# 基于信任的云计算身份管理模型设计与实现

李丙戌 吴礼发 周振吉 李华波
(解放军理工大学指挥信息系统学院 南京 210007)

**摘 要** 随着云计算的发展,身份管理问题已经引起业界高度关注。基于群签名的身份认证机制保证了云服务提供者不能通过外包的数据回溯用户的身份信息,并广泛应用于云计算环境的身份管理中,但它无法阻止恶意用户对云服务的非法访问。针对此不足,改进了现有的身份管理模型,将信任管理与群签名机制相结合,设计了基于信任的身份管理模型。本模型首先计算用户信任度并将其作为群签名分组的依据,再利用群签名机制实现用户认证,在应用中既能保证用户隐私,又能帮助云计算提供者保护资源。实验结果表明,本模型能有效识别恶意用户,帮助云服务提供者阻止恶意用户对资源的访问。

**关键词** 信任管理,群签名,身份管理,云计算
**中图法分类号** TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.09.033

## Design and Implementation of Trust-based Identity Management Model for Cloud Computing

LI Bing-xu WU Li-fa ZHOU Zhen-ji LI Hua-bo
(College of Command Information System, PLA University of Science and Technology, Nanjing 210007, China)

**Abstract** With the development of cloud computing, identity management issues of cloud computing have attracted great attention. Being widely used in cloud identity management, the identity authentication mechanism based on group signature guarantees that the cloud service provider cannot backtrack users' identity information through outsourcing data, but it cannot prevent a malicious user from accessing cloud services. To solve the problem, the paper designed an identity management model by integrating trust management with group signature mechanism. The model calculates the user's trustworthiness firstly, and then divides the users into groups according to the trustworthiness. At last, using the group signature mechanism, our model implements the authentication, which not only ensures user privacy in cloud but also helps the cloud providers to protect cloud services. Experiments show that the model can identify the malicious users effectively, and help the cloud service providers to prevent a malicious user from getting access to cloud services.

**Keywords** Trust management, Group signature, Identity management, Cloud computing

云计算的安全问题是阻碍其广泛应用的主要因素。云计算基础设施的组织模式,决定了其数据外包、多租户的特点[1],如图1所示。用户将桌面工作转移到云端,数据、软件、文档等都存储于不同的安全域。这些数据可能包含隐私信息,如病历、购物信息等,用户希望这些信息能保持匿名性。此外,不同用户的虚拟机可能驻留在同一个硬件节点,虚拟机间共享内存等资源,这为恶意用户对其他用户及云计算服务实施攻击提供了机会,而且虚拟机漏洞的存在使得攻击更容易实现。

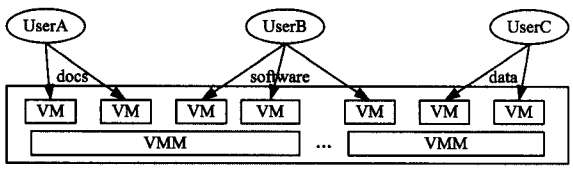


图1 云计算组织模式

传统的分布式系统则不具备以上特点,比如在Web服务模式中,数据并未外包,用户只将需要处理的数据交由服务提供方处理,接收处理后的结果如图2所示。向服务提供方发送的数据是可控的,且用户之间不存在冲突。因此,云计算比传统分布系统面临更多的安全威胁。

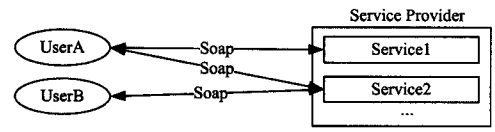


图2 Web服务组织模式

怎样在开放的、多租户共享的云计算运营模式中最大限度地保护隐私是一个值得研究的问题,然而云计算的开放性使得恶意用户很容易实施破坏[2]。解决该问题需要高效的、动态的、隐私保证的身份管理及授权,最好是将云计算模式下的身份管理以服务的形式向用户提供[3]。但现阶段基于云计算的用户身份管理主要集中于保护用户隐私,对恶意用户的识别方面则稍显欠缺。

到稿日期:2013-11-01 返修日期:2014-03-04 本文受江苏省自然科学基金项目(BK20131069)资助。
李丙戌(1982-),男,博士生,主要研究方向为网络安全,E-mail:libingxu_131@163.com;吴礼发(1968-),男,教授,博士生导师,主要研究方向为网络安全;周振吉(1985-),男,博士生,主要研究方向为网络安全;李华波(1981-),男,博士,讲师,主要研究方向为网络安全。

