基于 RSA 算法的云资源管理平台授权机制①

尹雪蓉[1,2], 宋耀光[1], 倪 巍[1]

[1](华存数据信息技术有限公司, 上海 200127)
[2](上海交通大学 信息安全与工程学院, 上海 200240)

摘 要: 云计算平台提供商部署和实施云资源平台时, 需要对该平台软件的使用进行管理与控制. 针对云资源管理平台授权模式缺乏的现状, 在项目搭建云资源管理系统的过程中, 设计了一套基于 RSA 算法的平台软件授权机制. 实践证明该授权机制通过对平台底层云资源合法有效的监督与控制, 从而解决云资源管理平台软件的授权问题, 并可作为云资源管理平台授权的解决方案进行推广.

关键词: 云计算; RSA 算法; 授权机制; 云资源管理平台; ICT

Authorization Mechanism for Cloud Computing Resource Management Platform Based on RSA Algorithm

YIN Xue-Rong[1,2], SONG Yao-Guang[1], NI Wei[1]

[1](ECData Information Technology Co.Ltd., Shanghai 200127, China)
[2](Shanghai Jiaotong University, SJTU, Shanghai 200240, China)

Abstract: When deploying and implementing a cloud platform, it is necessary for vendors to manage and control their software of the cloud platform. To solve the problem that currently there is few authorization model in cloud platform software management and control, we propose and design a mechanism for cloud platform software authorization based on RSA algorithm within the progress of building the cloud management system of a real project. The practice has proved that the authorization mechanism in this paper, by monitoring and manipulating the validity of underlayer resource in the platform, is effective to manage and control the cloud platform software usage, which can be generalized for cloud platform software authorization in many other cases.

Key words: cloud computing; RSA algorithm; authorization mechanism; cloud resource management platform; information communication technology

云计算技术是IT产业界的一场技术革命, 它的出现改变了用户对 ICT[1](Information Communication Technology 即, 信息通讯技术)资源的获取方式, 使其从购买产品独立构建 ICT 设施转为寻求社会化公共服务.

云计算创造了新的业务提供方式和商业模式, 形成了云计算制造业、基础设施服务业、云计算服务业为下中上游的云计算产业链[2]. 在其中, 代表云计算服务业的云计算服务商是该产业链的主导力量. 而云计算平台提供商通过协助云计算服务商搭建云资源管理平台向用户提供云计算资源, 满足和引领用户需求, 从而推动 IT 产业的发展.

然而对云平台提供商来说, 虽然实现了按需使用、弹性伸缩、安全可靠的云资源平台, 但是由于云资源平台在实际运营过程中, 云平台提供商与云平台运营方相分离, 云平台提供商无法对云资源平台的使用作具体管理和控制. 本文设计的授权机制是在建设云资源平台项目中, 对传统云资源管理平台进行改造, 通过区分平台底层云资源合法有效性来控制云资源管理平台的管理边界, 从而解决云资源管理平台的授权

① 基金项目:华云云计算产品与技术及应用示范服务中心建设项目(发改办高技[2011]2448 号文件)
收稿时间:2013-11-12;收到修改稿时间:2013-12-16

问题. 该授权机制对云模式下平台提供商与运营商的分成模式完善具有积极、重要的意义, 并能在日益增多的云计算项目中进行广泛推广.

1 云资源平台概述

在云计算环境下, 虚拟化实现了底层物理设备与上层操作系统、应用软件的解耦, 而云资源管理平台提供了一个可管、可控、可运营的服务提供环境, 使云计算服务提供商可以方便地将基础云资源以服务的方式提供给用户, 从而实现自动化部署调度与运维管理.

本文的授权机制基于具有一定通用性的云资源平台架构, 该平台架构主要由包含三个部分: 云资源、云资源管理平台以及门户, 如图 1 所示.

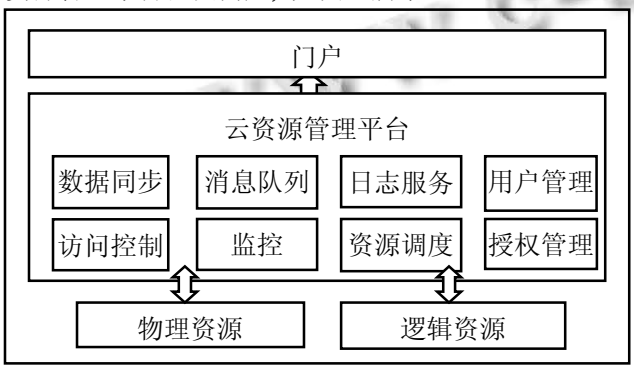

图 1 云资源平台架构

(1) 云资源: 主要包括物理资源和逻辑资源. 物理资源主要有服务器、存储体、网络系统硬件组成, 逻辑资源包括了计算、存储、网络、应用等综合软件资源构成;

(2) 云资源管理平台: 主要具有两大功能: 首先其对下提供对各种云资源的统一管理、监控、部署调度; 同时向上将抽象出各类逻辑资源通过服务交付的方式提供给不同类型的用户.

