

文章编号:1001-9081(2012)01-0013-03

doi:10.3724/SP.J.1087.2012.00013

# 安全服务云框架研究

孙磊\*, 戴紫珊

(信息工程大学 电子技术学院, 郑州 450004)

(\*通信作者电子邮箱 13523556215@139.com)

**摘要:**在分析云计算环境面临的安全问题基础上,基于云计算服务模式提出了安全服务云框架,分析了安全服务云框架基本工作原理和应用模式,提出了基于安全服务器状态进行多点择优部署的安全服务云调度算法。通过仿真实验表明,所提算法在服务响应时间、系统负载均衡方面明显优于随机调度算法。

**关键词:**云计算; 安全威胁; 安全服务云

**中图分类号:** TP301.6    **文献标志码:**A

## Research on framework of security service cloud computing

SUN Lei\*, DAI Zi-shan

(Institute of Electronic Technology, Information Engineering University, Zhengzhou Henan 450004, China)

**Abstract:** Following the analysis of cloud computing security in the paper, a framework of security service cloud computing was proposed based on cloud computing service pattern, which provided consistent standard model. Furthermore, the mechanism of the framework was introduced and analyzed, and a deployment algorithm of security service was proposed based on selection of the best computing server. The simulation results show that the proposed algorithm is better than random algorithm in terms of system load balance and service time.

**Key words:** cloud computing; security risk; security service cloud

## 0 引言

“云计算”<sup>[1]</sup>是目前IT领域最热的技术概念,从亚马逊<sup>[2]</sup>、IBM<sup>[3]</sup>、SUN<sup>[4]</sup>等公司的云计算推出,到“云计算”被看作是驱动下一代互联网的技术应用,云计算已经成为未来IT技术发展的方向和趋势。云计算将计算任务分布到由大量计算机构成的资源池,从而使用户能够根据需要获取计算能力、存储空间和应用,用户可以动态申请部分资源来支持各种应用,这样不仅使用户能够更加专注于自己的业务,也有利于提高资源利用效率、降低成本。从亚马逊、谷歌的云计算推出,到“云计算”被看作是驱动下一代互联网的技术应用,该领域研究风起云涌。

云计算在显著降低用户IT服务成本和带来信息管理极大方便的同时,云计算的安全问题也成了用户广为担忧的问题。云计算意味着用户任务和数据转移到用户掌控范围之外的云中,其安全风险<sup>[5]</sup>涉及到诸多方面。Gartner发布的《云计算安全风险评估》<sup>[6]</sup>中列出了云计算技术存在的管理权限、数据隔离等七大风险,云安全受到云安全联盟等越来越多研究机构和组织的关注,云计算的安全<sup>[7-8]</sup>涵盖用户使用自身终端平台访问云计算服务的全过程,包含了用户终端平台的安全、云计算服务平台的安全和通信安全三个方面的内容。用户终端平台的安全确保用户在享受云服务时自身平台的安全性。云计算服务平台的安全确保云服务的业务连续性,它是云计算安全的核心,包括云的安全治理和云的安全运维,涵盖系统安全、网络安全、应用安全、数据安全、应急响应、系统生命周期管理等领域。通信安全确保用户访问云服务时通信信息的安全性,对用户终端平台和云计算平台之间的通信信

息进行保护。

基于云计算平台和业务模式提供的信息安全服务,称为安全服务云(Secure Cloud),它是云计算时代的信息安全服务。安全服务云是专业的信息安全服务平台,能够集中对云计算环境面临的信息安全威胁进行处理,提供相应的信息加密解密、签名验签、统一身份管理和认证等信息安全服务。

## 1 安全服务云框架

### 1.1 基本工作原理

云计算的安全需求涉及终端、平台、通信多方面以及信息安全保密的全周期,涉及云计算基础设施层、平台层、应用层等多个层次。虽然云安全需求十分复杂、安全场景多样,但是作为最底层的基于密码的信息安全服务是共同的,因此本文将基于密码的信息安全服务抽象出来,从计算、存储等标准的云服务中独立出来,以云的方式构建安全服务云,向业务云提供安全即服务(security as a service)。

安全服务云以云服务的形式向业务云提供安全服务,如图1所示。它包括部署在云中的安全服务代理(Security Service Cloud Agent, SSCA)和安全云服务两部分组成。其中安全云服务由安全服务云管理(Security Service Cloud Management, SSCM)系统和身份管理服务、密钥管理服务、认证服务、加解密服务、签名验签服务等若干安全服务组成。

