一种基于信任协商机制的云服务资源信任验证方法

杨绍禹[1] 王世卿[1] 郭晓峰[2]
(郑州大学信息工程学院 郑州 450052)[1] (信息工程大学理学院 郑州 450000)[2]

摘 要 云计算环境下,服务资源分布广泛、迁移频繁,资源之间的信任关系不易建立与维护。传统的可信计算远程验证方法存在性能瓶颈和计算复杂等问题。在研究云服务资源信任验证方法的基础上,提出一种属性协商的远程验证方法。采用环签名算法和基于属性的敏感信息保护机制,提高了信任验证计算效率,减小了敏感信息泄露的风险。设计的安全模型证明了方法的安全性。通过Hadoop平台下的实验,验证了方法的有效性和可行性。

关键词 云计算,可信计算,远程证明,环签名,自动信任协商
中图法分类号 TP309 **文献标识码** A

Trust Negotiation-based Services Verification in Cloud Computing

YANG Shao-yu[1] WANG Shi-qing[1] GUO Xiao-feng[2]
(Information & Engineering College, Zhengzhou University, Zhengzhou 450052, China)[1]
(Institute of Science, PLA Information Engineering University, Zhengzhou 450000, China)[2]

Abstract In cloud computing, the resources of service are widely distributed and migrated frequently. The trust relationship between them is hard to establish and maintain. There are some problems for traditional remote attestation based on trust computing, such as performance bottleneck and computational-complexity. This article proposed a novel remote attestation mechanism based on property negotiation in cloud computing. According to the ring signature algorism and sensitive property-based protection, this mechanism promotes the computational efficiency and reduces the leakage risk of sensitive property. Security of the mechanism is verified by security model. Validity and feasibility are tested by the experiment on Hadoop platform.

Keywords Cloud computing, Trust computing, Remote attestation, Ring signature, Automated trust negotiation

1 引言

云计算环境中,服务资源具有组合方式灵活、迁移操作频繁等特点。为了有效地对这些资源进行安全管理,通常以安全域来控制资源的访问权限和安全级别[1,2]。安全域内部可以通过域内统一的管理单元对服务资源进行密钥分配、证书签发和权限控制等操作。但是,由于云服务资源分布广泛,集中的安全管理比较困难,安全域外的不可信资源与域内资源之间的信任关系不易建立与维护。

本文在研究可信计算远程证明方法的基础上,结合信任协商机制,通过属性信任协商的方式来建立域内资源与域外资源之间的信任关系。通过性能分析和实验,说明并验证了方法的可行性和有效性。本文第2节介绍可信计算远程证明方法,并叙述了远程证明方法的研究现状;第3节提出改进的可信云平台信任验证方法;第4节通过设计安全模型对可信云平台信任验证方法安全性进行分析;第5节对这种验证方法进行性能分析和比较,并通过实验验证了平台的有效性。

2 可信计算远程证明方法

可信计算(Trusted Computing)是由可信计算组织TCG(Trusted Computing Group)提出的一套信息安全保障的规范和标准体系[3,4]。可信计算通过加强硬件产品和操作系统等应用支撑平台的信任管理,扩大了用户的计算信任范围,保证了系统内的应用处于一个"干净"的环境中。

2.1 远程证明方法

可信计算中的平台远程证明方法是用来建立实体之间信任关系的主要技术。TCG最先采用的远程证明方法是Privacy CA方法[3]。该方法在每次进行认证时需由TPM(Trust Platform Module)根据EK公钥信息生成新的身份标识密钥AIK,且要求该密钥可被证书中心CA证明;随后,TCG又引入了直接匿名认证(DAA, Direct Anonymous Attestation)方法[4],DAA方法中使用了签名技术,并通过消息交互使验证方相信TPM对特定信息进行了签名,但不能得到TPM的身份标识。近年来,有很多相关研究围绕着远程证明过程效率改善、敏感信息保护以及异构环境信任验证等问题展开。比

到稿日期:2012-09-20 返修日期:2012-12-20 本文受国家"十一五"科技支撑计划项目(2006BAF01A00)资助。
杨绍禹(1980-),男,博士生,CCF会员,主要研究方向为信息安全、云计算,E-mail:ysymagnet@gmail.com;王世卿(1951-),男,博士,教授,主要研究方向为电子商务、信息安全;郭晓峰(1982-),男,博士,主要研究方向为分布式计算。

如，文献[5]提出了一个新的 DAA 机制，这个机制通过在椭圆曲线构造双线性映射缩短了私钥和签名长度，降低了 DAA 零知识证明过程中的时间复杂度。文献[6]将 DAA 签名者按照计算能力分为两类，即 TPM 签名者和 HOST 签名者。采用椭圆曲线和对称匹配的方法设计了一种 DAA 机制，其可以实现利用少量的 TPM 计算资源完成信任验证。为了更好地支持跨域认证，文献[7]通过引入可信第三方仲裁中心来进行跨域证书的颁发与验证。文献[8]针对异构的、分布式的开放系统，提出一种基于语言验证的虚拟机，其可以对运行在其上的动态代码和系统配置进行平台无关的信任验证。文献[9]和文献[10]对基于属性的远程证明(Property-Based Attestation，PBA)方法进行了研究，在 DAA 验证基础上对敏感的属性信息进行屏蔽与隐藏。

