数字海洋云计算平台工作流安全机制

阮进勇,徐凌宇,丁广太
(上海大学 计算机学院,上海 200444)

摘 要:云计算技术业已成为计算机资源交付使用的一种越来越受关注的方式。随着云计算技术的发展,其安全问题也面临巨大挑战。工作流管理系统是“数字海洋云计算平台”的重要组成部分,其中,资源鉴权和用户身份认证贯穿于工作流管理系统所有过程。文中研究数字海洋云平台上用户管理和定制复合模型工作流过程中的安全问题。根据数字海洋云平台上用户定制服务流时使用公有、私有资源安全问题和用户身份认证等功能,提出了一种工作流安全机制,结合手机和电子邮箱的双因素口令技术。

关键词:数字海洋云平台;身份认证;双元素技术;工作流
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2015)01-0155-04
doi:10.3969/j.issn.1673-629X.2015.01.035

Security Mechanism of Workflow on Cloud Computing Platform of Digital Ocean

NGUYEN Tien-dung, XU Ling-yu, DING Guang-tai
(School of Computer, Shanghai University, Shanghai 200444, China)

Abstract: In recent years, cloud computing technology has attracted much attention of various applications. Along with its development, cloud computing faces enormous challenges in security. Workflow management system is an important part of "cloud computing platform of the Digital Ocean of China". The functions of resource authentication and user identity authentication have played an important role in whole process of workflow management system. In this paper, study the security problem in the processing of user management and custom compound model on ocean cloud platforms. According to the security problem when users customize service flow with public and private resources on digital ocean cloud platforms and user identity authentication function, a workflow security mechanism, combined the technology of double factors of mobile phone and email, is proposed.

Key words: digital ocean cloud platform; identity authentication; double factor technology; workflow

1 概 述

当前,云计算技术业已成为计算机资源交付使用的一种越来越受关注的方式。云计算平台是一种功能可动态扩展的虚拟化计算环境,具有计算资源部署的灵活性和资源访问的低成本优势,然而,与传统数据业务系统类似,资源和系统的安全问题也是影响云计算普及和应用的关键问题之一。

云计算安全问题是多方面的,一方面,计算和数据资源的虚拟化对信息安全提出了新的要求;另一方面,云计算改变了网络应用模式,传统的安全产品无法满足新的环境要求[1]。云计算所面临的安全问题主要体现在如下几个方面:身份认证与权限控制、Web 安全防护和虚拟化安全等[2-3]。

因为用户通过网络将资源访问请求传输到“云”中,所以云计算应用的安全问题实质上涉及网络体系的安全性,但是又不同于传统网络,云计算应用引发了一系列新的安全问题。从服务层次来看,主要涉及终端用户云应用安全和云端的安全、IaaS 安全、PaaS 安全、SaaS 安全和虚拟化安全等[4]。

RSA 安全专家认为:目前,云计算环境下,用户对计算资源的控制程度大大降低,随着云计算的发展,海量的访问认证越来越复杂,身份认证技术模式需要变革和不断发展。从用户身份认证、资源鉴权、数据保密

收稿日期:2014-02-08 **修回日期**:2014-05-13 **网络出版时间**:2014-11-17
基金项目:国家科技部“十二五”规划项目(201105033-5)
作者简介:阮进勇(1985-),男,硕士研究生,研究方向为信息安全;徐凌宇,博士,教授,研究方向为信息融合、信息共享平台等;丁广太,博士,副教授,研究方向为图像处理与信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20141117.2205.020.html

性和完整性,以及数字签名的不可否认性等网络信息安全的五个要素来看,现代身份认证技术是网络信息安全的基础,静态口令仍然是目前最普遍使用的身份认证方式。然而,静态口令存在易于忘记、易于破解、难于管理、容易被第三方技术支持人员掌握等安全隐患。云计算的应用和网络技术是不可分开的,云计算的发展使得系统信息安全的隐患越来越大,简单的静态口令越来越不适合在云环境中的身份认证需求。