当用户需要向云服务提供者获得计算、存储等业务云服务时,如图2所示,首先需要进行身份注册,通过身份管理服务获取证书,或将用户原有证书与身份绑定。当用户登录获取云服务时,云计算环境将用户身份转交给安全服务云进行

收稿日期:2011-08-15;修回日期:2011-09-15。

作者简介:孙磊(1973-),男,江苏靖江人,副研究员,博士,主要研究方向:云计算基础设施可信增强、可信虚拟化;戴紫珊(1973-),女,河南南阳人,副研究员,博士,主要研究方向:云计算环境密钥管理。

认证,安全服务云将认证结果返回云服务提供者。在提供云服务时,当需要进行加解密和数字签名验证时,通过驻留在业务云中的安全服务云代理,向安全服务云提供请求,安全服务云根据用户的安全需求,提供数据加解密、签名验签服务。

安全服务构建时需要定义安全服务对象、对象安全属性、安全服务类型等信息。安全服务对象是指安全服务的对象,包括明文、密文、待签名消息、用户实体身份等对象类型;安全服务属性是指安全服务对象的属性,主要包括算法标识、密钥标识等服务属性类型;安全服务操作是指安全服务云对安全对象实施的操作,包括加密解密、签名验签、身份认证等操作。

## 1.2 安全服务云应用示例

下面以业务云需要加密服务为例描述安全服务云的工作

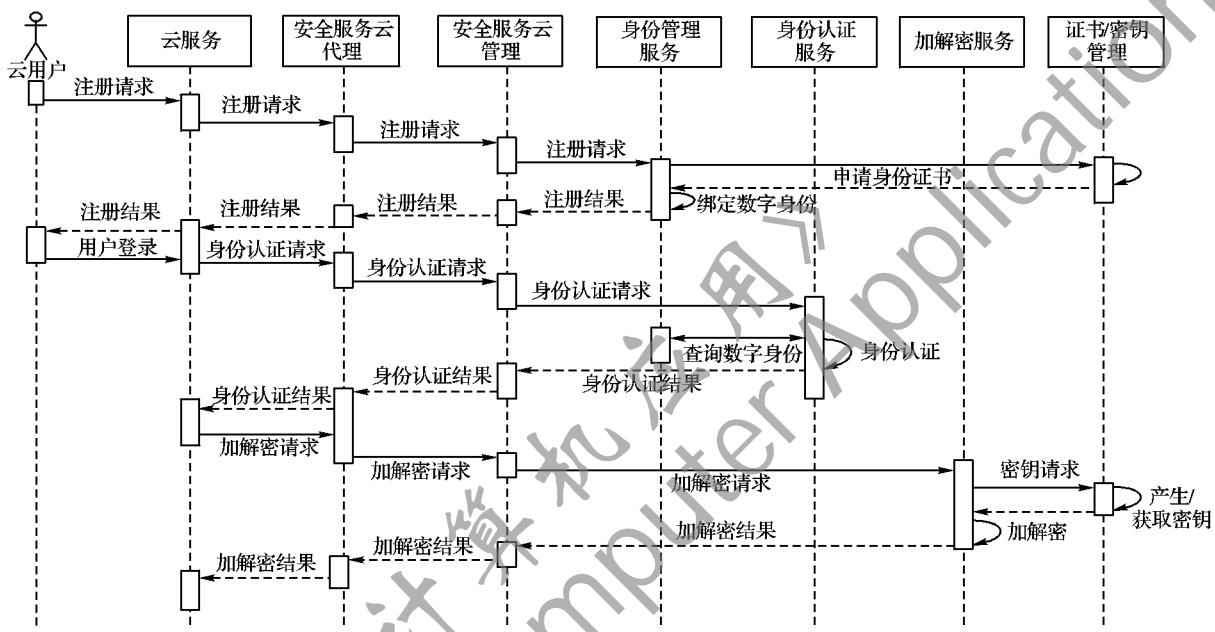


图 2 安全服务云工作原理

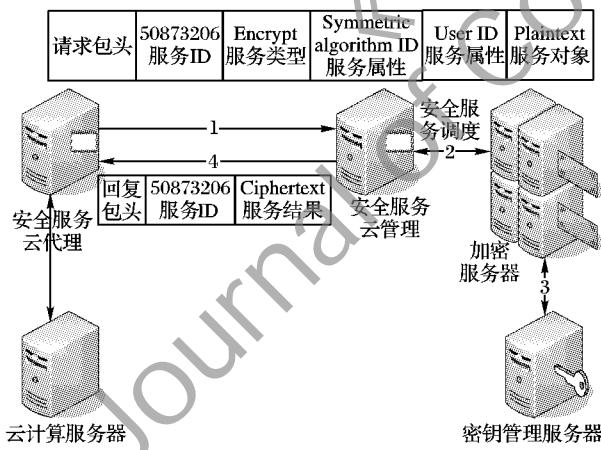


图 3 安全服务云应用原理

1) SSCA 生成加密请求,发送给 SSCM,数据包包括请求包头部、服务 ID、服务类型、算法 ID 和用户 ID 等服务属性、服务对象。其中:服务 ID 是 SSCA 发生的服务请求流水号,用于区别不同安全服务请求;服务类型表示为加密请求;服务属性指示的是对称密码算法的标识;服务对象是需要加密的明文。

2) 安全服务云管理系统 SSCM 收到请求后,根据请求包中的服务类型、属性,从采用同样对称算法的加密服务器中选择目前最合适的服务器提交加密请求。

3) 密码服务器从密钥管理服务器中生成或取出该服务

过程。当云计算服务器中数据需要进行加密时,通过 SSCA 向安全服务云请求加密云服务的过程如下(如图 3 所示)。

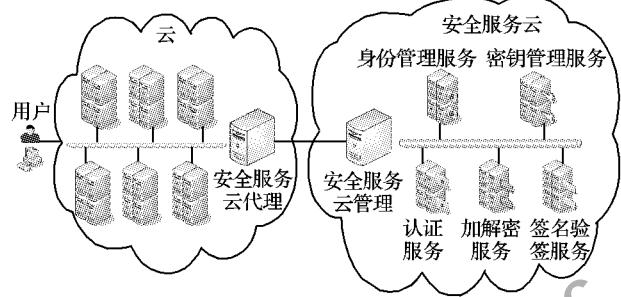


图 1 安全服务云组成

对象对应的密钥进行加密,云计算环境中的密钥管理协议可参考文献[9],最终将加密结果返回 SSCM。