2.2 存在的问题

通过对可信计算中远程证明方法目前研究成果的简述，可以看出远程证明过程中计算效率、跨域验证与敏感信息保护是重点关注的研究内容。TCG 提供的两种远程证明方法在签名方式上有一些不同。Privacy CA 方法需要认证中心在每次与验证方进行认证过程时都参与，这样的机制极易造成认证过程的性能瓶颈。同时，认证中心也有被验证方控制进行合谋攻击的安全威胁。为了解决 Privacy CA 认证方法中出现的问题，DAA 方法以零知识证明和 C-L 签名(Camenisch-Lysyanskaya)为基础，无需第三方持续参与，完成平台信任验证。但是，DAA 中的签名算法包含了大量的模幂运算，计算复杂度比较大，需要高性能的计算资源。关于证明方 TPM 平台配置信息隐私保护问题，在早期 TCG 发布的标准中没有涉及，而目前的标准和规范都采用了基于属性的远程证明方法。这种方法将平台配置信息封装在属性信息中，有效地保护了二进制形式的 PCR 数据。但是在验证双方的属性信息进行交互的过程中，会有一些不需要暴露给对方的敏感属性。这些信息可能会造成自身平台配置信息的泄露。同时，云服务资源迁移频繁，合法的属性证书拥有者可能无法保证迁移的资源仍然能够保持原有证书的合法性。在云计算环境下，服务资源之间需要一种无需第三方参与的、高效的、便利的远程证明方法。

3 可信云平台信任验证方法

可信云计算是将可信计算技术引入云计算环境，为云服务提供基础的安全支撑。可信云平台是可信计算在开放环境中的扩展，适合描述以层次化服务为主要内容的云计算。

3.1 属性协商的远程证明模型

云服务资源远程证明需要满足计算高效、信息隐藏和独立验证的安全验证要求。为此，我们提出了一种基于属性协商的远程证明模型，如图 1 所示。这个模型包含了 3 个层次，用户层、协商层和验证层，各层之间可以进行轻量级信息交互。其中，用户层主要是完成信任验证请求与响应任务，同时还需要建立双方协商通道；协商层主要任务是根据用户层的请求，进行属性匹配与敏感属性解锁、协商策略验证和属性证书生成等；验证层主要任务是利用远程证明方法生成各自的 TPM 平台配置信息，并采用基于环签名的方法对信息进行签名和验证。

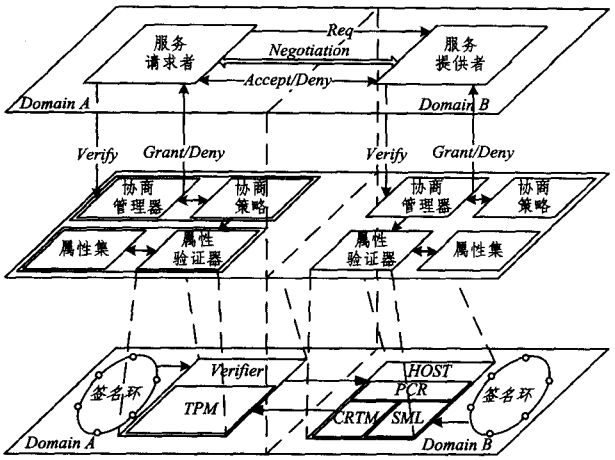

图 1 属性协商远程证明模型

1. 用户层

用户层由服务资源请求者和服务提供者组成。它们分别属于两个不同的管理安全域(Domain A 和 Domain B)，彼此之间无法通过集中验证的形式完成信任关系的建立。服务请求者发出信任验证请求(*Req*)并提供需要验证的属性内容。服务提供者根据 *Req* 以及验证属性向协商层发出验证消息。根据协商层进行属性验证的结果，决定建立或者拒绝建立信任关系(*Accept/Deny*)，或者进一步进行属性交互协商(*Negotiation*)。经过多次属性协商之后，不可信的双方建立信任关系。

2. 协商层

协商层由 4 个主要功能组件构成，即属性验证器、属性集、协商策略集合和协商管理器。属性验证器的主要作用是根据属性与平台配置信息之间建立的映射关系，验证是否满足属性的平台配置信息；属性集合是用来保存这种映射关系的存储单元；协商管理器与用户层进行通信，根据用户层要求和协商策略，决定解锁属性证书、发送属性验证请求和信任授权与拒绝(*Grant/Deny*)操作；协商策略集合保存用于进行信任协商的策略信息。协商层的工作可以分为两个方面的内容：一方面，接收用户层的验证和协商请求；另一方面，根据属性与 TPM 配置信息映射关系，进行基于属性的平台可信验证。

3. 验证层

验证层主要是由 TPM 和 TPM 载体 HOST 或 Verifier 组成，通过各自安全域内的 TPM 公钥组成签名环，用于对双方验证过程的消息进行签名。根据协商层的属性与 TPM 平台配置信息的映射关系，获取 PCRs 中的信息并进行 TPM 签名。将这些信息和 TPM 载体用来记录信任测量日志的 SML 信息一起发送给协商层。