本文在身份管理模型中引入信任因素，设计并实现了适合云计算环境的基于信任的身份管理模型。该模型以群签名技术为基础，结合信任管理技术实现了用户信任度评估。在使用云计算服务时既能最大限度地保护用户隐私，也能有效识别恶意用户，降低了云计算服务提供者遭受攻击的可能性。

第1节对现阶段国内外针对云计算环境的用户身份管理研究进行了概述；第2节给出关于群签名及信任模型的预备知识；第3节对基于信任的身份管理模型进行了设计；第4节阐述模型实现，并进行了实验分析；最后进行了总结，并展望了下一步工作。

## 1 相关工作

随着云计算技术的快速发展，国内外学者对云计算环境下的身份管理进行了深入研究。文献[4]设计了基于用户属性的身份管理模型。用户首先向注册中心注册，当访问云计算服务时，由该注册中心返回签名的用户属性，用户将该属性提交给云服务提供者，根据该属性云服务提供者对该用户进行认证。文献[5]对文献[4]进行了改进，即注册中心只要在用户注册阶段保持在线即可，而无需永久在线。二者认证过程都利用零知识认证协议(Zero-Knowledge Proof Protocol，ZKP)实现了用户的匿名访问及隐私保护。文献[6]设计了基于实体的身份管理模型，摆脱了对于可信第三方的依赖。该模型能给云服务提供者最小限度的敏感信息，并能保证用户的匿名登录，实现零知识鉴别，最大限度保护了用户的隐私。该模型将云计算服务提供者的信任度作为重要的准入条件：用户需要访问某一个云服务提供者时，首先评估其可信水平，若该可信水平在用户可接受的信任门限之上，则可以进行进一步的交易，否则将终止交互。但该模型没有对用户的可信任水平进行评估，减少了对恶意用户的过滤，降低了该模型保护云计算提供者的能力。为了适应云计算动态、高效、经济的特性，Govinda 等人[7]设计了具有匿名性及保证数据安全的身份管理模型。该模型以群签名技术为基础进行数据的加密及签名。但该模型只适用于私有云的情况，因为在私有云中用户的数量相对固定。而在公共云中用户的数量、种类都是不可预知的，所以需要考虑适用于公共云的身份管理模型。

国内在云计算身份管理方面同样进行了研究。文献[8]概述了云环境下利用用户行为评估用户信任度的重要性及可行性，阐述了评估用户可信的标准。但该文献并没有就此展开详细论述，也没就此对基于信任的用户管理进行建模。文献[9]设计了实现隐私保护的访问管理模型，模型基于盲签名及哈希链的加密原型实现用户的隐私保护及验证，同时实现访问控制。模型通过注册、令牌获取、预认证3个阶段实现对用户身份的管理，在用户与云服务提供者之间使用会话密钥保障通信的安全。

以上研究重点都集中在用户隐私保护上，没有考虑开放环境下的用户可能存在恶意行为，使得系统较为脆弱，容易导致云计算提供者被攻击。

## 2 研究背景

### 2.1 信任管理

信任管理的概念最早由 M. Blaze 等人提出[10]，其承认开放系统中安全信息的不完整性，系统的安全需要靠第三方提供附加的安全信息。信任相关的定义还没有一个统一的标准，本文借鉴文献[11]，给出信任的相关概念。

· 信任：一种建立在已有知识上的主观判断，是主体 A 根据所处的环境，对主体 B 能够按照主体 A 的意愿提供特定服务的度量；

· 直接信任：是主体 A 根据与主体 B 的直接交易历史记录而得出的对主体 B 的信任；

· 推荐信任：是主体间根据第三方推荐而形成的信任，也称间接信任；

· 信任度：是信任的度量表示，也称可信度。

目前信任的研究可以分为两大类，即基于策略的信任管理和基于信誉的信任管理。前者根据一组安全凭证和安全策略来建立实体间的信任关系。后者是在对参与者不能充分了解的情况下通过询问相邻节点，依靠节点推荐及历史交互经验确定参与者信任度的机制。云计算用户的不可预知性，适合建立基于信誉的信任管理模型。当前典型的基于信誉的信任模型主要有 eBay 系统中的信任模型[11]、EigenTrust[12]、PeerTrust[13]、PowerTrust[14]。