4) SSCM 生成安全服务回复包,发送给 SSCA,数据包包括回复包头部、服务 ID 以及加密的密文,由 SSCA 返回给请求加密的云计算服务器。

上述 SSCM 和 SSCA 之间通信安全依靠配置信道密码机,采用信道加密保证业务云与安全服务云双方通信过程的机密性、完整性和可鉴别。

## 2 安全服务调度算法

在第 1 章中,SSCM 系统需要选择合适调度算法调度安全服务器(第 1 章中的加密服务器)完成安全服务,安全服务调度算法就成为影响安全服务云服务质量的关键因素之一。本文根据各安全计算服务器的工作状态基于择优思想进行选择。安全服务云管理系统对各安全计算节点进行监控,并将所有服务节点 CPU 使用率(CPU)、内存空闲量(RAM)、带宽空闲量(BW)和密码模块性能(CM),主要采用密码模块处理速度)组成性能矩阵:

$$Q_s = \begin{bmatrix} q(CPU_1) & q(RAM_1) & q(BW_1) & q(CM_1) \\ q(CPU_2) & q(RAM_2) & q(BW_2) & q(CM_2) \\ \vdots & \vdots & \vdots & \vdots \\ q(CPU_n) & q(RAM_n) & q(BW_n) & q(CM_n) \end{bmatrix} =$$

$$\begin{bmatrix} Q_{11} & Q_{12} & Q_{13} & Q_{14} \\ Q_{21} & Q_{22} & Q_{23} & Q_{24} \\ \vdots & \vdots & \vdots & \vdots \\ Q_{n1} & Q_{n2} & Q_{n3} & Q_{n4} \end{bmatrix}$$

由于各种性能参数的表述方式差异较大,量化单位各不相同,没有一个统一的度量标准,无法很好地进行参照对比。因此,本文对各计算节点的性能参数进行无量纲化和归一化处理。归一化是指把各参数的值都映射到区间[0,1]。无量纲化是指通过数量变换,消除量纲和数量级对参数值的影响,使性能实际值转化为可以进行统一评价的判断值的方法。本文采用非比例变换法来做规范化,将指定参数之差按一定比例进行归一化和无量纲化处理。性能参数的规范化计算公式如式(1)所示:

$$P_{i,j} = \begin{cases} (Q_{i,j} - Q_j^{\min}) / (Q_j^{\max} - Q_j^{\min}), & Q_j^{\max} - Q_j^{\min} \neq 0 \\ 1, & Q_j^{\max} - Q_j^{\min} = 0 \end{cases} \quad (1)$$