3.2 基于环签名的消息签名算法

云环境下的服务资源之间进行信任验证是一个相对独立的过程。验证双方很难通过集中式的信任中心来鉴别对方身份的合法性。为了适应云服务资源远程验证的特点，提高信任建立效率，我们引入环签名方法来对交互消息进行签名。环签名的建立只需要输入环成员公钥、签名消息以及生成密钥所需的安全参数等信息。证明方与验证方可以直接通过双方的 TPM 公/私钥对进行远程身份验证，减少了之前远程证明方法中的第三方验证机构和不必要的交互通信。可信云计

算平台下，基于环签名的远程证明方法包括了3个阶段，分别是初始化安全参数、签名生成、签名验证。

1. 初始化安全参数

签名方基于强RSA假设，输入$\{0,1\}^{l_n}$创建强RSA安全参数，满足$n=p.q$（p,q为大素数）。随机选择$R_1,R_2,S,Z\in QR_n$，QR_n是二次剩余群，输出签名方公钥$pk_{proof}=(n,R_0,R_1,R_2,S,Z)$和私钥$sk_{proof}=p$。根据安全性需求，选择参与环签名成员数量$r$（$r$的数量与计算复杂度成正比），得到$r$个公钥组成的元组$(pk_1,pk_2,\cdots,pk_r)$签名，其中包含了签名方公钥$pk_i=pk_{proof}(1\leqslant i\leqslant r)$。TPM生成AIK密钥对$(AIK_p,AIK_s)$并将其保存在寄存器中。选取SHA256算法的Hash函数$Hash:\{0,1\}^*\rightarrow Z_p$。

2. 签名生成

1）对称密钥生成

根据选取的Hash函数生成TPM的AIK_p对称密钥k

$k=Hash(AIK_p)$

2）生成$g(x)$

随机选取大随机数串组成序列集合

$X=\{x_1,x_2,\cdots,x_i,x_{i+1},\cdots,x_r\mid x_k\in\{0,1\}^*,1\leqslant k\leqslant r,k\in Z^+\}$

$g(x):X\rightarrow\{y_1,y_2,\cdots,y_i,y_{i+1},\cdots,y_r\}$

3）计算$g(x_i)$和x_i

利用环方程$C_{kv}=(g(x_1),g(x_2),\cdots,g(x_r))=v$求解$g(x_i)$的值。按照文献[11]中的环方程，利用逐比特异或运算⊕来完成计算，方程如下：

$$C_{kv}(g(x_1),g(x_2),\cdots,g(x_r))=E_k(g(x_r)\oplus E_kg(x_{r-1})\oplus E_kg(x_{r-2})\oplus E_k(\cdots\oplus E_kg(x_1)\oplus v))$$

根据环方程，求解$g(x_i)$的方法如下：

$$g(x_i)=E_k(g(x_{i-1})\oplus E_kg(x_{i-2})\oplus E_k(\cdots\oplus E_kg(x_1)\oplus v)\cdots))\oplus D_k(g(x_{i+1})\oplus D_kg(x_{i+2})\oplus D_k(\cdots\oplus D_kg(x_1)\oplus v)\cdots))$$

其中，D_k和E_k是对称加密算法的加密、解密函数。最后，利用私有密钥sk_{proof}求解$x_i=g^{-1}(x_i)$。

4）输出环签名与AIK签名

签名方得到的环签名σ与TPM中消息m的AIK签名一起发送给验证方。

$\sigma=(AIK_p,pk_1,pk_2,\cdots,pk_r,v,x_1,x_2,\cdots,x_r)$

$Sig_{proof}=(SIGN_{AIK}(m),\sigma)$

3. 签名验证

1）验证$SIGN_{AIK}(m)$签名的真实性

使用AIK_p对签名进行解密，与消息的Hash值比对。

$E_{AIK_p}(SIGN_{AIK}(m))\overset{?}{=}Hash(m)$

2）验证环方程

根据签名方发送的AIK_p和$pk_1,pk_2,\cdots,pk_r$，使用生成阶段2）和3）公式重新验证环方程等号两边是否相等，如果相等则验证成功，否则失败。

3.3 属性协商

TCG1.1标准中，规范化的平台授权方法采用的是二进制验证。所有对验证对象的度量结果都存放在TPM的状态寄存器PCRs中。当需要进行平台信任关系鉴别的时候，从PCRs中获取平台配置信息，经过签名操作后发送给验证方。这种方法极易发生平台信息泄露的问题。随后TCG发布的标准中采用了基于属性的远程证明方法。这种方法通过建立可信属性与平台配置信息之间的映射关系，利用可信属性代替二进制度量信息。

可信属性是用来描述平台所能够满足的某一安全需求，例如某一个银行在线支付平台要求用户需要具有用户身份密钥（U盾）、安全签名证书和操作系统版本等一些安全要求。可信属性的验证过程是验证平台或者配置信息是否能够满足属性所包含的安全需求。这种验证能够屏蔽平台软件和硬件的配置信息，同时，对于动态的平台信息更新也能够灵活地变更。在云计算环境下，服务资源的配置信息或者安全属性信息容易被敌手获取而成为其攻击服务资源的依据。因而，对于一些敏感的可信属性应该加以保护和隐藏，以防止将不必要的属性信息泄露给敌手。