### 2.2 群签名

群签名具有隐私保护和可追踪的双重特性，在现代电子商务中起着重要的作用[15]。群签名一般由6个随机多项式时间算法组成[15]：

构建：根据安全参数 $K$，群管理员(Group Manager，GM)生成一个可用于群签名验证的群公钥(Group Public Key，GPK)，以及用于生成成员证书及签名打开的一个群私钥(Group Secret Key，GSK)。

成员加入：用户和 GM 进行交互，用户加入群，并获得成员证书及私钥，用于群签名的生成。GM 获得追踪信息，供以后进行用户验证。

签名：群成员利用自己的证书及私钥生成任意一个消息的群签名。

签名验证：签名接收者获得 GPK、消息和消息签名，可验证此消息来自该群中成员，但不能找出实际的签名者；同时同一成员的不同签名之间没有可链接性。

签名打开：GM 能打开并找出实际的签名者。

成员撤销：GM 可撤销群成员的身份，之后该用户将不属于该群。

群签名所具有的优良特性只适用于云计算中对于用户隐私保护的要求，云计算中的安全保障不仅需要保证用户的隐私，还要保障云计算服务提供者不被恶意用户侵害。下一节将对该模型进行详细阐述。

## 3 基于信任的身份管理模型设计与实现

### 3.1 模型设计

基于信任的身份管理模型(Trust-based Identity Management Model，TIdM)在群签名技术基础上引入信任。依据用户表现及历史交互经验，计算出该用户的全局信任度，将该信任度作为群签名中对用户分组的依据。当用户对云服务提供者进行认证时，云服务提供者能根据群签名判断用户所处的

信任分组，从而提供给用户相应水平的服务，或采取相应等级的防范措施。该模型的基本框架如图 3 所示。

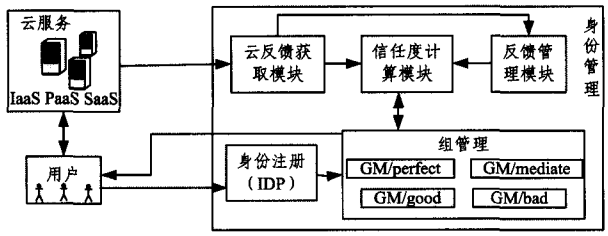


图 3　基于信任的身份管理模型框架

本模型共有 3 个参与交互的实体，即用户、身份管理中心、云服务。主要功能部件为身份管理服务，负责对访问云服务的用户实施集中式管理，包括用户身份注册、分组管理、信任度计算、云反馈获取、反馈管理等功能模块。将用户依据信任度分为 4 个组，分别为优（perfect（0.75－1.0]）、良（good（0.5－0.75]）、中（mediate（0.25－0.5]）、差（bad [0－0.25]），每个分组的管理员管理本组成员。模型实现以下多项式时间算法：

构建：$(PK_{gi}, SK_{gi}) \leftarrow setup_{gi}(1^k)$，其中 $k$ 为安全系数，$PK_{gi}$ 及 $SK_{gi}$ 分别代表对应第 $i$ 组管理员公钥及私钥。私钥由管理员保管，公钥则向公众公开。由“组管理模块”加以实现。

加入：$(SK_{Id}, C_{Id}) \leftarrow join(Id)$，根据用户 $Id$ 进行注册，产生用户证书及私钥。由“身份注册模块”及“组管理模块”完成。

签名：$signature \leftarrow sign(SK_{id}, C_{Id}, m)$，用户输入私钥、证书及时间戳 $m$，产生一个对于时间的签名。用户利用签名向云服务进行认证。

验证：$1/\perp \leftarrow verify(signature, m, PK_{gi})$，如果接受签名则输出 1，否则输出⊥。云服务方通过验证该签名，确定用户合法身份、新鲜性及具备的信任度。

评价：$T_c \leftarrow evaluate(signature)$，云服务根据用户行为给出评价。$T_c \in (0,1)$。“云反馈模块”将该评价值分成两部分，一部分进行计算，一部分进行存储。

信任度管理：$T_h \leftarrow history(T_c)$，将当前评价值进行存储，作为将来计算的参考值，“反馈管理模块”负责该管理功能。

信任度计算：$T \leftarrow compute(T_c, T_u, T_h)$，计算最终信任度，作为用户分组的依据。其中 $T_u$ 为用户最近的历史信任度。这次计算完成之后 $T_u$ 更新为 $T$ 的值。