云资源管理平台主要由以下模块组成: 数据同步、消息队列、日志服务、用户管理、访问控制、监控、资源调度、授权管理.

其中授权管理模块主要负责管理物理资源与逻辑资源的授权状态, 只有合法授权的资源才能被平台管理.

(3) 门户主要对用户提供了简单、易用的自助式 Web 服务界面. 主要有管理门户和用户门户两类.

2 授权机制与关键技术

授权机制[3]体现授权管理模块对物理资源与逻辑资源以及使用人的授权管理, 只有当云资源使用人对调用的物理资源与逻辑资源被确认合法授权, 资源才能被平台管理与被使用.

物理资源与逻辑资源合法授权的确认就是用户对云资源管理平台内资源调用时, 授权管理模块对用户调用资源的合法性进行鉴定, 它是通过输入特别的信息密码的方式, 由授权管理模块进行鉴定, 如果调用的资源是合法的资源, 授权管理模块就允许云资源管理平台对该资源进行管理与调用, 否则将不允许平台调用和管理该资源. 鉴定云资源合法性的过程就是授权机制的关键技术, 以下是授权机制所需的技术要素:

(1) RSA 非对称加密算法: 非对称加密算法[4], 也叫公开密钥算法, 是使用两把完全不同但又是完全匹配的一对密钥——公钥和私钥. 在使用公开密钥算法加密算法的过程中, 使用公钥加密的密文由私钥解密后得到的明文与原文相同. RSA[5]是公开密钥算法的一种具体实现, 它的安全性基于大数分解难题.

(2) 单向散列函数: 单向散列函数又称单向 Hash 函数[6]、杂凑函数, 是把任意长的输入消息串变化成固定长的输出串且由输出串难以得到输入串的一种函数. 这个输出串称为该消息的散列值. 一般用于产生消息摘要, 密钥加密等.

(3) 数字签名技术: 数字签名[7]是以电子形式存在于数据信息之中的, 作为其附件的或逻辑上与之有联系的数据, 可用于辨别数据签署人的身份, 并表明签署人对数据信息中包含的信息的认可.

3 具体方案设计

3.1 基于 RSA 算法的资源授权技术

(1) 授权机制技术内涵

在云资源平台搭建和运营的过程中, 云平台提供商与云平台运营相互分离, 云资源管理平台软件一般在云平台运营方生产环境下运行, 平台提供商无法时刻监督资源平台的使用情况, 尤其在云计算虚拟化环境下, 部署于虚拟机中的云资源管理平台软件很容易被克隆滥用. 虽然平台提供商无法防止云资源管理平台软件被复制滥用, 但是由于云资源管理平台管理的资源实体在云场景下必须有唯一标识以便云资源管理平台能够准确对其进行统一管理与调度, 由此平台提

供商可以通过对云资源管理平台底层的资源实体合法性的认定来确定云资源管理平台的管理边界并进行控制. 本文授权机制技术内涵便是通过对平台被管实体的合法性控制来确立平台软件的管理权限, 从而达到对平台软件使用进行授权的目的.

(2) RSA 算法资源授权技术设计思想

在云场景下, 资源和平台皆运行在运营方处, 因此在对资源进行授权时, 需要基于资源的唯一标识生成相应授权许可证.

授权许可证使用序列号机制[8]进行授权与加密, 序列号机制就是设计用户信息与注册码之间的数学映射关系. 一般来说, 映射关系越复杂, 注册码就越不容易被破解, 因此数学算法是序列号机制的核心.

本文设计的云资源管理平台授权机制, 在引入序列号授权机制的基础上, 结合非对称公钥算法 RSA 算法实现对管理平台下的云资源[9]进行合法性验证, 利用其大因数分解不可逆的特性, 增加序列号生成的复杂度, 从而加强其安全性.

3.2 模块设计与实现

对云计算环境下的应用场景进行分析后, 本文场景中主要有三个主要实体: 平台提供商、平台运营商以及资源管理平台.

(1)平台提供商搭建提供资源管理平台, 并将该平台交由平台运营商运营.