属性协商的验证方法，在基于属性的验证方法的基础上，利用自动信任协商机制[12]对属性交互过程进行控制，避免不必要的可信属性信息暴露给对方。

定义1（信任验证） $TRUST_i=\exists PCR_i\subseteq PCR,PCR=\{pcr_1,pcr_2,\cdots,pcr_m\},m\in Z^+$使得$\{E_{AIK_p}(SIGN_{AIK}(PCR_i,c))\equiv Hash(m)$ and $E_\sigma(g(x_1),g(x_2),\cdots,g(x_r))\equiv v\}$，其中$PCR$是TPM的平台配置信息状态寄存器，$c$是验证请求，且$PCR_i\subseteq PCR$，AIK是TPM的识别标志。

定义2 属性与验证的映射关系表示为$SPMR(SP,TRUST)$，其中属性集合

$SP=\{sp_1,sp_2,\cdots,sp_n\},TRUST\subseteq\bigcup_{TRUST_i}^{m},m,n\in Z^+$

定义3 属性协商ATN_{cloud}由一个五元组构成：

$\{c,SP,SPMR(SP,TRUST),Unlock(SP_2,SP_1),Negot\_Type\}$

其中包含了两个系统变量、两个行为函数和一个控制参数。c和SP分别是协商请求和用来建立协商的属性证书集，其中包含了自由未保护的证书和对敏感属性进行保护的加锁属性证书；$SPMR(SP,TRUST)$表示信任验证$TRUST$能够满足属性集合SP的安全需求；$Unlock(SP_2,SP_1)$表示属性证书集SP_1可以为SP_2解锁，使加锁属性证书变成自由未保护的状态。若SP_1为$\emptyset$，$Unlock(SP_2,\emptyset)$则表示SP_2中的证书是自由未保护的。$Negot_Type$是ATN的性能约束参数，根据协商参与者对云服务安全性和效率的需求，参数是从积极模式到谨慎模式连续的性能约束量。

属性协商过程如图2所示。

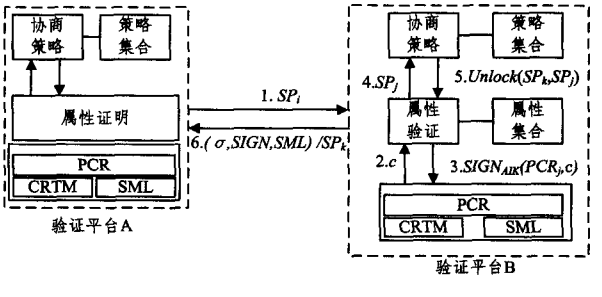

图2 属性协商信任模型

1. 验证平台A通过安全通道（前提假设平台间的通信是安全的）向平台B发出信任建立请求。这个过程是通过发送平台A信任验证的安全需求属性集合SP_i来实现的。

2. 验证平台B中的属性验证器根据协商策略对SP_i中可以暴露的属性集合SP_j（$SP_j\subseteq SP_i$）进行验证，生成可信计

算证明请求 c，获取 B 平台配置信息 $SIGN_{AIK}(PCR_j, c)$，将其与可信度量日志 SML 通过环签名生成验证消息发送给 B 平台。

3. 同时，根据协商策略，利用 A 平台属性集合 SP_i 解锁属性集合，得到平台 B 对平台 A 的安全属性需求 SP_k，并将其发送给 B 平台请求验证。

4. B 平台在收到 A 平台验证消息 $SIGN_{AIK}(PCR_j, c)$、SML 日志文件、平台 A 的协商安全属性需求 SP_k 后，首先通过协商验证函数 $SPMR(SP_i, TRUST)$ 验证其是否成立。如果成立，则说明属性协商成功，建立 A 与 B 之间的信任关系；否则，根据 A 平台的安全属性需求 SP_k 和平台 B 的协商策略重复步骤 1 操作，并将 B 平台的验证消息发送给 A。

4 安全性分析

本节对上一节提出的信任验证方法进行安全性分析，通过构造安全模型来验证方法的安全性。

4.1 安全模型

定义 4(敌手模型) 假设敌手 $\mathcal{A}$ 是一个满足属性协商的远程证明过程的恶意攻击单元。敌手 $\mathcal{A}$ 能够伪装成任一方给对方发送信任验证请求消息 $send(\mathcal{E}, m)$，$\mathcal{E} \in \{\mathcal{H}, \mathcal{V}\}$，同时，敌手 $\mathcal{A}$ 能够接收由 $\mathcal{E}$ 产生的远程证明验证消息。敌手 $\mathcal{A}$ 通过 $sendTPM(m)$ 能够与 TPM 通信，假定 m 包含了发送者的身份信息。此外，敌手 $\mathcal{A}$ 可能通过某种方式 $corrupt_{\mathcal{H}}$ 攻击 $\mathcal{H}$，获取 $\mathcal{H}$ 的配置信息 PCR_i。这里假设敌手 $\mathcal{A}$ 无法通过任何手段攻击 TPM。

