云计算密钥管理架构研究与设计

谢立军，朱智强，孙　磊，潘　宁
（解放军信息工程大学，郑州 450004）

摘　要：针对目前云计算环境中尚缺乏一个完整的密钥管理方案，分析了云计算环境密钥管理的特殊安全需求，基于 XML 密钥管理规范建立了云计算密钥管理框架。设计了云计算密钥管理架构以及各部分模块功能，提出了基于信任域的工作模式，对系统进行了性能和安全性分析，并提出相应的解决方案。实验分析结果表明，该方案相对于传统 PKI 系统性能更高，能够更好地满足云计算密钥管理需求。

关键词：云计算；密钥管理；XML 密钥管理规范；信任域；模块设计
中图分类号：TP309.7　　**文献标志码**：A　　**文章编号**：1001-3695(2013)03-0909-04
doi:10.3969/j.issn.1001-3695.2013.03.069

Research and design of cloud computing key management framework

XIE Li-jun, ZHU Zhi-qiang, SUN Lei, PAN Ning
(*PLA Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: This paper analyzed the special security requirement of cloud computing key management, and built the cloud computing key management framework based on XKMS. At first, it designed the cloud computing key management architecture and modules. Then proposed the trust domain-based working pattern. At last, it analyzed the performance and security of the framework and proposed the corresponding solutions. The results show that it can meet the cloud computing key management needs well.

Key words: cloud computing; key management; XKMS; trust domain; module designing

云计算将大量计算资源、存储资源与软件资源链接在一起，形成巨大规模的共享虚拟 IT 资源池，为远程计算机用户提供“召之即来，挥之即去”且似乎“能力无限”的 IT 服务[1]。它具有超大规模、虚拟化、通用性等特点，同时为实现用户信息资产安全与隐私保护带来极大的冲击与挑战。密码技术是解决这一安全问题的有效方法之一，而密钥管理是密码技术的核心问题，因此密钥管理成为保障云计算安全的重要技术。

公钥基础设施 PKI(public key infrastructure)是传统公钥管理的主要方法之一。它的核心组成是 CA(certificate authority)，通过为用户公钥签发公钥证书来保证系统中用户公钥的真实性和有效性。公钥证书较好地解决了公钥的真实性和有效性问题，使得 PKI 能够为网络用户提供较好的安全服务。但是对于云计算来说，PKI 无法直接部署，有两个原因：a)云计算覆盖范围广、用户众多，云计算需要提供统一的、标准的密钥管理服务，而各个国家地区的 PKI 技术标准不同，存在数据格式以及传输协议的差异，互操作性差；b)需要在客户端安装复杂的工具包，且所有的操作都需要在客户端执行，资源开销很大，部署应用困难，严重影响云计算服务器的效率。

XML 密钥管理规范(XML key management specification, XKMS)在应用程序与 PKI 之间建立一个抽象层，屏蔽了 PKI 底层技术，允许用户使用不同的 PKI 解决方案，解决了不同 PKI 系统之间的互操作性问题。文献[2]讨论了 XKMS 安全性问题，通过在每条消息中添加序列号来防止重放攻击。文献[3]提出了两种方法来解决 XKMS 消息传输安全性：a)使用边界传输协议的安全服务；b)使用一个没有安全特征的传输层协议。文献[4]通过两阶段协议提供对拒绝服务攻击的保护，并提出了通过消息签名、身份识别码、撤销码和恢复授权码来分别实现客户端和信任服务的身份验证。文献[5]分析研究了 XKMS 安全信道的问题，提出三种建立安全信道的方式，即 XML 签字、传输层安全(如 SSL、TLS 等)和网络层安全(如 IPSec)。但是，目前对于 XKMS 在云计算环境下还没有进行研究。本文通过研究云计算环境的特殊性，基于改进的 XKMS 建立了四层云计算密钥管理架构，设计了各部分模块，提出了基于信任域的工作模式；最后分析了满足云计算密钥管理的需求。