文中的研究是基于“数字海洋局云计算平台”课题。该课题中云资源的使用和管理涉及到资源鉴权和用户身份认证等功能,其中,资源鉴权和用户身份认证贯穿于工作流管理系统中。

1.1 数字海洋局云计算平台

数字海洋云计算平台研究的目的是:在参考国际主流云计算平台的基础上,结合中国海洋环境信息及产品的特点,研究并构建海洋环境信息云计算与云服务的体系架构。其主要功能如下:突破云环境下长时间序列海量海洋环境数据的快速并行检索,海洋环境信息远程并行可视化,基于语义的海洋环境信息分布式组织与管理,资源协调调度,分布式模型协同服务等多项关键技术等。制定一系列符合海洋环境信息特点的云计算与云服务标准规范,在基础框架下,利用“数字海洋”软硬件基础设施和信息服务体系,建立海洋环境信息云计算与云服务原型实用系统平台。

图 1 为数字海洋云平台结构。

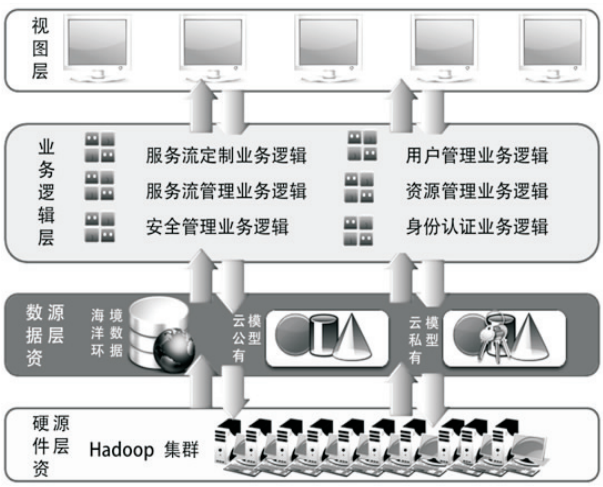

图 1 数字海洋云平台结构

在数字海洋云平台环境中,存在数据、计算模型、虚拟机等类型的资源。有效管理和监控各类资源和用户状态,为资源使用者提供一个统一的云计算平台,确保资源的安全和用户的隐私是数字海洋云平台必须考虑的问题。

1.2 数字海洋云平台中工作流的安全问题

随着云计算技术的迅猛发展,基于预定的工作流管理系统也在发展。工作流定制是数字海洋云计算平台中的主要内容之一。工作流的基本安全问题包括认证、授权、访问控制、审计、数据保密性和数据完整性等等。

在数字海洋云计算平台中,用户可以通过可视化建模方式定制复合模型工作流,把多个模型有机地组合成一个模型组,其复杂的处理过程由云平台自动执行完成,并将最终结果返回给用户。数字海洋云计算平台中模型工作流的主要功能为:

a. 用户可定制复合模型工作流的服务模式:包括用户定制方法、执行流程、与用户的交互方式等。

b. 可定制复合模型建模语言:用来描述复合模型中的模型工作流以及工作流内各模型间的关系。

c. 用户接口规范:模型提供者面向用户提供服务的标准接口,确保用户清晰了解模型的功能、输入、输出接口,方便准确地使用模型。

d. 模型、数据接口规范:研究如何发现和组织模型,模型间的互连及参数匹配,解决多模型的对接问题,能够实现用户私有模型与云公有模型的混合模型工作流,乃至用户私有数据与云公有数据及各类模型的混合使用。