1. 不可伪造性(Unforgeable)。敌手伪装成证明方 $\mathcal{P}$，通过伪造证明方属性集合 $cs_{\mathcal{P}}$ 使其满足 $SPMR(SP, TRUST)$，而实际上 $cs_{\mathcal{P}} \notin SP$。设计 $\mathcal{P}$，$\mathcal{V}$ 和 $\mathcal{A}$ 之间进行安全游戏 $Game_{\mathcal{A}}^{unforg}(1^k)$，敌手 $\mathcal{A}$ 首先从 TPM $\mathcal{M}$ 中选取 $cs_{\mathcal{P}} \notin SP$，接着敌手向证明方 $\mathcal{P}$ 发起攻击。如果敌手 $\mathcal{A}$ 产生的签名信息 σ 在验证方能够满足 $TRUST_i$，则在 $Game_{\mathcal{A}}^{unforg}(1^k)$ 中 $\mathcal{A}$ 获胜。敌手 $\mathcal{A}$ 获胜的概率表示为

$$SUCC_{\mathcal{A}}^{unforg}(1^k) = \Pr[Game_{\mathcal{A}}^{unforg}(1^k) = win]$$

定义 5 如果 $SUCC_{\mathcal{A}}^{unforg}(1^k)$ 是可以忽略的，则属性协商证明过程是不可伪造的。

2. 信息隐藏性(Information Hiding)。敌手能够获取证明方 $\mathcal{P}$ 的平台配置属性信息 $cs_{\mathcal{P}}$ 所表示的隐藏信息。设计 $\mathcal{P}$，$\mathcal{V}$ 和 $\mathcal{A}$ 之间进行安全游戏 $Game_{\mathcal{A}}^{IH}(1^k)$，敌手 $\mathcal{A}$ 选择证明方 $\mathcal{P}$ 进行安全攻击。最后，敌手 $\mathcal{A}$ 能够获得一个索引值 i。如果 i 能够作为 PCR_n 中的索引值，即 $pcr_i = pcr_k$，$pcr_k \in PCR_n$，则 $\mathcal{A}$ 获胜。敌手 $\mathcal{A}$ 获胜的概率表示为

$$SUCC_{\mathcal{A}}^{IH}(1^k) = \Pr[Game_{\mathcal{A}}^{IH}(1^k) = win]$$

$\mathcal{A}$ 获胜的条件是 i 能够作为 PCR_n 中的索引值，即 $pcr_i = pcr_k$，$pcr_k \in PCR_n$。

定义 6 如果 $SUCC_{\mathcal{A}}^{IH}(1^k)$ 是可以忽略的，则属性协商证明过程是可以保证信息隐藏的。

4.2 安全分析

根据上一节构建的安全模型对属性协商的远程证明过程进行安全性分析。

定理 1 属性协商远程证明是安全的，当且仅当证明过程满足不可伪造性和信息隐藏性。

证明：1. 不可伪造性

敌手 $\mathcal{A}$ 在进行 $Game_{\mathcal{A}}^{unforg}(1^k)$ 之前，首先需要初始化安全参数，这个过程是随机的。其生成能够使得 $\mathcal{A}$ 获胜的安全参数概率 $\varepsilon_1 \leqslant q^2/2^{ln}$，其中 q 表示协商轮数。接着，验证方 $\mathcal{V}$ 经过环签名算法的验证未发现敌手 $\mathcal{A}$ 伪造的 TPM 签名信息，该事件发生需要 $\mathcal{A}$ 知道 TPM 的身份私钥 sk，能够与签名公钥相匹配，其概率为 $\varepsilon_{TPM} = 1/pq$。敌手 $\mathcal{A}$ 伪造环签名信息，使得验证方 $\mathcal{V}$ 通过验证的概率为 $\varepsilon_{RING} = 1/(2^b)^{(r-1)}$，其中 r 为环签名成员数量。敌手 $\mathcal{A}$ 需要完成以上事件才能在游戏中获胜，其概率为 $SUCC_{\mathcal{A}}^{unforg}(1^k) \leqslant \varepsilon_1 \times \varepsilon_{TPM} \times \varepsilon_{RING}$，这个概率是可以忽略的，因而远程证明过程满足不可伪造性。

2. 信息隐藏性

敌手 $\mathcal{A}$ 进行 $Game_{\mathcal{A}}^{IH}(1^k)$ 时，首先发出安全属性需求，通过与验证方 $\mathcal{V}$ 进行 m 轮次的属性协商来解锁可能存在的加锁属性 $sp_{\mathcal{V}}$，其所表示的平台配置信息为 $PCR_n = \{pcr_1, pcr_2, \cdots, pcr_n\}$。$\mathcal{A}$ 能够在协商过程中解锁 $sp_{\mathcal{V}}$ 的概率为 $\varepsilon_{UNLOCK} = 1/m$。$\mathcal{A}$ 通过获取的属性 $sp_{\mathcal{V}}$ 验证平台配置信息获取 PCR_n 的概率是 $\varepsilon_{PCR} = 1/pq + 1/r$，其中 pq 为大素数乘积，r 为签名环成员数。$\mathcal{A}$ 从 n 个 pcr 值中输出索引值 i，其概率为 $1/n$。敌手 $\mathcal{A}$ 需要完成以上事件才能在游戏中获胜，其概率为 $SUCC_{\mathcal{A}}^{IH}(1^k) = \varepsilon_{UNLOCK} \times \varepsilon_{PCR} \times 1/n$，这个概率是可以忽略的。因而，远程证明过程满足信息隐藏性。