1　云计算密钥管理架构

1.1　云计算密钥管理特殊性

虚拟化是云计算的关键技术之一，它允许在同一台物理服务器上同时运行多个用户虚拟机。由于每个用户的需求不同，使得云计算存在以下几个特性：a)虚拟机中的操作系统不同；b)一个虚拟机可能存在几种身份，而且每个身份的安全等级会不同；c)用户对不同的服务，定制的服务质量不同。同时，云计算还具有虚拟机快速部署和动态迁移的特性。

云计算这些不同普通网络的特性，对密钥管理也提出了更

收稿日期：2012-07-21；**修回日期**：2012-09-05

作者简介：谢立军(1988-)，男，山西运城人，硕士研究生，主要研究方向为云计算、密钥管理(xie20060220130@sina.com)；朱智强(1961-)，男，河南信阳人，教授，主要研究方向为云计算、信任安全；孙磊(1973-)，男，江苏靖江人，副研究员，博士，主要研究方向为云计算基础设施可信增强、可信虚拟化技术；潘宁(1988-)，男，辽宁铁岭人，硕士研究生，主要研究方向为云计算.

高的要求：

a)云提供商需要提供能够面向不同操作系统和不同密钥管理技术标准的密钥管理客户端，同时该客户端可以快速安装、配置。

b)要保证密钥在虚拟机迁移过程中和完成后的安全性和可用性。

c)不同等级间密钥的访问控制更加复杂。

1.2 XKMS 概述

XKMS 协议由两部分组成，即 XML 密钥信息服务规范(X-KISS)和 XML 密钥注册服务规范(X-KRSS)。X-KISS 和 X-KRSS 都是按照 XML Schema 结构化语言定义的，都使用简单对象访问协议(simple object access protocol，SOAP1.1)进行消息的通信，它们提供的服务和消息的语法定义都遵守 Web 服务定义语言(Web service definition language，WSDL1.0)[6]。

X-KISS 定义了密钥的信息服务规范，它向密钥使用者提供密钥信息服务，任何客户端实体都可以使用此服务。XKISS 提供查询和验证两种服务。

X-KRSS 定义了密钥的管理服务规范，它向密钥管理者提供密钥管理服务，客户端实体在使用该服务之前首先必须通过信任服务的身份验证。XKRSS 提供注册、重新发布、撤销和恢复四种服务。

1.3 云计算密钥管理架构

由于云计算是分布式计算、互联网技术、大规模资源管理等技术的融合与发展，因此其密钥安全性需求更高，管理难度更大。文献[7]中认为，云计算中密钥管理面临的问题和挑战包括安全密钥存储、密钥访问、密钥备份和可恢复性。它建议密钥管理从云服务提供者中分离出来，这样在经过法律授权需要提供数据时，可以保护云服务提供者和云用户免受冲突。文献[8]提出的云计算密钥管理框架由云计算密钥客户端和云计算密钥管理服务器组成，基于统一管理框架和机制提供全面、有效的云计算密钥管理服务。

目前云计算以计算中心的方式分布在世界各地，而现有的 PKI 具有明显的区域性和行业性特征相，因此云计算可以利用现有的 PKI 提供者来提供密钥管理服务。

根据云计算部署模式，本文设计了四层云计算密钥管理架构，包括密钥管理客户端、信任服务、密钥管理服务中心和 PKI 提供者，如图 1 所示。

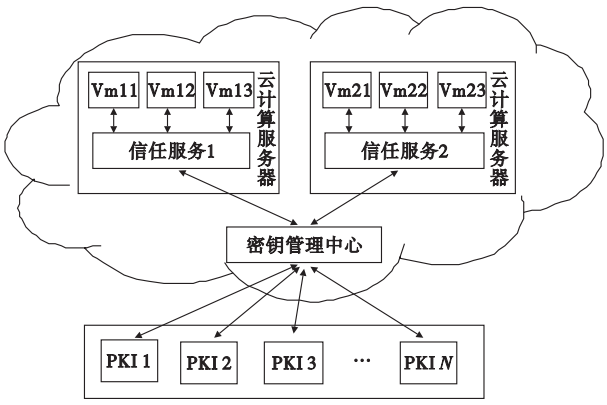

图1 云计算密钥管理架构

此架构涵盖四个管理层次，范围从小到大分别包括虚拟机、云计算物理服务器、云计算中心和整个云。

以中国云计算为例，北京云计算中心、河南云计算中心、广东云计算中心等，形成整个中国云；相对应的有北京 CA、河南 CA、广东 CA 等，作为底层 PKI 提供者。每个 CA 分别为本地区的云用户颁发证书。

