文章编号: 1006-2475(2012)09-0109-06

云计算信任管理研究

李 连,朱爱红,苏 涛

(海军航空工程学院,山东 烟台 264001)

摘要: 首先分析信任及信任管理相关概念,分类综述信任管理研究进展;其次,对信任管理相关技术进行分析和点评;最后结合云计算的特征,探讨现有信任管理技术存在的不足及云计算环境下信任管理的研究方向和研究重点。

关键词: 云计算; 信任管理; 策略; 声誉; 云模型

中图分类号: TP393 **文献标识码:** A **doi**: 10.3969/j.issn.1006-2475.2012.09.028

Research on Trust Management for Cloud Computing

LI Lian, ZHU Ai-hong, SU Tao

(Naval Aeronautical and Astronautical University, Yantai 264001, China)

Abstract: Firstly, this paper analyzes the related concepts of trust and trust management; then, some typical trust management models are introduced and compared. Finally, based on the analysis of the shortcomings and problems of the trust management in cloud computing, this paper discusses on the trend of research and applications of trust management.

Key words: cloud computing; trust management; policy; reputation; cloud model

0 引 言

云计算是一种基于互联网实现随时随地、按需、便捷地访问共享资源池的计算模式,资源虚拟化和服务化是其最重要的外部特征[1]。实际应用中,虽然云计算环境下服务资源非常丰富,但存在动态变化、自治性强、安全难控等特征,促使人们尤其关心云安全,云计算在提供服务的同时也将不可避免地出现诸如安全漏洞、恶意攻击等既有信息系统中普遍存在的共性安全问题。云计算中虚拟服务的规模化、集约化和专业化等特征决定了云计算中心可以实现集约化和专业化的安全服务,使得云计算安全程度大大提高。目前用户在使用云服务的过程中所关注的云安全焦点将会进一步转移到信任管理上来,传统的信息安全将会进一步发展为服务方和被服务方之间的信任和信任管理问题。可以说,人们普遍关心的云安全,实际上更多的是云计算中的信任管理[2]。

由于云计算环境下服务实体身份无法全部准确验证,并且由于缺乏公正且操作性强的评价机制,难以保障服务使用者快速有效地获得所需服务。信任管理技术能够使服务使用者从众多云服务中选择安全、有效、质优的服务,它通过在服务交互双方之间建立信任度的方法评估服务,帮助服务请求者选择正确的服务提供者,不仅保护了服务请求者的权益,而且促进了服务提供者的优胜劣汰。

信任管理的研究内容包括服务实体之间信任关系的描述、建立、验证和维护,涉及计算机科学、经济学、心理学和社会学等学科,其复杂性使得学术界至今仍没有达成统一的系统性认识。本文首先分析信任及信任管理相关概念,综述信任管理研究进展;随后对一些典型的信任管理模型分析和点评;最后,讨论云计算环境下信任管理的特点以及未来的研究方向和研究重点。

1 信任及信任管理

1.1 信任的定义及性质

由于研究的出发点不同,学术界对信任有不同的定义。例如,Farag Azzedin 认为信任是在某一特定内容范围内,根据实体行为所体现的可靠程度、安全程度、依赖程度等,对实体能力的坚定信念。D. Gam-

收稿日期: 2012-03-05

作者简介: 李连(1965-),男,山东淄博人,海军航空工程学院教授,博士,研究方向: 信息安全; 朱爱红(1968-),女,江苏扬中人,教授,博士,研究方向: 信息安全。

betta[3] 认为信任(或不信任)是评价一个实体执行一个特定行为的主观可能性程度,评价在对该行为进行监控(或根本不可能监控该行为)之前和与该行为对其自身行为产生影响的情况下进行。

信任具有如下性质:(1)信任具有上下文相关性。信任与上下文环境紧密相关,信任值应是针对特定的上下文环境而言的。(2)信任具有主观性。不同的用户实体对同一服务提供实体的评价因主观喜好的不同而不同。(3)信任是有条件传递的。在一定条件的约束下,信任是可传递的,通常信任会随着传递链路的增长而衰减。(4)信任具有动态性。实体之间的信任关系是不断变化的过程,随着时间、交互次数等不断变化而变化,每一次交互都会影响它们之间的信任关系。(5)信任具有可度量性。尽管信任具有不确定性和动态性,但可以根据一些外在特征加以量化和度量,其结果的精确程度与信任评估的方法有直接关系。