5 性能分析与实验

采用基于属性协商的远程证明方法不仅满足安全属性，而且相比其他几种常用的远程验证方法，具有效率和跨域访问等方面的优势。本节在对比其他几种远程证明方法的同时，采用 Hadoop 云计算平台验证了方法的有效性和可行性。

5.1 性能分析

为了对本文提出的基于环签名的远程证明方法(Ring-Sig)执行效率进行分析，用如下符号描述所涉及的运算与操作：E 表示指数运算；R 代表加密/解密运算(RSA)；P 表示双线性对运算；H 是 SHA 散列函数运算。在相同安全初始化参数的前提下与两种 DAA 远程证明方法(IDAA[13]和双线性 DAA[14])的验证效率进行对比，基于环签名的远程证明方法在计算效率上具有一定的优势。对比如表 1 所列。

表 1 效率分析

验证方法与参与者		加入阶段	签名阶段	验证阶段
双线性 DAA	HOST	6P	3E+ET+3P	0
	TPM	3E	3E	0
	VERIFIER	0	0	E2+E3+5P+(n+1)E
	验证中心	(n+2)E+2E2	0	0
IDAA	HOST	17E+22R	44E+31R	0
	TPM	11E+10R	9E+6R	0
	VERIFIER	0	0	37E+30R
Ring-Sig DAA	HOST	3E+H	H+(r+2)E	0
	TPM	E+H	r×R+H	0
	VERIFIER	0	0	H+ r×R

在表 1 中，双线性 DAA 中的 n 表示有非法证书的 TPM 数量，Ring-Sig DAA 中的 r 表示构成签名环的 TPM 数量。从这个效率分析表中可以看出，这 3 种 DAA 方法的运算效率是不同的。双线性 DAA 方法的运算速度比较慢，因为包含有指数次方级的运算和操作，同时还与参数 n 的可能取值有关。后两种方法的计算效率都不涉及过多的指数运算，

Ring-Sig DAA 方法的效率与签名环中的 TPM 数量 r 有关系，同时 SHA 算法也与散列表长度有关，在能够保证远程验证过程安全性的前提下，应该选取尽可能少的环成员。

与 2.2 节提到的其他两种远程证明方法相比较，采用环签名的属性协商的远程证明方法具有一定的性能优势。首先，环签名不需要第三方验证单元参与，可以根据其他 TPM 公钥构建签名环，降低了验证交互开销；其次，环签名计算类型简单，包括哈希运算、ASE 和 RSA 加密解密运算，计算复杂度相比其他两种验证方法有所降低；验证方对于环签名消息验证方法较方便，判断签名方平台可信性过程效率高。对比如表 2 所列。

表 2　性能对比

Property	Privacy-CA	DAA	Ring Sig-RA
第三方支持	强	弱	无
运算复杂度	一般	高	低
共谋攻击威胁	有	有	无
身份隐藏	一般	好	好
签名撤销	易	难	易
跨域验证	不支持	支持	支持

5.2　实验验证

为了能够更好地验证云计算环境下属性协商的远程证明的有效性和可行性，参考文献[2]中的可信云平台架构构建可信云计算模型，采用 Hadoop 作为实验平台（见图 3），利用 TPM 的功能模拟器 TPM-Emulator 代替 TPM 硬件，对跨安全域的服务资源进行可信验证。

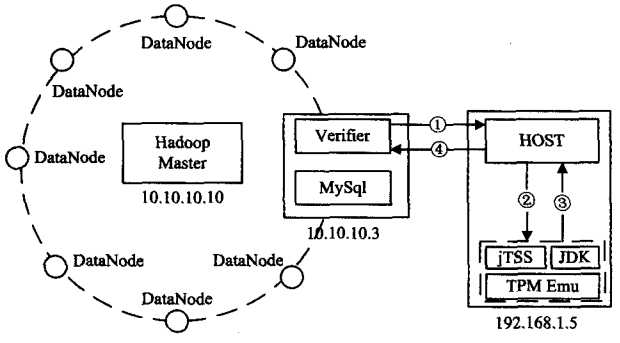

图 3　基于信任协商机制的 Hadoop 可信云平台

1. 平台配置

平台的硬件配置包括 106 个以 PC 和虚拟组织构成的节点组成局域网，千兆交换机 3 台。软件配置包括 ubuntu10.04（内核 2.6.32）；Hadoop 0.20.203 平台；TPM 模拟器 tpm_emulator-0.7.4；密码算法为 gmp-5.0.4；jdk1.6.0_26；TCG 软件栈 jTSS_0.6；数据库 Mysql1-4.4。