e. 工作流的定制、解析和引擎的实现:工作流以模型为节点定制完成某项任务的工作流。

图 2 为工作流示意图。

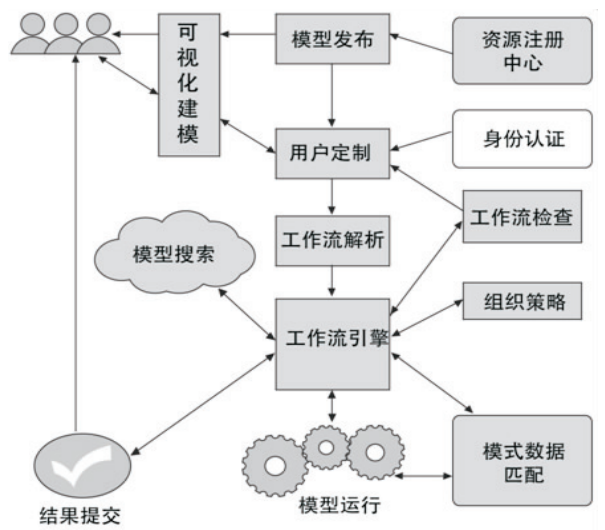

图 2 工作流示意图

在数字海洋云计算平台中,需要存储公有和私有资源,用户在定制服务流的过程中,面临的安全问题如下所述。

(1)用户通过权限控制,使用公有和私有资源定制服务流。

(2)用户通过权限控制,使用公有和私有服务流。

(3)用户下载自己提交的服务流的运行结果。

以上安全问题是数字海洋云计算平台应该考虑和解决的。

2　工作流安全机制

2.1　身份认证技术

云计算是传统计算机与网络技术发展的融合产物。随着并行计算、分布式计算、网格计算的发展,云计算这种新型的计算模式逐渐进入网络计算领域. 身份认证技术是为了在计算机网络中确认操作者身份而产生的。用户身份认证一般遵从三种基本方法:验证用户生理特征,验证用户是否拥有物理介质式的令牌和验证用户是否知道某个密码[5-7]。

云计算系统的基本安全需求是:建立统一、集中的认证和鉴权系统,以满足云计算多用户环境下复杂的用户权限管理策略和海量访问认证要求,提高云计算系统身份管理和认证的安全性[8-11]。基于密码的身份认证技术是最基础的一种身份认证技术。与静态口令相对应的强身份认证技术,包括:生物认证技术、数字证书认证技术、动态口令(One-Time Password,OTP)认证技术、智能卡身份认证技术、短信(手机)认证、电子邮件认证和多因素风险身份认证等[12-15]。文中根据数字海洋云平台上用户定制服务流时使用公有和私有资源的安全问题,提出了一种结合短信和电子邮件的双因素口令技术。

2.2　工作流系统中身份认证

数字海洋云平台中,用户可定制符合模型工作流服务模式、复合模型建模语言等。用户访问的数据在数字海洋云计算平台中都是以公有和私有资源的形式存放的。用户如何访问公有和私有资源定制服务流,以及得到服务流的运行结果,并且确保公有和私有资源的完整性和安全性,是工作流中的主要安全问题。海洋数据计算中身份认证的模型如图 3 所示。文中提出的解决方案如下所述。

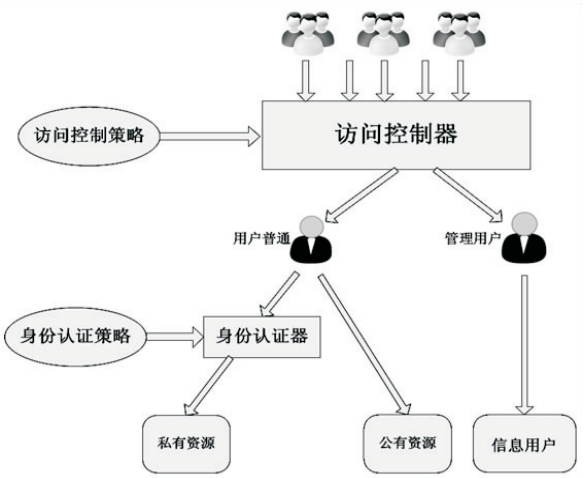

图 3　海洋数据计算中身份认证的模型

首先,用户注册成为普通用户,在登录数字海洋云平台之后,定制服务流之前,通过手机和电子邮件得到一对密码。云平台身份认证服务器通过这对密码确认用户的身份,进而容许或拒绝用户的工作流定制过程的启动。

其次,在工作流定制过程中,如果用户所提交的服务流需要访问私有资源,则进一步核实用户身份和资源访问权限,以防止非法用户访问私有的资源。在数字海洋云计算平台中,通过身份认证服务器鉴定使用私有资源的用户是否合法。