根据获取方式的不同,信任可分为直接信任和推荐信任。直接信任是用户实体与服务供应实体之间,因为直接的服务交互建立的一种信任关系;推荐信任是用户实体根据其他用户实体的推荐,与服务供应实体之间建立的一种信任关系。

1.2 信任管理的内涵与分类

1.2.1 信任管理的内涵

"信任管理"的概念由 M. Blaze 等人于 1996 年首次提出[3],即信任管理采用一种统一的方法描述和解释安全策略、安全凭证以及用于直接授权关键性安全操作的信任关系,内容包括制定安全策略、获取安全凭证、判断安全凭证集是否满足相关的安全策略等。M. Blaze 等人提出的信任管理本质是使用一种精确、理性的方式来描述和处理复杂的信任关系。而 D. Gambetta-A. Adul-Rahman 等学者却认为信任是非理性的,是一种经验的体现,可以通过评估实体间的历史交往经验,确定是否在实体间建立信任关系。A. Adul-Rahman 等人从信任的主观性入手提出了一些用于信任评估的数学模型[4],这些信任评估模型的功能包括:信任的表述及度量、信任度推导和综合计算等。

1.2.2 信任管理的分类

根据主体之间信任关系描述和获取方法,信任管理分为基于策略的信任管理和基于声誉的信任管理。

(1)基于策略的信任管理。

基于策略的信任管理利用证书验证的方法建立和验证信任关系。PolicyMaker 是 M. Blaze 等人开发的第一代信任管理系统[5],根据策略和凭证进行信任决策。策略和凭证都是完全可编程的,称为断言。在 PolicyMaker 的应用框架中,应用系统负责凭证的收集和签名验证,然后负责把凭证转换成 PolicyMaker 断言,并通过调用 PolicyMaker 的推理引擎进行授权决策。由于 PolicyMaker 只是一个实验性质的信任管理系统,只依据输入的参数进行判断,对凭证的收集及安全性验证交由应用系统负责,势必会加重应用系统的负担,并可能因凭证收集不全导致一致性验证失败。

KeyNote 是由 M. Blaze 等人开发的第二代信任管理系统,它在继承 PolicyMaker 的断言机制等核心思想和原则的基础上,对 PolicyMaker 的一些不足进行了改进;它在系统设计和实现上与 PolicyMaker 存在很大区别;它采用特定的断言语言描述策略和凭证,有利于促进信任管理系统的标准化并使其易于集成到应用系统中,而且由于无须应用系统负责凭证的签名验证,减轻了应用系统的负担。与 PolicyMaker 一样,它也存在因凭证收集不充分而导致的一致性证明失败问题。

REFEREE 是 Y. -H. Chu 等人开发的一个信任管理系统,旨在解决 Web 浏览安全问题。它采用与 PolicyMaker 类似的完全可编程的方式为 Web 客户和服务器提供了一个通用的政策评估机制和信任政策语言,根据策略进行凭证的收集和签名验证。其灵活的一致性证明验证机制一方面使其具有较强的处理能力,另一方面也导致其实现代价较高。

基于策略的信任管理适用于大规模分布式计算系统中的授权和访问控制,可以保护敏感资源或服务,但不能为请求者提供安全保护,故难以为分布式应用提供完整的信任管理解决方案。

(2)基于声誉的信任管理。

基于声誉的信任管理利用已有的历史经验和推荐经验对实体间的信任关系进行度量和评估,通过不断的证据收集和信任更新,能够较好地实现信任关系的动态管理。1994 年,Marsh 提出的信任计算模型被普遍认为是第一个比较全面、正式的信任模型[6]。Marsh 用重要性、效用、能力、风险、时间等变量来描述信任,并给出一种合成信任的方法。由于该模型需要确定很多变量,而在真实的情况下很难获得这些变量,实现起来比较困难。