2. 实验方案与设计

在 Hadoop 平台的基础上，为每个节点部署 TPM 仿真环境来模拟可信计算架构。这个仿真环境由用来模拟硬件 TPM 功能的 TPM-Emulator 与交互接口 jTSS 和 JDK 组成。证明方所在环境与验证方所在环境是跨域的，彼此之间没有第三方验证中心进行身份鉴别。证明方节点 192.168.1.5 具有自身域内 TPM 公钥组成的签名环，验证方节点 10.10.10.3 也是如此，各自都根据身份验证安全强度维护签名环。根据 Master 节点的调度访问域外证明方节点，首先由验证方发起远程证明请求，然后按照协议进行交互，最后确定与域外证明方节点的信任关系。

3. 实验结果与分析

根据从证明方发起远程证明请求到确定双方信任关系的时间 t，通过 3 种远程验证方法和几种签名环生成方式在 Hadoop 平台上验证相同配置下远程证明的效率。实验结果如图 4 所示。

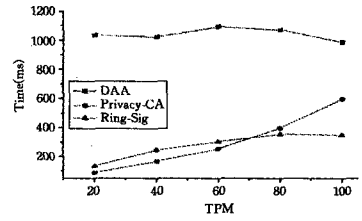

图 4　远程证明过程的实验结果

在 Hadoop 管理的安全域中包含的节点数（TPM 数量）与远程证明的效率有关。由于远程匿名证明方式与安全域中主机数量没有太大关系，它的时间开销主要来自于零知识证明过程和与验证中心、证明方的通信，因此时间开销基本稳定在 1s 左右。而对于 Pravacy-CA 远程证明方法来说，它的时间开销除了通信和计算，还有在验证中心进行自身公钥合法性验证中的查找时间。因而，其时间开销随着 TPM 数量的增加呈上升趋势。基于环签名的远程证明方法的主要时间开销来自签名环构建和环方程求解过程，安全域内节点较少时，其时间开销与 Pravacy-CA 相似。但是，随着节点数的增加，其时间开销增速明显趋缓。

为了评估属性协商过程中敏感信息保护对协商时间开销的影响，通过对每一轮协商过程所需时间来对 4 种属性集合部署方式下的协商效率进行验证。实验结果如图 5 所示。从实验结果中可以发现，敏感属性保护级别最低的 0-locked 部署方式协商时间开销最小。而保护级别最高的 6-locked 部署方式无法像其他几种部署方式一样收敛于 0ms，说明在有限次协商轮次中无法达到协商成功状态。属性集合中用于保护敏感属性的加锁证书数量越多，隐私保护程度越高，但是，协商效率会变得逐渐低下。在没有很好的协商策略保证的前提下，高比例的非自由属性组成的属性集合比较容易造成协商死锁状态。因此，在云计算环境中，为了兼顾敏感属性信息不被泄露，同时保证协商效率，需要考虑协商策略的设计和加锁属性的配置问题。

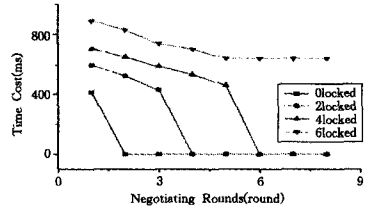

图 5　属性协商过程的实验结果

结束语　云计算环境下，服务资源的迁移和组合操作比较频繁，资源之间的信任关系不易评估和管理。通过对可信计算远程证明方法的研究，构建可信云平台来保障资源之间访问与调度的安全性。结合信任协商机制，通过属性证书的交互来建立域间资源的信任关系。通过在 Hadoop 下的实验验证了基于信任协商机制的信任验证方法的有效性和可行性。为更好地提高协商效率，防止敏感信息泄露，下一步研究计划围绕属性协商策略在信任建立过程中的作用展开，在分

析协商策略的基础上，能够在属性集合中找到最小非自由属性子集。

参 考 文 献

[1] Santos N, Krishna P. Towards Trusted Cloud Computing[A]// HotCloud'09 Proceedings of the 2009 conference on Hot topics in cloud computing, 2009[C]. CA, USA: USENIX, 2009: 22

[2] Armbrust, Michael, Fox, et al. A view of cloud computing[J]. Communication of the ACM, 2010(4): 50-58

[3] Trusted Computing Group. Trusted Computing Platform Alliance main specification version 1. 1b[EB/OL]. http//www. Trustedcomputinggroup. org, 2011-11

[4] Trusted Computing Group. Trusted Computing Platform Alliance main specification version 1. 2[EB/OL]. http//www. Trustedcomputinggroup. org, 2012-08

[5] Brickell E, Chen Li-qun, Li Jiang-tao. A New Direct Anonymous Attestation Scheme from Bilinear Maps[J]. Lecture Notes in Computer Science, 2008(4968/2008): 166-178

[6] Chen Li-qun. A DAA scheme requiring less TPM resources[J]. Lecture Notes in Computer Science, 2011(6151): 350-365