与用户登录数字海洋云平台类似,当用户定制是服务流需要访问私有的资源时,系统要求用户进行身份认证。此时,认证服务器发送两个密码到用户手机和电子邮件。用户拿到两个密码之后,将密码提交到验证服务器进行比对验证。如果身份认证通过,则用户可以使用私有的资源;如果身份认证失败,则身份认证器最多允许身份认证连续失败 5 次,超过 5 次身份认证的功能暂停 10 分钟。身份认证过程如图 4 所示,实现过程描述如下:

第一步:用户发送一个请求,要求访问私有资源。

第二步:认证服务器发送密码到用户手机和电子邮件。

第三步:用户得到密码。

第四步:用户提交密码。

第五步:认证服务器对比密码和分析密码提交者的机器特征,并返回结果(允许用户访问或停止用户访问)。

身份认证服务器发送两个密码时,身份认证服务器还使用倒计时函数,如果超时 10 分钟,则两个密码失效,系统对私有资源自动保密。

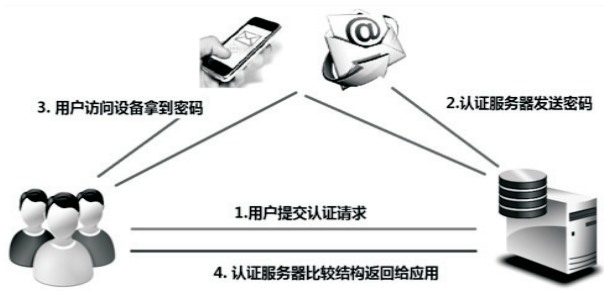

图 4　身份认证的机制

如图 5 所示,用户发送一个使用私有资源的请求,身份服务器立刻生成 2 个密码发送到客户手机和电子邮件,这个过程的伪代码如下所示:

```
Procedure generate(pass) //发送密码
Key1:String(6); //密码 1;
Key2:String(6); //密码 2;
if Access() then //用户要使用私有资源;
Key1=Random();
Key2=random(); //身份认证服务器通过随机函数生成 2 个密码;
Transfer1(Key1); //身份服务器通过短信发 Key1 到手机号
```

码的用户;

Transfer$_2$(Key$_2$) ; //身份认证器通过网络发 Key$_2$到电子邮件的用户;

CountTime(time); //身份认证器通过倒计时的函数,Key$_1$,Key$_2$有效;

end if

end procedure

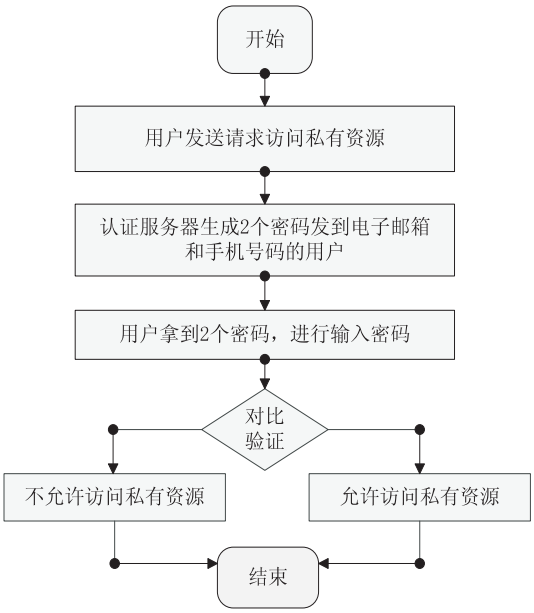

图 5 数字海洋云平台中身份认证模型

之后,用户在手机上和电子邮件里,得到密码,然后提交这两个密码给身份认证服务器,身份认证服务器进行密码比对,此过程伪代码如下:

Procedure Authentication( ) //身份认证

Mess:String(6) //短信的密码

Mail:String(6)//电子邮件的密码

shu=1;

while(shu<=5) do

if(mess=Key$_1$)和(Mail=Key$_2$)then

Access(user)=true; //允许用户可能用他们的资源;

else Access(user)=false; //不允许用户进入使用私有的资源;

shu=shu+1;

end if

end while

while (shu>5) do

CountTime(time); //使用倒时间的函数暂时停止用户的身份认证功能;

end while

Shu=0;

end procedure

身份认证机制使得用户可以在定制工作流混合使用私有资源和公有资源的过程中,保证私有资源的安全性,用户可以放心地在数字海洋云平台上存储他们的私有资源。同时,通过结合使用短信和电子邮件,提高资源的安全性。在不使用动态口令的情况下,仍能保证安全级别。