打开：$Id \leftarrow open(signature)$，打开用户产生的群签名，还原用户 $Id$。

撤销：$1/\perp \leftarrow revoke(Id)$，撤销成员的组身份。

### 3.2　模型贡献

上节中的操作实现了用户的身份管理功能，其表现出来的一些性质主要来自于基于信任度的分组及群签名技术，具体表现如下：

匿名性：文中的签名利用文献[16]中的签名方案予以实施，并沿用文献中的符号。用户注册得到的证书 $C_{Id}=(A_i, e_i)$，在签名过程中将用户的证书嵌入到 $T_1$、$T_2$ 及 $T_3$ 之中，且 $T_1=A_i \times y^{\omega}$，$T_2=g^{\omega}$，$T_3=g^{ei} \times h^{\omega}$，$\omega$ 为用户选取的随机值。云服务在验证过程中无需解密 $T_1$、$T_2$ 及 $T_3$，这保证了用户匿名性。

权威性：利用群管理员公钥 $PK_{gi}$ 对签名进行验证。如通过，则证明用户来自于该群组，是经过该机构认证的合法用户。

可测量性：签名的验证利用对应的组的公钥，则可以确定用户的信任度范围。比如利用 perfect（0.75－1.0]分组的公钥进行的验证，则用户的信任度属于区间(0.75－1.0]。云服务可以据此进行进一步的安全策略。

动态性：用户的信任度通过 $T \leftarrow compute(T_c, T_u, T_h)$ 计算，其中每个参数都不是固定不变的。本次计算完成后 $T_u=T$，$T_h$ 是时间的函数，随着访问时间而变化，$T_c$ 是最新的反馈。所以用户的信任度会动态进行更新。

### 3.3　协议交互过程

用户首次访问云服务时，首先需要向身份管理中心进行注册，获得合法的身份及签名私钥。具体的过程如图 4 所示。其中第 4 步的“分配分组”将新注册用户的信任度设置为0.5，分配到信任级别为“中”的分组。这样分组是出于安全性的考虑，用户表现良好时会很快地进入到更高级的分组中，从而得到更优质的服务。

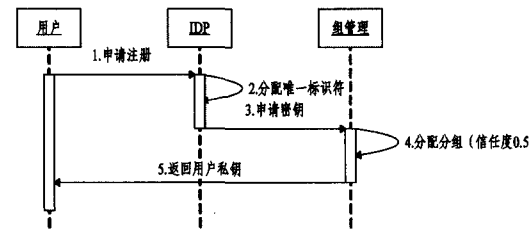


图 4　用户注册时序

用户在拥有了合法身份之后就可以按需访问云服务了，云服务根据用户的签名得知，用户是合法的并且属于某一个可信的分组。依据该分组的可信等级给用户提供相应的服务。详细过程如图 5 所示。

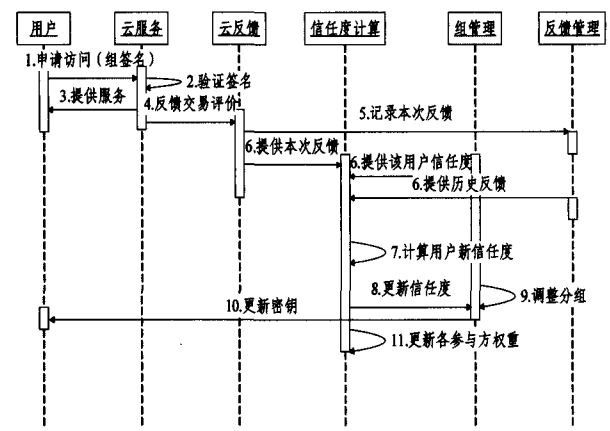


图 5　用户访问服务时序

图中需要说明的是，通过第 2 步的验证，可以确定该用户属于信任度较低的分组，为了最大限度地给用户提供服务，云服务端会根据本地的安全策略与用户进行进一步协商。云服务端会要求用户进一步提供可信的属性，以确定是否给该用户提供服务。这属于信任自动协商的研究范围，由于篇幅限制，不再赘述。图中第 7 步计算出的新信任度如果还处在原来的分组范围内，则不需要进行后续第 9、10 步的操作。