通过式(1),可将服务节点实际性能矩阵转换成为判断矩阵,如式(2)所示:

$$P_s = \begin{bmatrix} P_{11} & P_{12} & P_{13} & P_{14} \\ P_{21} & P_{22} & P_{23} & P_{24} \\ \vdots & \vdots & \vdots & \vdots \\ P_{n1} & P_{n2} & P_{n3} & P_{n4} \end{bmatrix} \quad (2)$$

得到判断矩阵之后便可以对服务节点计算性能进行排序。本文采取计算节点综合性能质量的方法,给服务节点进行评分排序。对于加密、解密、签名、认证等不同类型安全服务请求,根据安全服务类型确定CPU使用率、内存空闲量、带宽空闲量和密码模块性能等选择权值 $W_j$ ( $W_j \in [0,1]$ , $\sum_{j=1}^4 W_j = 1$ ,( $j = 1,2,3,4$ ))。通过权值计算出每个安全服务节点的综合性能质量 $R_i$ ( $i = 1,2,\dots,n$ ),其计算公式如式(3)所示:

$$R_i = \sum_{j=1}^4 (P_{ij} \times W_j); \quad i = 1,2,\dots,n, \quad j = 1,2,3,4 \quad (3)$$

从 $n$ 个服务节点找出适合该次安全服务的最优服务节点 $R_{best}$ 的计算公式如式(4)所示:

$$R_{best} = \max_{i=1}^n (R_i); \quad i = 1,2,\dots,n \quad (4)$$

### 3 仿真实验

安全服务是一种特殊的云服务,本文采用可扩展的云仿真平台CloudSim<sup>[10]</sup>对安全服务调度算法进行仿真实验。由于CloudSim只是对现有标准的云服务和资源调度进行仿真,对于密码计算服务等安全服务未提供仿真支持,要评价本文提出的安全服务调度算法,需要基于CloudSim仿真框架进行扩展,在物理服务器(Host类)和虚拟机(Vm类)性能描述中添加安全服务属性和安全服务对象等描述,在Scheduling Policy这一层通过编写DatacentreBroker类中的方法函数bindCloudletToVM(),实现本文提出的安全服务调度算法,扩展后的仿真框架如图4所示,重新编译后,编写仿真程序可以进行安全服务调度算法的仿真。

本文采用安全服务平均完成时间和系统负载方差两个指标,来比较本文提出的安全服务调度算法和CloudSim原有资源调度算法(随机算法)的性能:

1) 安全服务平均完成时间是指从安全服务提交请求到

返回安全服务计算结果之间的时间间隔, $N$ 个安全服务任务完成后统计计算其平均值;

2) 系统负载方差为 $\sum_{i=1}^n (R_i - \bar{R})^2$ ,表示每完成一定数量服务后,对系统中各个服务器的资源利用率 $R_i$ 进行采集和拍照,取每一个服务器的综合性能质量 $R_i$ 与系统平均综合性能质量 $\bar{R}$ 计算方差,得到系统负载方差。

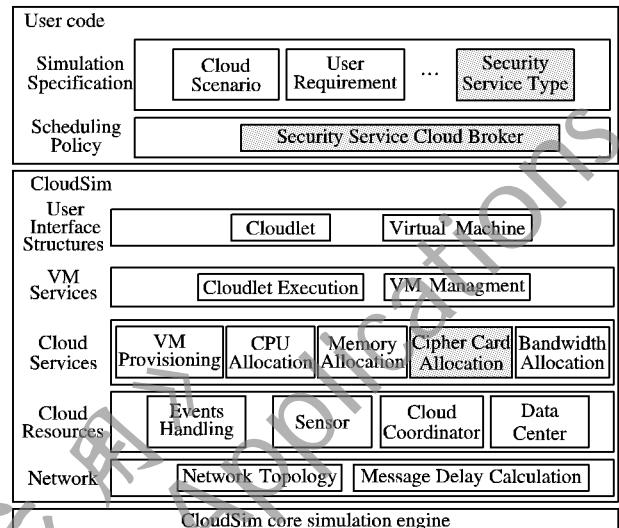


图4 基于CloudSim扩展的安全服务仿真框架

实验开始后,首先创建一个具有40台服务器(Host)和80个虚拟机计算节点(Vm)的数据中心(Datacenter),分别采用本文算法和CloudSim自带的随机算法进行实验,执行200个相同的任务,每完成20个任务输出一次任务平均完成时间和系统负载方差。实验结果如图5~6所示,从实验结果可以看出,采用本文提出的安全服务调度算法所得到的安全服务平均响应时间明显小于采用随机算法的服务时间,同时安全服务云中的系统整体负载均衡能力(负载方差较小)明显好于采用随机算法的负载均衡能力。