(2)平台运营商负责使用资源管理平台对底层云资源进行统一管理.

(3)资源管理平台由平台运营商管理.

该机制主要分为以下几个模块: 授权许可证生成与分发、资源注册、资源授权验证.

3.2.1 授权许可证生成与分发模块

该授权机制下授权许可证生成与分发模块[10]如图 2 所示.

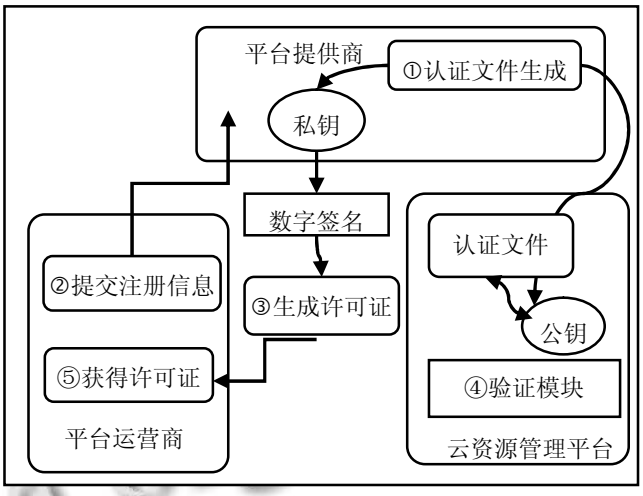

图 2 授权许可证生成与分发示意图

授权许可证生成与分发主要包括以下几个步骤:

(1)授权许可证的认证文件生成

首先在平台提供商处, 使用 RSA 算法生成一对密钥对, 该密钥对由私钥和公钥组成.

由于公钥将随云资源管理平台部署于平台运营方处, 为了防止公钥被篡改, 需要使用 MD5 算法对公钥生成摘要, 并进行混淆从而生成认证文件.

生成密钥对与认证文件后, 由平台提供商保留私钥, 并将公钥以及认证文件一同部署进资源管理平台中.

(2)资源注册信息提交

当平台运营商在实际运营云资源管理平台的过程中, 需要对权限范围之外的资源进行管理时, 需要先将所需管理的资源唯一标识提交给平台提供商进行注册. 注册信息主要包括资源类型、资源型号(生产公司、产品名、版本号)、资源的唯一标识、以及申请人等. 注册信息通过 XML 格式提交给云平台提供商, 格式信息如下所示:

```
<Registration>
    <Resource Type= “资源类型”>
        <Model name = “资源型号”>
            <Company>公司</Company>
            <Product>产品</Product>
            <Version>版本</Version>
        </Model>
    </Resource>
    <ResourceID>资源标识</ResourceID>
    <Applicant>资源申请人</Applicant>
</Registration>
```

(3)生成授权许可证

云平台提供商在收到云平台运营商提交的注册信息后, 根据运营商通过注册信息抽取并产生用于生成授权许可证的注册因子, 使用私钥对该注册因子进行数字签名从而产生一个与资源信息相关的序列号, 并使用该序列号生成授权许可证文件, 然后将许可证文件分发给平台运营商.

3.2.2 云资源注册时序图

当平台运营商获取到授权完毕的资源序列号之后，便可以使用该序列号在云资源管理平台下注册，注册成功的云资源可由该平台进行管理. 注册信息将记录在数据库中，以备查询控制等使用. 云资源管理平台对资源进行注册的时序图如图 3 所示.

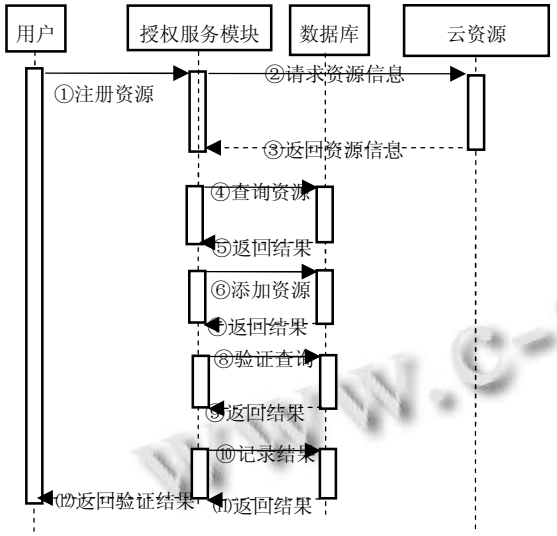

图 3　云资源注册时序图

在云资源管理平台注册云资源的过程中，主要的消息交互对象包括用户、授权服务模块、数据库、运资源. 其中用户代表云资源管理平台的使用者，他通过门户向授权服务模块发送请求；授权服务模块作为云资源管理平台软件系统中的组件，主要对上提供授权服务；数据库主要记录云资源管理平台所有在管对象的信息，为授权服务模块提供业务数据支撑；云资源是需要被授权的资源实体，它具有唯一标识. 具体交互过程如下所示:

(1)用户发送资源注册信息以及对应的序列号等注册请求给授权服务模块，授权服务模块先通过资源注册信息向云资源请求其唯一标识;

(2)在获取到其标识后，授权服务模块通过标识查询资源，如果查询到了该资源则说明该资源已被添加过，则退出注册添加流程. 否则便添加该资源，并进行授权认证.

(3)授权完成后记录其授权结果，并最终返回验证结果. 验证通过的云资源，可以被正常使用，否则系统将对其进行屏蔽.

3.2.3　云资源验证流程

云资源在注册后会在云资源管理平台的数据库中留下记录，在具体使用时，每当平台加载该云资源，平台将先对该云资源进行授权验证. 只有通过了验证的云资源才能成功加载，否则，该资源将被云资源管理平台屏蔽. 云资源验证过程如图 4 所示.

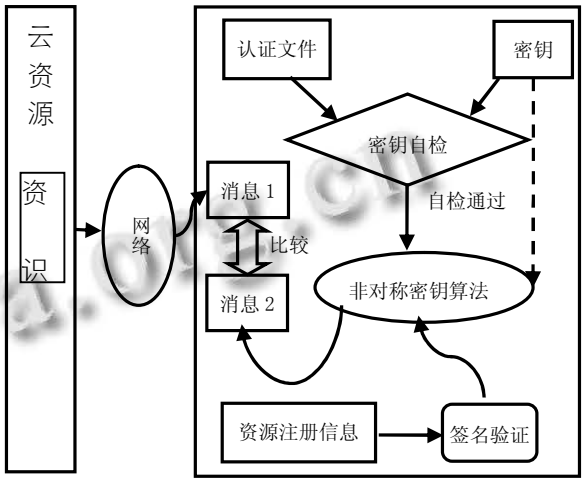

图 4　云资源验证示意图

该验证过程主要包括以下几个步骤:

(1)云资源在加载过程中，将其资源标识通过网络传输到云资源管理平台，保存为消息 1.

(2)云资源管理平台在接收到资源标识后，为防止平台密钥被篡改，先进行密钥自检，自检过程主要是通过密钥与密钥所产生的认证文件进行比对. 当两者比对通过则表示平台上的密钥真实有效.

(3)密钥自检后，资源平台从数据库里寻找该资源的注册信息，通过非对称密钥算法对注册信息进行签名验证，并将所得到的消息 2，通过比较消息 1 与消息 2 的值，当两条消息相同，则表示该资源为合法有效资源，则云资源管理平台正常对其请求进行操作管理. 否则，说明资源不合法，云资源管理平台将屏蔽其所有请求.

4　实验测试与分析

本资源平台授权机制主要由以下几个模块组成: 资源许可证认证文件生成、资源许可证分发、云资源验证、云资源注册. 为了验证本授权机制的合理性、可用性以及本授权机制对云资源管理平台安全性的加强. 本文以 IBM 服务器 Power 7R1 作为底层控制资源设计了如下实验进行测试:

4.1 测试实验配置与环境

实验所需硬软件设备配置如下表 1 所示:

表 1 测试软硬件设备配置表

设备名	数量	描述
IBM Power 7R1	2	作为底层云计算资源
V7000	1	作为共享存储用于搭建简易云资源平台
云资源平台软件	1	包含本文授权机制的云资源管理平台软件
普通 x86PC 机	2	一台用于部署云资源管理平台软件, 一台用于对资源进行授权
授权许可证生成与发布软件	1	用于对资源的授权许可证进行生成与发布

具体测试环境按照图 5 进行部署:

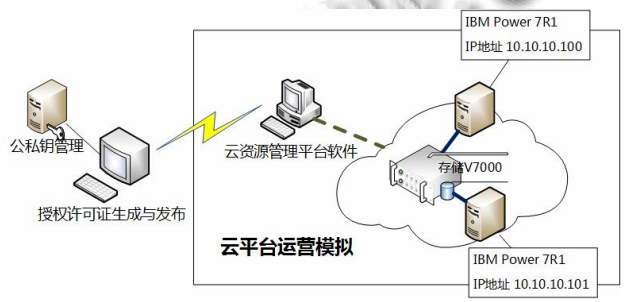

图 5 测试环境部署图

部署过程如下所示:

(1)将两台 IBM Power 服务器与存储 V7000 相连接, 配置 V7000 作为共享存储同时配置一台 Power 服务器 ip 地址为 10.10.10.100, 另一台为 10.10.10.101.