基于声誉的信任管理根据信任值计算方法不同可分为两类[7]:基于局部声誉的信任管理和基于全局声誉的信任管理。全局信任管理综合网络中所有其他实体的看法,为网络中的每个实体计算一个全局

信任值,代表性模型有 EigenTrust、PeerTrust、PowerTrust 等; 局部信任管理通过询问有限的其他实体以获取对某个实体的信任评价,再结合自己和该实体直接交互的历史经验来确定该实体的信任值,代表性模型有 Richardson、FilmTrust、FIRE 等。

基于声誉的信任管理主要用于隔离恶意的服务或服务提供者,能保证请求者的安全,但不适合保护敏感服务或资源。

1.3　信任评估模型

信任管理涉及的关键技术主要有信任表述、信任度量和信任度评估等。目前信任值的表示方法有多种,有的用离散值表示实体的信任值,有的采用取值在 [0,1] 之间的概率值表示信任值,有的则采用模糊理论中的特征向量和隶属度等概念定量化描述实体的信任值,还有的基于灰色系统理论用灰类描述实体间的信任关系。近几年有学者提出基于云模型的信任表述方法,根据信任关系及其描述方式的特点,用云模型表述信任值[8]。而信任度评估就是根据数学模型建立的运算规则,在时间和观测到的证据上下文的触发下动态地进行信任值的重新计算,是信任管理的核心工作。根据信任的主观性特征,实体之间可以依据历史交往经验建立信任关系,通过信任评估技术可以对实体之间的信任值进行评估。本节将介绍一些著名的信任评估模型。

1.3.1　基于概率统计的信任评估模型

此类模型的基本思想是: 实体间历史交往经验中成功与失败的活动次数符合某种概率统计规律,根据这种规律可构建实体间的信任关系模型,典型代表为 Beth 模型。Beth 模型[8-9] 将实体间历史交往经验分为肯定经验和否定经验,根据信任是否由经验推荐将信任分为直接信任和推荐信任,并给出了信任度推导和综合计算公式,即以对实体完成任务的期望为基础,根据肯定经验和否定经验的次数计算实体能够完成任务的概率,此概率即为实体的信任度。Beth 模型的不足之处在于: 仅采用肯定经验度量信任关系,并采用简单的算术平均法综合多个推荐信任,无法很好地消除恶意推荐所带来的影响。

基于概率统计的信任评估模型将信任完全建立在精确的数学模型之上,将信任的模糊性等同于随机性,不能很好地反映信任的本质。

1.3.2　基于模糊逻辑的信任评估模型

信任是一种人类的认知现象,具有很强的主观性和模糊性。前面提及的基于概率统计的信任评估模型以概率模型对主观信任进行建模,这相当于是将信任的主观性和不确定性等同于随机性。为了更加准确地把握和反映信任的本质属性,唐文、陈钟等人提出了基于模糊集合理论的信任管理模型,用模糊集合理论中隶属度描述信任的模糊性,通过信任的综合评判获得信任向量,并将其作为信任度量机制。该模型的主要不足之处: 隶属函数否定信任的随机性,把模糊性作为信任的唯一特性来研究,而且因素评判矩阵的建立和各因素的权重分配均有很大随意性,模型评价机制复杂,实际应用可行性较差。

1.3.3　基于观念空间的信任评估模型

Josang 认为信任都可以用一种真或假的二值陈述来表示,但事实上由于知识上的不足与缺陷,有时候却很难对某些陈述得出真或假的明确结论。针对这个问题,Josang 引入事实空间和观念空间来描述和度量信任关系,并提供了一套主观逻辑运算子进行信任度的推导和综合计算。其中,观念空间用三元组 $w=\{b,d,u\}$ 表示,b、d、u 分别描述对陈述的信任程度、不信任程度和不确定程度; 事实空间由一系列实体产生的事件组成,分为肯定事件和否定事件。Josang 基于二项事件后验概率的 Beta 分布函数给出了一个由肯定事件数和否定事件数计算的概率确定性密度函数,并以此来计算实体产生的某个事件的概率的可信度。假定 r 为事实空间中的肯定事件数,s 为事实空间中的否定事件数,则 b、d、u 可分别表示为:

$$b=\frac{r}{r+s+1},\quad d=\frac{s}{r+s+1},\quad u=\frac{1}{r+s+1}$$

与 Beth 模型相比,该模型对信任的定义比较宽松,使用推荐算子计算信任度。该模型的不足之处: 该模型虽然使用事实空间和观念空间从多方向描述和衡量主观可信的关系,但只是将随机性等同于模糊性,没有完全反映信任的模糊性特点; 并且由于不区分直接信任和推荐信任,采用统一的方法计算信任度,无法有效消除恶意推荐带来的影响。

2　云计算信任管理面临的挑战

与传统的安全授权机制相比,信任管理具有灵活性、可扩展性以及可靠性等特点,适用于开放、自治、异构的云计算中的授权问题。由于云计算的开放、动态和自治的本质,云环境中存在大量不可靠的服务和欺诈行为,造成了实体间交互安全和服务质量的不确定性。建立有效的信任管理模型,能够补偿云计算内在的不确定性,降低服务交互风险,提高服务的可信性。但目前云计算信任管理面临诸多挑战:

(1) 信任模型的多样性导致信任管理和信任评估方法的不兼容性。近年来,众多学者在不同的研究

背景下采用不同的数学方法提出了各自的信任模型，有的基于普适计算环境，有的基于网格环境，有的基于 P2P 网络，其信任获取、信任传递和信任评估方法在不同的数学理论框架下，表现形式各有不同，存在着很大的不兼容性。至今尚没有提出一套完整的基于云计算环境的信任管理模型，能够安全地实现云计算环境下信任值的安全存储、分发、访问和更新。

(2) 现有的信任管理模型动态性较差。由于云环境边界的动态变化，各服务实体在动态地进出，服务实体间的信任关系随机建立，随着时间变化而动态变化，具体表现为两个方面：①实体提供服务的动态性。一个实体可能通过提供大量的可信服务获得较高信任值，然后因为提供了一些恶意或虚假的服务，使得其信任值降低。②推荐可信度的动态性。一个服务实体可能通过大量诚信推荐获得较高的推荐可信度，然后提供虚假推荐。目前的信任管理系统大都只解决了静态信任管理，而忽略了信任管理的动态性。

(3) 集中式的信任管理模型已经不适应云计算环境。在传统的网络环境(如 Internet) 中，信任关系的建立依赖于可信的第三方，采用集中式信任管理模式，一般以 Web 服务注册中心为基础添加一个管理信任和声誉的机构，这种模式的好处就是实现简单。然而，云计算环境中很可能没有一个全局控制中心，或者同时有多个控制中心，建立集中式信任管理系统存在一定困难。此外，集中式的信任管理往往会伴随着额外的费用和开销，当云计算服务实体规模较大时，需要具有很强计算能力的计算机或集群才能满足全局信任和信誉实时评估的需求，影响系统的扩充；而且集中式信任管理易于被攻击，信任管理控制中心的崩溃会导致信任管理系统的崩溃，所有与之相关的服务都会出问题。

(4) 跨域的信任管理模型研究不够深入。云计算环境中进行交互的服务实体可能处于不同的信任域，并遵循不同的安全策略。一方面由于信任域隶属于不同管理机制，跨域级的信任无规范，域间信任度不统一，域与域之间无法比较；另一方面跨域调度的评价都采用送回原实体所在域，无法避免原信任域在管理上协同作弊的问题。针对上述问题，需要研究实现一种域间信任评价模型，解决不同信任域间的信任评价与转换。

3 云计算信任管理的发展方向

针对云计算信任管理面临的挑战，结合云计算特点，本文认为云计算信任管理的主要发展方向有以下几个方面：

3.1 统一规范的信任信息描述机制

云计算环境中服务实体的信任信息所蕴含的内容极其丰富，而且与应用的上下文密切相关。由于不同的信任信息描述方法导致的信任模型不兼容性极大影响了信任管理系统的实现和应用，因此需要采用一种统一、通用的方式来规范地描述信任信息。可以基于现有的信任描述方法，研究相对简单、完备有效且自适应能力强的信任描述方法，使其兼具各描述方法的优点并满足应用需求。由于云计算中的安全性需求动态变化，服务实体的信任度也随之动态变化，需进一步研究云计算中动态信任关系的收集、表述、度量、评估理论和方法，并结合其他学科的知识，继续探索适合描述信任关系的新模型。