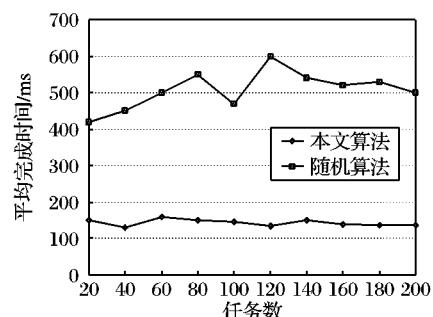


图5 平均完成时间

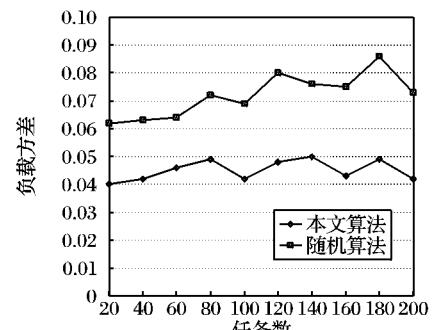


图6 负载方差

$w(M_{A_i}^*)^T = 0$ 。然后  $S$  随机选取  $t' \in \mathbf{Z}_N, R_0, R'_0 \in G_{p_3}$ ,  $\{R_{att}\}_{att \in S_U} \in G_{p_3}$ 。令  $t = t' + w_1 a^q + w_2 a^{q-1} + \dots + w_n a^{q+1-n}$ ,  $S$  按下述方法计算  $SK_U$ :

$$\begin{aligned} K_U &= g^a g^{at'} R_0 = g^{a'} (g^a)^{t'} \prod_{j=2}^n (g^{a^{q+2-n}})^{w_n} R_0; L_U = g^t R'_0 = \\ &g^{t'} \prod_{j=1}^n (g^{a^{q+1-j}})^{w_j} R'_0; \text{对 } \forall att \in S_U, \text{若有 } att \in S_B, \text{则 } K_{U_{att}} = \\ H_1(att)^t &= L_U^{h_{att}} \prod_{j=1}^n (g^{t'a^{j/b_i}} \prod_{k=1, k \neq j}^n (g^{a^{q+1+j-k/b_i}})^{w_k})^{M_{A_{i,j}}^*}; \text{否则} \\ K_{U_{att}} &= H_1(att)^t = L_U^{h_{att}}, \text{最后返回 } SK_U; \end{aligned}$$

4) MasterReveal。由于  $S$  不知道系统主密钥, 模拟失败。

$M$  以至少  $1/(P^2L)$  的概率选择  $S$  在初始化阶段选定的会话作为测试会话, 根据新鲜性的定义,  $M$  不允许进行 MasterReveal 询问, 不允许揭示  $\{\bar{x}_1, \dots, \bar{x}_{n_A^*}\}, SK_A$  和腐化  $B$ , 此时  $M$  能区分开被  $S$  修改的安全性游戏与真实安全性游戏的唯一方法是向  $H_2$  询问  $(\bar{x}_1, SK_A)$ , 因此除过一个可忽略的猜测概率  $2/N$ ,  $S$  的模拟不会失败。而当  $M$  成功地进行了伪装攻击, 则  $M$  一定向  $H_3$  询问了  $(Z_1, Z_2, Z_3, EPK_A, f_{Ac-A}^*, EPK_B, f_{Ac-B}^*)$ , 并且  $DPBDHE(v, Z_1/e(X, g^{a'}) = 1, DPBDHE(v_2, Z_2/e(Y, g^{a'})) = 1, e(X, Y) = e(g, Z_3)$ , 则  $S$  可解决 GDPBDHE 挑战:  $e(g^s, g^{a^{q+1}}) = Z_1/e(g^s, g^{a'})$ , 而  $S$  成功的概率为:

$$Adv_{GPBDHE}(S) \geq \frac{1}{P^2L} \cdot Adv_{\Pi}^{ABAKE}(M) - \frac{2}{N} - O\left(\frac{L^2}{2^k}\right)$$