使用手机和电子邮件成本低廉,而且安全级别较高。但是,此身份认证机制可能碰到的问题是:用户注册、登录和验证时,手机和邮箱通讯不畅,以及密码盗用。为了克服这个问题,用户在注册、登录和验证时,需要进行短信和电子邮件的回复验证,通过回复信息的分析,保证注册的手机和邮箱与用户身份相对应。回复信息的精细分析是文中遗留的研究内容之一。

认证服务器发送密码机制如图 6 所示。

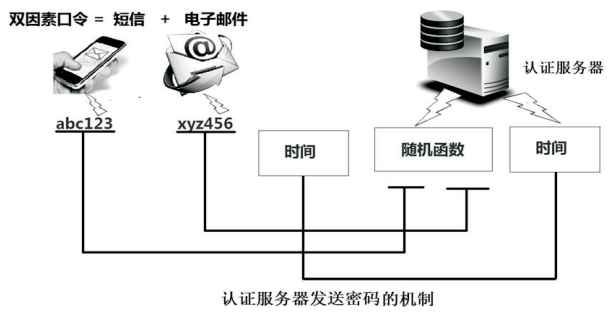

图 6 认证服务器发送密码机制

3 分析与评价

目前,许多网上应用服务提供商使用动态时间令牌的机制,通过动态口令产生一组数字作为登录密码,访问私有资源,特别是有些银行系统已经应用这个技术。此技术的不足之处是:容易产生丢失、转借、硬件显示不清、时间不能同步和电源电量不足等问题,有的还要求用户把动态口令卡带在身上。如果在数字海洋云平台中简单地使用动态口令技术,将会给用户的使用带来不便。用户希望使用一种更便利的方式来定制工作流中要使用的私有资源。文中提出的结合手机和电子邮箱的双因素身份认证技术能满足要求。

4 结束语

文中研究数字海洋云平台上用户管理和定制复合模型工作流过程中的安全问题。根据数字海洋云平台上用户定制服务流时使用公有和私有资源的安全问题,提出了一种结合手机和电子邮箱的双因素口令技术。此方法应用在数字海洋云平台进一步提高了用户在定制服务流的过程中资源使用的安全性,并且此方法运行成本低廉。用户注册、登录和验证时,通过手机和邮箱回复信息的精细分析进行身份验证是一个更加经济和有效的方法。

参考文献:

[1] 王伟兵. 一种基于云计算的动态可扩展应用模型[J]. 计算

(下转第 182 页)

5 结束语

三网融合技术和云计算给区域数字图书馆带来了新的服务理念,同时也带给了用户更加贴心的服务。用户在融合网络中可以随时随地通过各种终端获取区域云数字图书馆提供的服务。文中主要研究了三网融合环境下区域数字图书馆云服务框架模型。对这些框架模型的研究有助于区域数字图书馆提高用户服务水平并且降低区域数字图书馆本身的运营成本。当然,这种服务框架模型还存在很多不成熟的地方,但是随着相关研究的不断完善,相信在未来一定能建设出让用户满意的区域云数字图书馆。

参考文献:

[1] 2010 年政府工作报告[R/OL]. 2013-12-02. http://news.xinhuanet.com/fortune/2010-01/14/content_12805982.htm.

[2] Federal cloud computing strategy[EB/OL]. 2013-12-02. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909616.

[3] 孙培燕,张玉梅. 云计算技术在图书馆中的应用[J]. 情报科学,2011,29(4):552-554.

[4] 胡开胜,唐国华. 基于云计算理念的区域数字图书馆平台建设研究[J]. 图书情报工作网刊,2011(7):17-22.

[5] 李文文,陈 雅. "三网融合"背景下的数字图书馆建设[J]. 情报资料工作,2011(4):90-92.

[6] 支小莉,廖文昭,蔡立志,等. 面向互联网应用的云操作系统的架构设计[J]. 上海大学学报(自然科学版),2013,19(1):44-48.