1.4 模块设计

以上介绍了云计算密钥管理架构，下面介绍各部分的模块组成。

a)密钥管理客户端部署于云用户虚拟机中，负责将用户应用程序所需的信任服务以 SOAP 消息的格式发送给信任服务器端，接收并解析信任服务器端的应答消息，向应用程序提供请求消息的处理结果。它包括客户端应用交换接口、消息构造/解析模块、加/解密算法模块、XML 签名模块、可信证明模块以及信任服务交互接口，如图 2 所示。

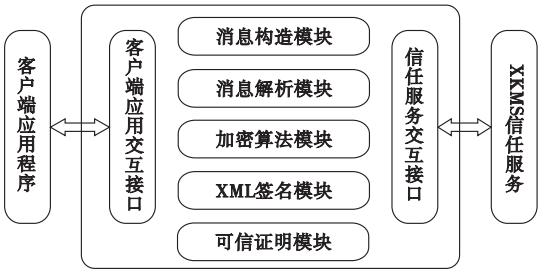

图2 密钥管理客户端

b)信任服务器端部署于云计算应用服务器中，属于一个独立的虚拟域，负责接收客户端发来的请求并回复、与密钥管理中心进行通信。信任服务体现了一种“软件转换为服务”的思想，它作为 PKI 提供者的代理，承担了很多原先由 PKI 用户完成的密钥/证书的操作，如证书解析、LDAP 目录访问、CRL 等。云用户不再需要安装、运行庞杂的 PKI 客户端软件，而只需要使用一种单一的客户端软件就可以享受服务的方式获取密钥/证书信息。它包括客户端交互接口、消息解析/构造模块、证书验证模块、XML 签名模块以及密钥管理中心交互接口，如图 3 所示。

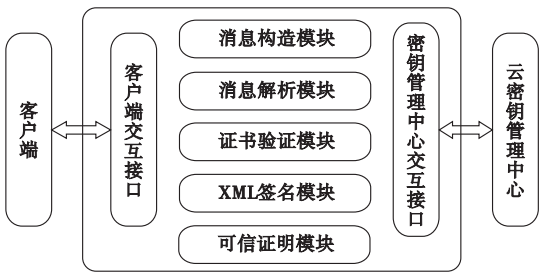

图3 密钥管理信任服务端

c)密钥管理中心处于云的逻辑边界，是云计算与外界 PKI 联结的管理中心，负责将云计算中的密钥管理请求整合、调度，并转发至 PKI。它包括信任服务交互接口、消息构造/解析模块、任务调度模块、可信证明模块以及 PKI 交互接口，如图 4 所示。

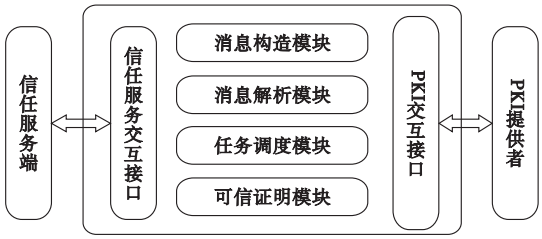

图4 云密钥管理中心

1.5　云计算密钥管理方案

1)系统初始化　其包括用户端、信任服务端、密钥管理中心和 PKI 密钥参数的确定。

2)用户密钥注册　用户端提交注册请求到信任服务端,信任服务端对消息进行解析并通过数字签名进行验证,之后提交到密钥管理中心;密钥管理中心将请求分配到相应的底层 PKI,最后 PKI 为用户颁发数字证书。信任服务端将用户的数字证书保存在本地证书库,供以后查询。

