the comparison of adaptive ant colony algorithm and basic ant colony algorithm

5 结论(Conclusion)

针对基本蚁群算法收敛速度慢，运算量大，陷入局部最优的缺陷，本文提出一种自适应蚁群算法，使其随着全局最优解的变化而适当的改变视野范围的值。实验结果表明，改进的自适应蚁群算法在收敛速度、迭代次数、计算量，寻优精度均优于基本型蚁群算法，适用于在急救车辆调度过程中实现最优路径的规划，为急救车选择最优路径到达患者位置提供了有利依据。

参考文献(References)

[1] 杨丽锦.浅析蚁群算法的原理及应用方向[J].电脑知识与技术,2009(6):12−14.

[2] 杨琼.具有感知觉特征的蚁群算法在连续函数优化中的应用[D].四川师范大学,2009.

[3] 马宪民,刘妮.自适应视野的人工鱼群算法求解最短路径问题[J].通信学报,2014(1):16−17.

[4] 蒋艳玲,张军.蚁群算法的参数分析[J].计算机工程与应用,2007(20):34−35.

[5] 王晔,吴晓军.基于改进人工蚁群算法的RBF网络及其在人脸表情识别中的应用[J].计算机应用研究,2008(9):28−30.

作者简介：

周桂宇(1986−)，女，硕士，助教.研究领域：网络环境下智能信息处理与自动化数据采集.

张 桐(1980−)，男，硕士，讲师.研究领域：现代物流装备及自动化.