3.2 基于云模型的信任管理

信任是一个抽象的心理认知，当实体之间的信任关系不能明确定义的时候，它是不稳定、模糊和随机的，因此建立一种具有直观、简洁语义并能反映实体信任模糊性的信任管理模型是信任研究的一个基本问题。

云模型是一个很好的解决不确定性问题的方法，于 20 世纪 90 年代初由李德毅院士提出，它能将不确定性概念中的模糊性和随机性有机地结合起来，实现定性概念和定量数值间的不确定性转换[10-12]。将云模型引入信任管理领域，可以客观地反映信任的模糊性和随机性本质，能较为科学地解决本文 1.3 节介绍的各种信任评估模型存在的不足，开辟一个信任管理的新方法，不仅能兼顾主观信任的不确定性和模糊性，并能在信任的定性表示和定量表示之间架起一座桥梁。应用云模型解决云计算环境下的信任管理问题，通过对云模型进行扩展可得到信任的量化、推理算法，灵活直观，能很好地体现人类的思维特征和习惯[13]。

目前这一领域的研究尚处于初级阶段，有很多亟待研究的课题，下一步的研究重点主要有：进一步研究信任之间的关系，研究信任关系的合理度量方式，分析云计算中的信任联系；研究如何提高模型的实用性和可操作性；研究如何在具体的环境中根据实体的交互构建合适的信任云；研究如何利用信任云进行信任决策等。

3.3 跨域的基于策略和信誉的信任管理模型

基于策略和基于信誉两种信任管理具有很强的互补性。基于策略的信任是一种理性信任，在计算机的安全技术发展中，认证、授权、访问控制等都可以看

作是基于策略的信任。而基于信誉的信任是一种感性信任,取决于经验并随着服务实体行为的结果变化而不断修正。基于信誉的信任管理试图通过模拟人类社会中的交互和信任关系,在计算机世界中建立起一种量化的互信关系,从而可以辅助决策制定。目前的大多数信任管理都将两者分离开,单独进行信任关系处理,无法提供全面的信任评估功能。综合两种机制的研究将是云计算信任管理的研究方向。

基于策略和信誉的云计算信任管理模型应既考虑证书的属性信任,又考虑经验信任评价、时间因素、交易次数等影响因素,并增加信任反馈机制,使得对信任的评价随着时间和经验动态变化,既能够防止恶意评价和合谋欺骗的攻击,又能激励服务提供方提供更好的服务[14]。考虑到云计算中服务的请求方和提供方可能分属不同安全域,安全策略也可能不同,针对跨域分层的信任管理系统应是研究重点。具体研究内容包括:

(1) 信任建模。对云计算中动态信任关系的相关性质、信任的表述、信任模型设计、信任度计算与评估等方面进行理论上的研究。考虑实体拥有的证书产生的信任、实体间直接交易产生的直接信任以及其他主体的推荐信任,将云环境中的信任分为属性信任、直接信任、推荐信任、上下文信任,并确定信任之间的关系具有单向性、条件性传递的特点,建立信任的模型。

(2) 信任度的计算方法。由于跨域的信任管理模型既要处理同一域内的实体信任量化和评估,又要处理不同域的实体信任量化和评估问题,所以首先要确定域内信任量和域间信任量的计算公式。此外由于信任关系可分为属性信任、直接信任、推荐信任和上下文信任等多种类型,因此各类信任度计算方法的确定非常重要。具体研究内容包括各种信任度权值的确定,交易次数、时间等影响因子的确定,对恶意行为的惩罚因子的确定,综合信任度的计算公式的确定等。