[7] 李 倩. 跨库检索工具分析及在图书馆的应用[J]. 现代情报,2011,31(10):91-94.

[8] 白如江. 粗糙集理论在跨库检索系统中的应用[J]. 图书情报工作,2005,49(10):41-44.

[9] 王政军,金玉玲. 虚拟化技术在数字图书馆中的应用[J]. 现代情报,2010,30(10):77-80.

[10] 张龙昌,沈德海,王晓明,等. 移动社会网络关键技术[M]. 沈阳:东北大学出版社,2012.

[11] Back G,Bailey A. Web services and Widgets for library information systems[J]. Information Technology and Libraries,2010,29(2):76-86.

[12] 陈 臣,马晓亭. 云计算环境下数字图书馆云服务平台与云服务模式研究[J]. 情报资料工作,2012(4):42-45.

[13] 张 鼐. 一种基于语义 Web 的数字图书馆模型研究[J]. 图书馆学研究,2011(9):34-37.

[14] 李玮娴. Widget 在公共图书馆社区信息服务的应用探讨[J]. 图书馆学研究,2010(6):60-62.

[15] 吴志强,王义翠,马慧娟. 协同信息推荐:一种数字图书馆个性化信息服务新模式[J]. 图书馆,2011(1):45-47.

[16] 潘旭伟,李泽彪,祝锡永,等. 自适应个性化信息服务:基于情境感知和本体的方法[J]. 中国图书馆学报,2009(6):41-48.

[17] 卢培文,赵 荣,朱宗霞,等. 基于 Widget 的个性化图书馆服务[J]. 图书情报工作,2009(S1):71-73.

[18] 陶 强,刘宴兵,肖云鹏. 面向多终端异构系统的中间件平台体系结构研究[J]. 计算机工程与设计,2012,33(4):1431-1436.

(上接第 158 页)

机工程与应用,2011,47(15):15-18.

[2] 陈丹伟,黄秀丽,任勋益. 云计算及安全分析[J]. 计算机技术与发展,2010,20(2):99-102.

[3] 郭春梅,毕学尧,杨 帆. 云计算安全技术研究与趋势[J]. 信息网络安全,2010(4):16-17.

[4] 彭易杭,王粉梅,史娟荣. 云计算应用在炮兵信息系统中的安全性研究[J]. 考试周刊,2011(34):157-159.

[5] 周晓斌,许 勇,张 凌. 一种开放式 PKI 身份认证模型的研究[J]. 国防科技大学学报,2013,35(1):169-174.

[6] 孙韩林,刘建华. 公众网络统一身份认证服务及标准研究[J]. 电信科学,2012,29(2):84-88.

[7] Security and high availability in cloud computing environments[M]. [s.l.]:IBM,2011.

[8] 李晓飞. 云计算环境下的用户隐私问题浅析[J]. 南昌教育学院学报,2013,28(2):194-194.

[9] 李红霞. 云计算中身份认证与访问控制管理系统的实现策略研究[D]. 北京:北京邮电大学,2011.

[10] 余幸杰,高 能,江伟玉. 云计算中的身份认证技术研究[J]. 信息网络安全,2012(8):71-74.

[11] 周楝淞,杨 洁,谭平嶂,等. 身份认证技术及其发展趋势[J]. 通信技术,2009(10):183-185.

[12] 邓 婧. 基于 OTP 技术的网上银行安全身份认证应用研究[D]. 北京:对外经济贸易大学,2006.

[13] 李 歆,管党根. 数字证书认证技术在资料库等系统中的应用[J]. 人民长江,2009,40(4):74-76.

[14] 刘林东,邬依林. 基于云计算的 USBKey 身份认证技术研究[J]. 广东第二师范学院学报,2011,31(5):78-84.

[15] 张立斌,高仲春,张 晶. 云计算环境下统一身份认证平台的设计与实现[J]. 工业控制计算机,2013,26(7):91-92.

数字海洋云计算平台工作流安全机制

作者： 阮进勇， 徐凌宇， 丁广太， NGUYEN Tien-dung， XU Ling-yu， DING Guang-tai
作者单位： 上海大学 计算机学院,上海,200444
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(1)