[7] 周彦伟，吴振强，蒋李. 分布式网络环境下的跨域匿名认证机制[J]. 计算机应用，2010(08): 2120-2124

[8] Haldar V, Chandra D, Franz M. Semantic Remote Attestation-A Virtual Machine directed approach to Trusted Computing[A]// USENIX Virtual Machine Research and Technology Symposium [C]. 2004

[9] Chen Li-qun, Löhr H, Manulis M. Property-Based Attestation without a Trusted Third Party[J]. Lecture Notes in Computer Science, 2008(5222): 31-46

[10] 刘吉强，赵佳，赵勇. 可信计算中远程自动匿名证明的研究[J]. 计算机学报，2009(7): 1304-1310

[11] Bender A, Katz J, Morselli R. Ring Signatures: Stronger Definitions, and Constructions without Random Oracles[J]. Journal of Cryptology, 2009(1): 114-138

[12] Zou De-qing, Du Shang-xin, Zheng Wei-de, et al. Building Automated Trust Negotiation architecture in virtual computing environment[J]. Journal of Supercomputing, 2011(1): 69-85

[13] 陈小峰，冯登国. 一种多信任域内的直接匿名证明方案[J]. 计算机学报，2008(07): 1122-1128

[14] Brickell E, Chen L, Li J. A New Direct Anonymous Attestation Scheme from Bilinear Maps[C]// LNCS 4968. Springer-Verlag, 2008: 166-178

(上接第 73 页)

参 考 文 献

[1] Xiong Li, Liu Ling. PeerTrust: supporting reputation-based trust for Peer-to-Peer electronic communities [J]. IEEE Transactions on Know ledge and D ata Engineering, 2004, 6(7): 843-857

[2] Kamvar S, ScholsserM, Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P netw orks [A]// Proc. 12 th Int'l World Wide Web Conf[C]. New York: ACM Press, 2003: 640-651

[3] Kamvar S D, Schlosser M T. EigenRep: Reputation management in P2P networks[C]// Lawrence S, ed. Proc. of the 12th Int'l World Wide Web Conf. Budapest: ACM Press: 123-134

[4] Colorni A, Drigo M, Maniezzo V. Distributed Optimization by Ant Colonies[C]// Proc of the 1st European Conf Artificial Life. 1991: 134-142

[5] Colorni A, Drigo M, Maniezzo V. An Investigation of some Properties of an Ant Algorithm [C]// Proc of PPSN '92. 1992: 509-520

[6] 窦文，王怀民，贾焰，等. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J]. 软件学报，2004, 15(4): 571-583

[7] 李俊青，潘全科，王文宏，等. 蚁群优化在 P2P 网络防范 DDoS 攻击中的应用研究[J]. 计算机应用研究，2009, 26(1): 339-341

[8] 于真，郑少峰，王少杰，等. P2P 信任模型研究[J]. 小型微型计算机系统，2009, 30(9): 1715-1719

[9] 李绍滋，王挺，周昌乐. 基于蚁群算法的非结构化 P2P 信息检索[J]. 计算机工程与科学，2009, 31(8): 99-103, 139

[10] 余智华. Peer-to-Peer 信任模型中的恶意行为分析[J]. 计算机工程与应用，2007, 43(13): 18-21

[11] 王新生，李学，贾冬艳. 基于蚁群算法的非结构化 P2P 资源搜索机制[J]. 计算机工程，2009, 35(7): 189-190, 194

(上接第 79 页)

[2] Vaze C S, Varanasi M K. The Degree-of-Freedom Regions of MIMO Broadcast, Interference, and Cognitive Radio Channels With No CSIT[J]. IEEE Transaciotns on Information Theory, 2012, 58(8): 5354-5374

[3] Nosrat-Makouei B, Andrews J G, Heath R W. User Arrival in MIMO Interference Alignment Networks [J]. IEEE Transactions on Wireless Communications, 2012, 11(2): 842-851

[4] Gui Xin, Kang Gui-xia, Zhang Ping. Linear Precoding Design in Multi-User Cognitive MIMO Systems with Cooperative Feedback [J]. IEEE Communications Letters, 2012, 16(10): 1580-1583

[5] Xie Xian-zhong, Zheng Pin-lian, Gang Qu. Delay-Tolerance SLNR Precoding to Mitigate Inter-cell Asynchronous Interference [J]. Journal of Jilin University (Information Science Edition), 2010, 28(1): 1-7

[6] Zhang Hong-yuan, Mehta N B, Molisch A F. Asynchronous Interference Mitigation in Cooperative Base Station Systems[J]. Wireless Communications, IEEE Transactions, 2008, 7(1): 155-165

[7] Lee K-J, Lee I. MMSE Based Block Diagonalization for Cognitive Radio MIMO Broadcast Channels [J]. IEEE Transactions on Wireless Communications, 2011, 10(10): 3139-3144

[8] Park H, Park S-H, Lee I. Weighted Sum MSE Minimization under per-BS Power Constraint for Network MIMO Systems[J]. IEEE Communications Letters, 2011, 16(3): 360-363

[9] 胡智伦，何世彪，张新春，等. 认知无线电中基于干扰温度的信道容量及中断概率[J]. 重庆理工大学学报：自然科学版，2010, 24(6): 83-88