(3) 信任反馈和惩罚机制。云计算中服务实体间的信任信息不是一成不变的,而是随着信任关系的改变而改变的,因此需要对实体信任信息进行实时更新和反馈。现有很多信任模型缺乏反馈机制,在信任传递过程中,缺乏有效的计算服务信任传递和反馈信任传递的方法,严重影响了信任传递的可靠性和有效性。同时由于缺乏激励与惩罚机制,造成获取推荐信任困难,恶意推荐大量存在。为打击恶意推荐和共同欺诈行为,需要分析各类恶意攻击行为的特征,确定信任值的区间分类特性,设定适当的阈值,识别信任是正常还是何种恶意攻击,并生成反馈信任度和惩罚因子,动态调整信任度值。

(4) 跨域的信任管理模型。云计算中服务资源数量众多、种类丰富,服务提供者与请求者之间的关系可能是动态变化、异构和跨域的。信任管理控制中心应能够根据安全策略快速地处理实体的访问请求,建立包括信任信息收集、信任管理系统、信任信息综合处理机制、信任评价与反馈机制在内的信任管理模型架构。可将云计算中的信任关系分为上下两层,上层是域间信任关系,下层是域内信任关系。在划分信任域时,可将采取相同管理策略或有相似资源的实体放到同一个域中,这样可以有效地减少网络的通信,降低系统的成本。

3.4　跨域的基于信任管理的角色访问控制机制

由于云计算环境中可能没有一个全局控制中心,或者同时有多个控制中心,用户、角色以及权限之间的分配关系难以管理,并且云计算实体的权限管理有很多不确定性,而信任是处理不确定性的一个较好选择。此外,传统的 RBAC 隐含采用静态的信任关系,一个实体要么完全信任另一个实体,要么完全不信任,与现实应用的情况并不相符,因此传统的 RBAC 不能解决云计算中的授权与访问控制问题。

为解决云计算的授权与访问控制问题,可以考虑综合 RBAC 和信任管理的各自优点,将信任管理与传统的 RBAC 访问控制机制相结合[15],引入信任等级概念,根据用户所属的信任等级动态调整用户的角色,实现权限的动态分配; 并针对域内和域间的不同特点,基于域中心服务器,实现一个跨域的基于信任管理的 RBAC 访问控制架构。新的访问机制对角色进行扩展,增加信任度信息,每个赋予该角色的实体进行交易后根据信任度值的动态变化而分配新的角色,通过采用动态度量用户的信任级别来对角色实施授权委托约束,能进一步细化授权控制粒度,有效降低威胁风险,而且实现跨域的访问控制,为云计算的各种资源提供完善的安全保护。在具体设计与实现时要重点解决加入信任信息的角色形式定义、域间角色转化技术、域间策略集成技术等科学问题。具体研究内容包括:

(1) 加入信任度信息以及信任级别的 RBAC 模型的建立。具体包括: 模型中用户属性集、会话实例集、信任级别集、会话历史集、权限集、约束集等基础语义的形式定义,模型中信任级分配、角色信任级分配、信任角色分配等授权规则的形式定义。

(2) 结合信任管理模型,实现基于信任级的角色

授权过程。计算角色实体的信任度,根据实体的信任度所属信任等级设置访问控制策略,即由信任级对角色分配关系实施约束,通过信任级动态调整角色权限分配关系,用户信任级别的改变直接影响到用户的权限分配,从而利用带信任信息的角色关系进行更细粒度的授权管理,有效地解决服务资源的动态访问控制问题。

(3)针对域内和域间的不同特点,基于域中心服务器,实现一个跨域的基于信任管理的 RBAC 访问控制架构。

4 结束语

云计算的核心模式是服务,服务的前提是用户和服务提供方建立信任。本文对信任管理和信任评估技术的研究现状进行了分析和总结,指出了它们的优势与不足,结合云计算的特征,探讨了云计算环境下信任管理的研究方向和研究重点。

参考文献:

[1] Wikimedia Foundation Inc. Cloud Computing [EB/OL]. http://en.wikipedia.org/wiki/Cloud_computing, 2009-05-23.

[2] 李德毅,陈桂生,张海粟. 云计算热点问题分析 [J]. 中兴通讯技术, 2010,16(4):1-4.