## 5 结语

本文基于全安全的 CP-ABE 机制, 提出了一种全新的两轮全安全的 ABAKE 协议, 并在 ABeCK 模型中证明了其安全性。与其他同类协议相比, 新协议在安全性和属性认证方式上同时具有优势, 并且通信开销更小, 更适合于在实际的属性基加密系统中应用。如何进一步提高协议的执行效率是下一步要研究的工作。

## 参考文献:

- [1] ATENIESE G, KIRSCH J, BLANTON M. Secret handshakes with dynamic and fuzzy matching [C]// NDSS 2007: Proceedings of the Network and Distributed System Security Symposium. San Diego:

(上接第 15 页)

## 4 结语

本文在分析云计算环境面临的安全威胁基础上, 提出了一种提供安全保密服务的安全服务云框架, 提供统一身份认证、数据加解密、数据签名验签等基础安全服务, 在此基础上提出了一种安全服务调度算法。实验仿真结果表明, 本文提出的安全服务调度算法在平均服务响应时间、系统负载均衡等方面明显好于随机调度算法。下一步将围绕安全服务整体调度算法及其优化开展研究, 确保安全服务云的高效和可靠。

## 参考文献:

- [1] 陈康, 郑纬民. 云计算: 系统实例与研究现状[J]. 软件学报, 2009, 20(5): 1337–1348.  
[2] Amazon. Amazon elastic compute cloud [EB/OL]. [2011-04-15]. <http://aws.amazon.com/ec2/>.  
[3] IBM. IBM blue cloud solution [EB/OL]. [2011-05-20]. <http://www-900.ibm.com/ibm/ideasfromibm/cn/cloud/solutions/index.shtml>.  
[4] SUN. Cloud architecture introduction white paper [EB/OL].

- USENIX Association, 2007: 159–177.  
[2] WANG H, XU Q, BAN T. A provably secure two-party attribute-based key agreement protocol [C]// Proceedings of Intelligent Information Hiding and Multimedia Signal Processing. Washington, DC: IEEE Computer Society, 2009: 1042–1045.  
[3] BIRKETT J, STEBILA D. Predicate-based key exchange [C]// Proceedings of Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 2010: 282–299.  
[4] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [C]// PKC'11: Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography. Berlin: Springer-Verlag, 2011: 53–70.  
[5] YONEYAMA K. Strongly secure two-pass attribute-based authenticated key exchange [C]// Pairing'10: Proceedings of the 4th International Conference on Pairing-based Cryptography. Berlin: Springer-Verlag, 2010: 147–166.  
[6] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption [C]// Advances in Cryptology – EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2010: 62–91.  
[7] LAMACCHIA B, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange [C]// ProvSec'07: Proceedings of the 1st International Conference on Provable Security. Berlin: Springer-Verlag, 2007: 1–16.  
[8] BEIMEL A. Secure schemes for secret sharing and key distribution [D]. Haifa: Israel Institute of Technology, 1996.  
[9] WATERS B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions [C]// Advances in Cryptology – CRYPTO 2009, 29th Annual International Cryptology Conference. Berlin: Springer-Verlag, 2009: 619–636.  
[10] OKAMOTO T, POINTCHEVAL D. The gap-problems: A new class of problems for the security of cryptographic schemes [C]// PKC 2001: Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography. Berlin: Springer-Verlag, 2001: 104–118.

- [2011-05-13]. [http://developers.sun.com/blog/functionalca/resource/sun\\_353cloudcomputing\\_chinese.pdf](http://developers.sun.com/blog/functionalca/resource/sun_353cloudcomputing_chinese.pdf).  
[5] LEMON S. Cloud computing not secure enough [EB/OL]. [2011-05-10]. <http://www.Cio.com/article/>.  
[6] HEISER J, NICOLETT M. Assessing the security risks of cloud computing [EB/OL]. [2011-03-25]. <http://www.gartner.com/DisplayDocument? id=685308>.  
[7] 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.  
[8] SANTOS N, GUMMADI K P, RODRIGUES R. Towards trusted cloud computing [C]// HotCloud'09: Proceedings of the 2009 Conference on Hot Topics in Cloud Computing. Berkeley: USENIX Association, 2009: 1–5.  
[9] 孙磊, 戴紫珊. 云计算密钥管理框架研究[J]. 电信科学, 2010, 26(9): 26–30.  
[10] CALHEIROS R N, RANJAN R, de ROSE C A F, et al. CloudSim: A novel framework for modeling and simulation of cloud computing infrastructures and services [R]. Melbourne: University of Melbourne, 2009.