3)密钥查询　客户端发送〈ds:KeyInfo〉元素请求给信任服务端,根据被查询密钥是否存在于信任服务端,服务端返回满足客户端要求的包含公钥的〈ds:KeyInfo〉元素:信任服务可以在本地解析〈ds:KeyInfo〉元素,也可以把客户端请求转发给其他的 PKI 服务器。

4)密钥迁移　随着用户虚拟机的迁移,用户密钥也要迁移。密钥管理中心通知原虚拟机所处的信任服务 A 迁移目的信任服务 B。首先信任服务 A 与 B 进行身份认证和可信证明;然后信任服务 A 利用 B 的公钥加密用户的密钥,传输给 B,B 收到后用自己的私钥解密,密钥迁移过程结束。这样,通过信任服务之间传输用户密钥,避免了通过密钥管理中心迁移密钥产生的瓶颈问题。

2　基于信任域的工作模型

信任域[9]是公共控制下或服从一组公共策略的系统集,简单来说就是信任的范围。识别信任域及其边界对构建 PKI 很重要。由于信任的建立实质上取决于实体之间的关系,因此在定义信任域边界和信任关系时,实体之间的主观判断起到了更重要的作用。

本文的信任域包含两层含义:a)处于同一个云计算服务器内的虚拟机为第一层信任域,以信任服务器为信任锚;b)处于同一个底层 PKI 服务范围的虚拟机为第二层信任域,以 PKI 的 CA 为信任锚。根据云计算特点以及 PKI 各信任模型的优缺点,各 PKI 通过混合信任模型建立信任关系。根据信任域的两层含义,参考文献[10]中提出的两种应用模型,将云计算密钥管理服务分为三种工作模式:a)处于同一信任服务器的信任域的工作模式;b)处于同一 PKI 信任域的工作模式;c)处于不同 PKI 信任域的工作模式。下面以证书验证请求/响应为例分别说明三种工作模式。

2.1　同一信任服务器域内证书验证

虚拟机发送验证请求到信任服务,信任服务通过查询本地证书库和 CRL 来对证书进行验证。这里的信任根是信任服务。同一信任服务器域内工作模式如图 5 所示。

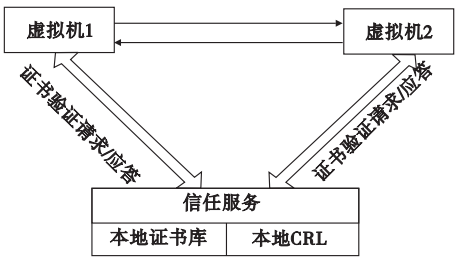

图5　同一信任服务器域内工作模式

2.2　不同信任服务器间证书验证

虚拟机发送验证请求到信任服务,由于信任服务本地证书库和 CRL 中没有所请求验证的密钥,所以将请求转发到 PKI 进行验证,并将验证结果返回到信任服务。这里的信任锚是 PKI 的 CA。其工作模式如图 6 所示。

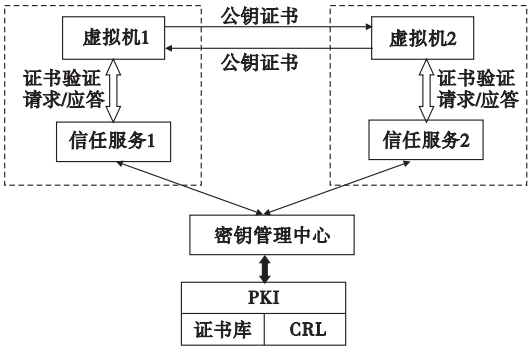

图6　不同信任服务器间工作模式

2.3　不同 PKI 提供者之间的证书验证

验证请求到达 PKI 后,PKI 通过桥 CA 发布的交叉认证证书与其他 PKI 建立信任关系,验证证书路径,并将结果返回至信任服务。其工作模式如图 7 所示。

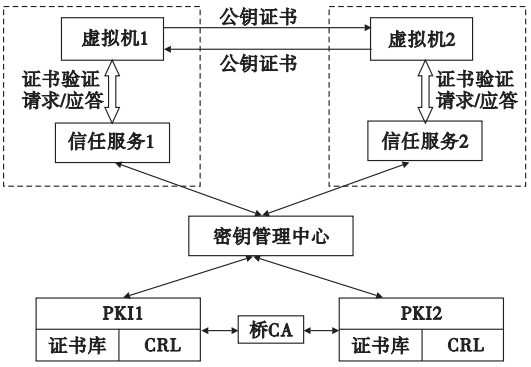

图7　不同PKI之间的工作模式

3　性能和安全性分析

3.1　信任服务模式

信任服务分为代理方式和混合方式两类[2]:

a)代理方式。其仅作为应用程序与 PKI 解决方案之间的中间层,本身不进行密钥生成、证书签发等操作,仅负责对客户端用户身份的认证,根据 XKMS 请求与特定的 PKI 提供者进行交互。这种方式实现简单,安全风险比较小;缺点是用户数量比较少时,与 PKI 提供者间进行交互所需的通信时间在响应时间中所占比重较大。

b)混合方式。其具备密钥/证书管理功能,是某一类型的 PKI 提供者,在一定程度上可以担任 CA 的角色进行证书的签发。如果请求消息的密钥、证书是可以直接处理的,则不再与其他 PKI 提供者进行交互。这种方式当用户多数是自 PKI 服务的使用者时,效率比较高,同时,由于本身能够提供对密钥证书的处理,可以不依赖其他 PKI 提供者实现全部的 XKMS 服务。

根据部署情况,本文采用混合方式的信任服务,但与文献[2]不同,这里的信任服务只提供 PKI 的验证、查询功能,不提供密钥产生和证书签发服务,在一定程度上增加了信任服务的工作效率,并减少了信任服务的安全威胁。

3.2　异步响应

XKMS 支持以下两种处理模式:

a)同步处理模式。消息发送者在发送消息以后,必须接收到响应者的响应才能继续其他的工作,否则消息发送者只能处于等待状态。同步传输模式的最大优点在于简化了网络通信的过程,易于实现,而且安全性比较高,对通信双方没有特殊的功能要求;其主要缺点是运行效率比较低,消息发送方在得到响应消息之前必须处于等待状态,这是对资源的一种浪费。

b)异步处理模式。消息发送者不需要接收者的响应或者不需要接收者立即响应,发送者在完成发送后即可进行其他操作,等接收者处理完请求后,消息发送者才提取结果。这种机制效率比较高,但它实现起来比较复杂。

针对本文提出的四层密钥管理架构,每层之间的传输需要一定的时间和宽带资源,加之云用户众多、密钥请求数量大,无法保证每个请求都能够及时接收到应答,因此采用异步处理模式。在请求发出后,发送者会定期向服务器发送状态查询 statusRequest,服务器回复状态查询结果 statusresult,直到请求消息处理完成后,服务器以 pendingresult 返回处理结果。

3.3 可信证明

在云计算环境下,XKMS 信任服务作为一个 Web 服务提供给用户。由于在云环境中,XKMS 的客户端处于云服务器的虚拟机中,而虚拟机处于用户的掌控之外,而且没有明确的物理边界,相对于目前普遍使用的个人电脑来说,系统安全性较弱,更容易受到攻击。如果用户在虚拟机遭到攻击的情况下仍然使用密钥管理服务,那么密钥的安全性会大大降低,因此在使用密钥管理服务之前,确保用户虚拟机安全和信任服务器可信是很重要的。基于 TPM 的可信证明,在客户端申请信任服务之前,增加客户端和信任服务之间相互的可信证明,确保服务的安全性和可靠性。这里客户端的可信包含虚拟机平台的可信和客户端软件的可信两个方面。

文献[11]综合阐述了多种可信证明方法,并从证明对象、证明时机等多个角度对这些证明方法进行分析和比较。针对云计算的虚拟化特点,既要证明平台的可信,又要证明应用程序的可信,所以本文利用一个可信虚拟监控器(trusted virtual machine monitor,TVMM)把一个不可窜改的硬件平台转换成为多个虚拟机,并且这些虚拟机彼此被隔离。在现有的技术中,可以在云计算服务器中加入可信平台模块(TPM)来作为不可窜改的硬件平台,将其虚拟化为多个 vTPM,并利用 TVMM 进行管理。在程序执行之前,利用每个虚拟机中的 vTPM 进行完整性度量,保证平台和应用程序在安全、可信的情况下才能进行通信。