[3] 汪永好,曾广平,肖超恩,等. Internet 应用安全中的信任研究与进展 [J]. 计算机科学, 2010,37(9):28-31.

[4] 徐锋,吕建. Web 安全中的信任管理研究与进展 [J]. 软件学报, 2002,13(11):2057-2064.

[5] 刘鹏,刘欣,陈钟. 信任管理研究综述 [J]. 计算机工程与应用, 2004,40(32):39-43.

[6] 张宇,陈华钧,姜晓红,等. 电子商务系统信任管理研究综述 [J]. 电子学报, 2008,36(10):2011-2020.

[7] 官尚元,伍卫国,董小社,等. 开放分布式环境中信任管理综述 [J]. 计算机科学, 2010,37(3):22-28,35.

[8] 田俊峰,蔡红云. 信任模型现状及进展 [J]. 河北大学学报:自然科学版, 2011,31(5):555-560.

[9] 王惠芳,朱智强,孙磊. 分布式网络系统中的信任研究 [J]. 计算机工程, 2008,34(1):10-13,16.

[10] 顾鑫,徐正全,刘进. 基于云理论的可信研究及展望 [J]. 通信学报, 2011,32(7):176-181.

[11] 周伟,许峰,韦琳. 基于云模型的电子商务信任机制的研究 [J]. 计算机技术与发展, 2011,21(3):165-169.

[12] 韦凯,刘欣欣. 基于云模型的网格用户主观信任管理模型 [J]. 华南理工大学学报:自然科学版, 2011,39(2):81-87,94.

[13] 陈倩,宋俊杰. P2P 网络下信任模型研究 [J]. 计算机与现代化, 2011(10):88-92.

[14] 孙秋景,曾凡平. 一种信誉机制与云模型相结合的 P2P 环境信任模型 [J]. 小型微型计算机系统, 2010,31(7):1328-1332.

[15] 戴常英,张会娟. 基于信任度的 Web 服务跨域访问控制 [J]. 计算机工程与科学, 2009,31(8):42-45.

(上接第 75 页)

参考文献:

[1] 安国国际科技股份有限公司. AU6437 USB2.0 Single-LUN Flash Card Reader Controller Technical Reference Manual V1.08 [R]. 安国国际科技股份有限公司, 2012.

[2] Terminus Technology Inc. FE1.1S USB 2.0 High Speed 4-Port Hur Controller Data Sheet [R]. Terminus Technology Inc., 2010.

[3] Terminus Technology Inc. FE1.1S USB 2.0 High Speed 4-Port HUB Controller Product Brief [R]. Terminus Technology Inc., 2008.

[4] Terminus Technology Inc. FE1_1s_B_SSOP28_V1_0 [R]. Terminus Technology Inc., 2008.

[5] 零点工作室,刘刚,彭荣群. 精通 Protel DXP 2004 SP2 原理图与 PCB 设计(第 2 版) [M]. 北京: 电子工业出版社, 2011.

[6] 萧世文,宋延清. USB2.0 硬件设计 [M]. 北京: 清华大学出版社, 2006.

[7] 许永和. USB 外围设备设计与应用 [M]. 北京: 中国电力出版社, 2002.

[8] 张宏. USB 接口设计 [M]. 西安: 西安电子科技大学出版社, 2002.

[9] 胡晓军,张爱成. USB 接口开发技术 [M]. 西安: 西安电子科技大学出版社, 2005.

[10] 孟令许,解振东. 基于 GL850A 的 USB HUB 的设计及应用 [J]. 仪器仪表用户, 2012,19(2):59-61.

[11] 杨英,詹克团,袁国顺. 一种全速 USB 集线器的设计 [J]. 微电子学与计算机, 2005,22(3):128-130,135.

[12] 张宁. 简单自制 USB HUB [J]. 大众硬件, 2004(9):128.

[13] 邵小桃,蒋延生,汪文秉. 一种新型 USB2.0 高速集线器的设计与实现 [J]. 微型机与应用, 2003,22(7):22-24.

[14] 陈乃塘. USB HUB 装置的架构剖析 [J]. 电子测试, 2005(1):44-50.