用户希望退出该系统时，则与 IDP 进行交互，由分组管理模块相应分组的 GM 对用户密钥进行回收销毁即可。

### 3.4 模型实现

为了验证提出模型的有效性，对原型系统予以实现。其中群签名主要借鉴成熟的 ACJT[16] 群签名方案实现。但由于 ACJT 不具备成员撤销的功能，因此借鉴了文献[17]给出的方法进行成员撤销。论文的主要工作在于实现了用户信任度计算及分组。

组管理模块依据用户的信任度对用户进行分组。3 个因子即 $T_c$、$T_h$、$T_u$ 决定了用户总体信任度，其中 $T_c$ 表示交易完成后云服务的反馈，$T_h$ 表示其他云服务对该用户的历史反馈，$T_u$ 表示在交易前用户的信任度。用户的信任度可表示为 $T=(W_c\times T_c)+(W_h\times T_h)+(W_u\times T_u)$，其中为了规范信任度的取值范围，$T_c$、$T_h$、$T_u$ 都在[0,1]之间取值。$W_c$、$W_h$、$W_u$ 分别表示云服务反馈权重、历史反馈权重、交易前用户信任度权重，在[0,1]之间取值并且满足约束 $W_c+W_h+W_u=1$，设置 $W_u$、$W_c$、$W_h$ 三者的初始值分别为 0.5、0.25 和 0.25。因为 $W_u$ 是 $T_u$ 的权重，所以它应当比其他权重都要大，但如果太大会影响其他信任度对实际信任度的反映，太小会在以后的交易中难以恢复，所以取一个中间值符合实际情况。$T_c$ 及 $T_h$ 在信任度计算中贡献相当，所以 $W_c$ 和 $W_h$ 初始值设置为相同，在以后的交易中会根据实际情况增减。$T_u$ 的初始值如上节所述设置为 0.5，而 $T_c$ 根据当次交易设定，$T_h$ 设置为 0，因为没有历史记录。$T_h$ 是根据众多历史反馈计算而得到的，而距离现在越远的反馈对现在的影响越小，假设权重 $W_c$ 的衰减速度与权重成正比。这样假设是符合实际情况的，比如开始权重较大则其衰减速度必然较快，距离本次交易的时间越久权重越小，其衰减速度也就越慢，该假设也是常用的时间衰减函数的假设。基于此假设可推导每一个历史反馈的权重随时间变化的衰减函数 $\frac{d\omega_c}{dt}=-\omega_c$，$\omega_c=Ce^{-t}$，其中 $\omega_c$ 指历史反馈应当具有的权重。该公式中常数 $C$ 是在 $t_0$ 时刻的权重值即 $W_c$，所以该公式就变成了 $\omega_c=W_ce^{-t}$。最终的用户信任度公式为 $T=(W_c\times T_c)+(W_u\times T_u)+W_h\times(\Sigma T_{ci}\times\omega_{ci})$，其中 $i$ 只是根据时间顺序对历史反馈进行排序而产生的记号，$T_{ci}$ 表示历史反馈的第 $i$ 个反馈，其实际值是该云服务在刚交易完成后的反馈，$\omega_{ci}$ 为依据衰减公式计算出的第 $i$ 个反馈权重。

以新的信任度为依据评估本次反馈及历史反馈的可靠程度，定义 $\delta\in[0,1]$ 作为对反馈的云服务进行奖赏或者惩罚的临界值。当 $|T_c-T|\leqslant\delta$ 时，对实施该反馈的云服务进行奖赏，否则进行惩罚。同样根据 $|T_u-T|$ 与 $\delta$ 的关系对用户交易前信任度进行奖赏及惩罚。这里 $\delta$ 的取值决定了整个系统是严格的系统还是比较宽松的系统，$\delta$ 取值过大时得到奖赏的条件比较宽松，大多数的反馈会得到奖赏，这样默认用户是可信任的，容易造成对恶意用户的误报；$\delta$ 取值过小时则惩罚过于严格，容易造成对用户的过度惩罚。模型中取 $\delta=0.5$，因为该值为整个取值区间的中间值，奖惩适中。当 $|T_c-T|\leqslant\delta$ 时，说明云服务的反馈较为可信，需要对其权值增加以示奖赏，即 $W_c=W_c^{|T_c-T|}$。当 $|T_c-T|\geqslant\delta$ 时，说明云服务的反馈失实，需要减少其权值进行惩罚，即 $W_c=W_c^{\frac{1}{|T_c-T|}}$。对 $T_u$ 的奖惩计算与上述过程类似，就不再赘述。