4 实验分析

本章对于本文提出的云计算密钥管理方案进行实验仿真。采用澳大利亚墨尔本大学的网格实验室和 Gridbus 项目提出的云仿真平台 CloudSim 作为实验仿真工具,使用版本为 CloudSim-2.1.1,并建立 100 个虚拟机。将这 100 个虚拟机平均分为两类:a)虚拟机安装 XKMS 客户端,采用本文提出的密钥管理架构和方案;b)安装 PKI 客户端,直接与底层 PKI 通信。将其分别进行密钥注册、密钥查询、密钥迁移等操作。对其执行过程的平均完成时间(T)、平均通信量(I)、平均占用虚拟机内存(M)的情况进行监测,结果如表1所示。

表1 实验结果

操作		XKMS	PKI
密钥注册	T(s)	100	110
	I/Mb	25	27
	M/mb	5	10
密钥查询	T/s	80	140
	I/Mb	20	21
	M/Mb	2	5
密钥迁移	T/s	156	300
	I/Mb	50	113
	M/Mb	3	10

监测结果显示,本文提出的基于 XKMS 的密钥管理方案相对于传统 PKI 系统来说,在密钥注册、查询和迁移过程中所需要的时间和消耗的资源更少,在性能上更优。

5 结束语

本文针对目前云计算尚缺乏完整的、统一的密钥管理方案的问题,提出了基于XKMS的四层云计算密钥管理架构。该架构包括信任服务客户端、信任服务器、密钥管理服务中心和PKI提供者,将传统 PKI 作为云计算密钥管理的底层服务者,而且利用 XKMS 作为应用程序与 PKI 之间的抽象层,屏蔽了PKI底层技术的差异性,提高了云计算密钥管理的互操作性。本文还针对此架构设计了各部分模块功能,根据不同信任关系设计了三个工作模式。最后,分别从三个方面分析了改进架构的性能和安全性,并进行了比较,从多种方案中选择出较优的方案。

下一步工作将进一步细化各模块的设计,并就各模块之间的协议进行研究。同时就信任服务客户端和信任服务器端之间、信任服务器端和密钥管理中心之间的可信证明和身份认证作更进一步的研究,保证整个系统的安全性。

参考文献:

[1] 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.

[2] 张啸农. 基于 XML 的密钥管理体系的研究[D]. 长沙:长沙理工大学,2007.

[3] 尹辉. XML 密钥管理系统的研究与设计[D]. 郑州:郑州大学,2006.

[4] 高功应. 一种基于 XKMS 的密钥管理模型研究[D]. 武汉:华中科技大学,2006.

[5] 陈越,任年民,兰巨龙. XML 安全技术及一个新的基于 XML 的 Web 安全模型[J]. 计算机科学,2004,31(B09):95-97,125.

[6] HALLAM-BAKER P. XML key management specification (XKMS 2.0). W3C working draft[D/OL]. (2005). http://www.w3.org/TR/2005/REC-xkms2-20050628/.

[7] ARCHER J. Security guidance for critical areas of focus in cloud computing v2.1. cloud security alliance[EB/OL]. (2009). http://www.cloudsecurityalliance.org/guidance.

[8] 孙磊,戴紫珊,郭锦娣. 云计算密钥管理框架研究[J]. 电信科学,2010(9):70-73.

[9] 关振胜. 公钥基础设施 PKI 及其应用[M]. 北京:电子工业出版社,2008.

[10] 陈莉,张浩军,祝跃飞. XKMS 的应用研究[J]. 计算机应用研究,2006,23(9):116-118.

[11] 施光源,张建标. 可信计算领域中可信证明的研究与进展[J]. 计算机应用研究,2011,28(12):4414-4419.