(2)在一台 x86 主机上部署云资源平台软件, 并配置主机网络使得该主机能够访问 10.10.10 网段.

(3)在另一台主机上部署授权许可证生成与发布软件, 配置主机网络使得它与云资源平台软件运行主机互相连通.

4.2 测试步骤

按照上述部署图部署完成后, 运行云资源管理平台软件, 此时管理平台中无任何计算资源.

测试步骤如下:

(1)在云资源管理平台, 进入 ip 地址为 10.10.10.100 的 Power 服务器控制台, 输入命令 “uname -uM” 可以得到该 Power 的硬件标识. 如下图 6 所示:

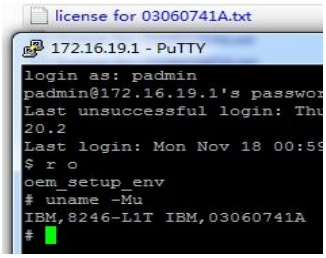

图 6 Power 硬件标识

(2)将获取的硬件标识提交给授权许可证分发软件进行注册

(3)在授权许可分发软件中, 输入硬件标识和与资源平台认证文件对应的私钥文件, 软件自动产生一个代表授权许可证的 TXT 文件. 如下图 7 所示:

图 7 授权许可证文件

(4)由授权许可分发软件将该授权许可证文件发送至云资源管理平台所在 pc 机上.

(5)在云资源管理平台软件上, 进入注册计算资源选项, 输入 ip 地址为 10.10.10.100 的服务器作为连接目标, 选择 “IBM Power 7R1”作为资源设备类型, 将授权许可证文件路径添加其中进行注册

(6)同样在云资源管理平台上, 进入注册计算资源选项, 输入 ip 地址 10.10.10.101 的服务器作为连接目标, 同样选择 “IBM Power 7R1”作为资源设备类型, 添加 10.10.10.00 主机的许可证文件进行注册

测试结果: 在步骤(5)中, 由于许可证文件与资源设备相匹配, 资源成功注册, 并能使用云资源管理平台进行日常管理维护, 而步骤(6)中, 由于设备与许可证不匹配, 资源注册失败. 该设备无法被管理与正常使用.

测试结果表明了在本文授权机制下, 底层云资源的合法性可由平台提供商来控制, 非法的云资源无法被平台加载管理, 该机制可以让云平台建设提供商更好地对其所建设的云平台管理对象进行合法性监管、监督和控制云资源平台管理软件的使用.

5 结论

本文从现阶段云计算发展过程中产生的云资源管理平台授权问题出发，结合传统软件授权机制中序列号授权机制与非对称公钥算法 RSA，实现了云资源管理平台资源合法性授权验证，该授权机制可以有效控制云资源管理平台中非法资源的泛滥，完善了云资源管理平台授权模式，保障了云平台提供商的经济利益，因此该机制在现有云资源管理平台授权问题中具有一定使用与推广价值.

参考文献

1 雷万云,等.信息化与信息管理实践之道.北京:清华大学出版社,2012.

2 中国电子信息产业发展研究院赛迪顾问股份有限公司.中国云计算产业发展及应用实践.北京:电子工业出版社,2012.

3 Rabiiti F, Bertino E, Kim W. A model of authorization for next-generation database systems. Journal ACM Tran. on Database Systems (TODS), 1991,16(1):88−131.

4 Schneier B, et al.应用密码学协议、算法与 C 源程序.北京:机械工业出版社,2007.

5 覃中平,张焕国,等.信息安全数学基础.北京:清华大学出版社,2006.

6 周晓斌,许勇,张凌,等.一种开放式 PKI 身份认证模型的研究.国防科技大学学报,2013,35(1):169−194.

7 Li X, Liu CX. The research of RSA-based undeniable signature method. Proc. of the 2012 Int. Conf. on Communication, Electronics and Automation Engineering. 2013, 181: 801-806.

8 段钢.加密与解密.第 2 版.北京:电子工业出版,2008.

9 Xu X. From cloud computing to cloud manufacturing. Robotics and Computer-Integrated Manufacturing, 2012, 28(1): 75−86.

10 Pinkas B, Sadeghi AR. Secure Computing in the Cloud. DAGSTUHL Reports, 2011, 1(12): 1−10.