## 4 实验及分析

原型系统中签名功能的正确性及安全性依托于文献[16,17]，文献中给出了必要的证明，这里不再赘述。本节对新加入的关于信任度计算的功能进行测试，测试该系统是否能反映用户的真实信任度，从而识别出恶意用户。本实验设定了一个用户，一个身份管理中心，多个云服务的实验环境。实验采用墨尔本大学开发的云计算仿真平台 CloudSim[18] 模拟了 50 个云服务，部署了一个身份管理中心服务。设置以下场景进行测试，检验本原型系统对用户信任度计算的有效性。

场景 1　在系统初始化完成之后，用户从注册获得初始信任值开始，以不同的信任度分别随机访问云服务，记录系统将用户初始信任值调整到真实信任度需要的交易次数。为简单起见，在计算衰减函数 $\omega_c=Ce^{-t}$ 过程中，时间 $t$ 以交易的次数来衡量。这并不影响用户信任度最终的计算，因为只是把 $t$ 的随机性改成了定长。用户分别以真实信任度为 1、0.5、0 访问云服务，3 种情况下，每次交易完成后计算得到的用户信任度如图 6 所示。图中横轴为用户同云服务的交互次数，纵轴为每次交易完成后模型计算得到的用户信任度。

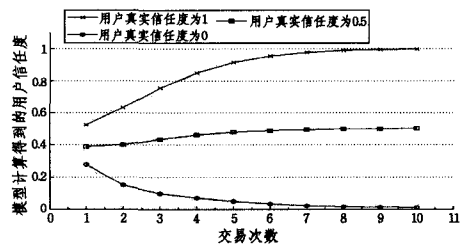


图 6　系统根据初始信任度调整计算信任度

图中 3 种情况下用户的初始信任度均为 0.5，在交易过程中模型计算得到的用户信任度逐渐趋向实际值，大约进行 6 次交易之后，计算出的信任度可近似等于用户真实信任度。当用户以真实信任度 0.5 进行交易时，第一次交易完成后信任度会稍有下降，然后再慢慢上升，这是因为一般云服务给出的反馈会低于用户的真实值，这也是模型慢增快减的体现。当用户以信任度 0 进行访问时，说明用户是恶意用户，系统同样能很快地计算出该用户的信任度，从而识别该用户的恶意身份。

场景 2　用户在访问云服务过程中其真实信任度会任意变化，系统能否及时进行调整，是检验模型有效性的又一指标。本次场景中模拟用户进行 50 次交易，进行了 3 次实验。1)用户真实信任度瞬间改变，每 10 次交易用户更改一次信任度，分别为 1、0、0.5、0.8、0.2；2)用户真实信任度从最小值逐渐平滑地递增，直到最大值；3)用户信任度从最大值逐渐平滑地递减，直到最小值。每次交易完成后计算得到的用户信任度如图 7 所示。图中横轴为用户同云计算服务交互的次数，纵轴为每次交易完成后模型计算得到的用户信任度。用户起始访问云服务时，系统首先设置用户信任度 0.5，所以图中曲线均是以信任度为 0.5 开始。随着用户真实信任度的变化，系统会很快地进行调整。无论是剧烈变化还是逐渐变化，模

型计算出的信任度都可大致反映用户真实信任度的变化趋势。

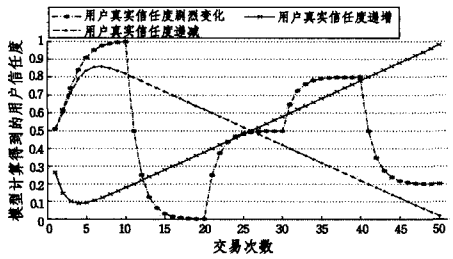


图 7　系统随用户信任度调整计算信任度

通过公式 $E=\sqrt{\frac{\sum_{i=1}^{n}(T_i-T_i^{real})^2}{n}}$ 计算系统的错误率，如表 1 所列，其中 $n$ 指交易次数，$T_i$ 指第 $i$ 次交易完成后由系统计算出的信任度，$T_i^{real}$ 指第 $i$ 次交易时用户的真实信任度。

表 1　系统计算信任度错误率

| 实验序号 | 错误率(%) |
|---|---|
| 1 | 8.23 |
| 2 | 3.05 |
| 3 | 3.08 |

由表 1 可看出，用户信任度变化激烈的时候系统的错误率较高，因为系统需要一定的过程才能计算较准确的信任度，计算偏差主要出现在这样的调整过程中。用户信任度平滑改变时系统的错误率较低，在实际可容忍的范围内。

上述两个场景的实验及分析表明，本系统计算的用户信任度是准确且有效的，能反映用户的真实信任度，所以能识别出信任度较低的恶意用户。云服务提供者可根据用户信任度提供相应等级的服务，实现对资源的保护。

**结束语**　文中结合信任管理及群签名的知识，设计并实现了一种适用于云计算的身份管理模型。该模型不仅能够有效地保护用户隐私，而且也使云服务能确定用户的可信范围，对云本身也起到一定的保护作用。

在模型中信任度计算与群签名机制是松散耦合的，增加了模型的处理过程，使得签名效率在一定程度上有所降低。设计基于信任的群签名机制，把信任度作为用户的一个重要属性，甚至是可以唯一标识用户的属性嵌入到群签名算法中，实现信任度计算与签名机制紧耦合，是下一步的研究方向。

## 参 考 文 献


[1] CSA. Cloud computing Architectural Framework[EB/OL]. Https://wiki. cloudsecurityalliance. org/guidance/index. php/Cloud_Computing_Architectural_Framework,2011-01-11

[2] 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

[3] Olden E. Architecting a Cloud-Scale Identity Fabric[J]. IEEE Computer,2011,44(3):52-59

[4] Bertino E,Paci F,Ferrini R. Privacy-preserving Digital Identity Management for Cloud Computing[J]. IEEE Date Engineering, Bulletin,2009,32(1):21-27

[5] Chow S S M,He Y J,Hui L C K,et al. SPICE-Simple Privacy-Preserving Identity-Management for Cloud Environment[C]// Applied Cryptography and Network Security. Springer Berlin Heidelberg,2012:526-543

[6] Angin P, Bhargava B, Ranchal R, et al. An entity-centric approach for privacy and identity management in cloud computing [C]//2010 29th IEEE Symposium on Reliable Distributed Systems. IEEE,2010:177-183

[7] Govinda K, Sathiyamoorthy E. Identity anonymization and secure data storage using group signature in private cloud[J]. Procedia Technology,2012,4:495-499

[8] Tian L,Lin C,Ni Y. Evaluation of user behavior trust in cloud computing[C]// 2010 International Conference on Computer Application and System Modeling (ICCASM). IEEE,2010,7: V7-567-V7-572

[9] Xiong J,Yao Z,Ma J,et al. PRAM:privacy preserving access management scheme in cloud services[C]// Proceedings of the 2013 International Workshop on Security in Cloud Computing. ACM,2013:41-46

[10] Blaze M,Feigenbaum J,Lacy J. Decentralized trust management [C]// 1996 IEEE Symposium on Security and Privacy. IEEE, 1996:164-173

[11] 李永军，代亚非. 对等网络信任机制研究[J]. 计算机学报，2010，33(3)：390-405

[12] Kamvar S D,Schlosser M T,Garcia-Molina H. The eigentrust algorithm for reputation management in p2p networks[C]// Proceedings of the 12th international conference on World Wide Web. ACM,2003:640-651

[13] Li Xiong,Liu Ling. PeerTrust:A Trust Mechanism for an Open Peer-to-Peer Information System[J]. IEEE Transactions on Knowledge Data Engineering,2004,16(7):843-857

[14] Zhou Run-fang,Huang Kai. PowerTrust:A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing[J]. IEEE Transactions on Parllel and Distributed Systems,2007,18(4):460-473

[15] 程小刚，王箭，杜吉祥. 群签名综述[J]. 计算机应用研究，2013，30

[16] Ateniese G,Camenisch J,Joye M,et al. A practical and provably secure coalition-resistant group signature scheme[C]// Advances in Cryptology—CRYPTO 2000. Springer Berlin Heidelberg,2000:255-270

[17] 陈泽文，王继林，黄继武，等. ACJT 群签名方案中成员撤销的高效实现[J]. 软件学报，2005，16(1)：151-157

[18] Calheiros R N,Rajiv R,Anton B,et al. CloudSim a Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms[J]. Software-Practice and Experience,2011,41(1):23-50