移动云计算中的信任建立问题研究

郎为民，姚晋芳
（解放军国防信息学院，湖北省武汉市 430010）

摘　要　信任建立的目标是确保数据的可信、真实、可靠和忠诚。在移动云计算中，由于数据存储和数据处理是在云端以远程方式进行的，因而信任是移动云计算安全中一个非常重要的参数。文章讨论移动云计算中的信任含义、特征、类型，研究弱信任链、控制和可视化缺失等信任相关问题，探讨服务级协议、审计、测量与评级、自评问卷、信任和声誉模型等 5 类信任建立方法，最后分析黑盒、由内向外以及由外向内等信任评价方法。

关键词　移动云计算；信任建立；信任类型；信任评估

0　引言

云计算是一种新兴的计算范式。它能够在 IT（信息技术）预算中节省大量成本。根据国家标准与技术研究院（NIST）的标准[1-2]，云计算是一种用于实现对可配置计算资源（如网络、服务器、存储、应用和服务）共享池的便捷、按需网络访问的模型。在管理成本最小或与服务提供商交互最少的情况下，这些资源能够被快速提供和发布。

云计算具有一些很好的特征，如投资低、易于维护、灵活性高、快速部署、服务可靠、可用性和可扩展性好、按使用量付费的模式、弹性好、类型广泛的网络平台和多租户等。存在着 3 种云服务模型：SaaS（软件即服务）、PaaS（平台即服务）以及 IaaS（基础设施即服务）。

移动云计算是云计算与移动设备、移动网络的集成。因此，移动云计算提供了比云计算更好的移动性。它通过移动设备来使用云计算技术。基本上，移动云计算中的数据存储和数据处理操作都发生在移动设备之外的基础设施中。虽然云计算和移动云计算似乎具有很大的吸引力，但它们在大多数地方仍然不受欢迎。这背后的主要原因之一就是信任问题。信任是云计算、移动云计算、传感器网络、移动自组织网络和电子商务相关领域面临的主要挑战。

根据词典的定义，信任意味着对某人或某物的可靠性、可信性、真实性、有效性、忠诚度或能力的坚定信念。信任为我们提供了对事物按预期行动或实施的信心和依赖。我们信任一个知根知底且按照我们期望行事的系统。如果一个系统为我们提供的服务相关信息不足，且运行不安全，则我们不会信任该系统。

信任问题是云计算发展面临的最大障碍之一。2010 年，富士通研究所在一项调查中发现，88%的潜在云消费者会担心他们的数据安全。云消费者总是担心谁可以访问他们存储在云服务器中的数据，他们想要更多地了解后端物理服务器上所发生的情况。这种调查表明，从业人员和研究人员迫切需要迅速消除信任障碍。

云服务提供商和云消费者之间的信任度对于人们广泛接受移动云计算非常重要。云服务提供商必须评估和鼓励可信客户并从系统中删除恶意客户。这将使他们能够提供可靠和有效的服务。云消费者还应该选择可信的云服务提供商并避开不道德的云

基金项目：国家自然科学基金资助项目“节能无线认知传感器网络协同频谱感知安全研究”（编号 61100240）。

服务提供商。为了赢得消费者的信任，云服务提供商必须提供更高的透明度、赋予消费者更大的数据和流程控制权以及明确的安全规定。为实现移动云计算在全球范围内的有效部署，在云服务提供商和云消费者之间建立可信赖关系是一项必要条件。如果移动用户不信任云服务提供商，并使自己远离云计算服务，则整个移动云计算技术将变得无用。

1　信任特征

信任具有如下重要属性[3]：

a)信任是与域相关的。在不同的应用领域中，信任具有不同的属性。所以，应当将信任的内涵局限在若干个具体域中。

b)在数学意义上，信任是不对称的。如果实体 X 信任实体 Y，则不意味着实体 Y 也将信任实体 X。

c)信任不具备可传递性。这意味着，如果实体 X 信任实体 Y，实体 Y 信任实体 Z，则无法保证实体 X 信任实体 Z。

d)信任可能会动态发生变化。例如，随着云服务提供商性能和服务质量的变化，云消费者可能会对特定云服务提供商的信任度进行动态调整。

e)信任是关于实体的概率值，且它通常在 0 和 1 之间的实数范围内变化。在初始条件下，信任值通常为 0.5。

f)信任是多维的。一个典型实例是我们在电子商务中计算交易实体的信任值。这里，可以使用诸如产品质量、产品价格、产品交付速度等信任属性来估计信任值。

g)信任是对某一实体的个人看法。不同的人可能拥有不同的背景，他们对单一实体可能拥有不同的评价标准。因此，针对同一系统或实体，置信水平可能会因人而异。

2　信任的构成

我们可以将信任组件划分为安全性、隐私、可审核性和可追责性。

2.1　安全性

安全性使得未授权人员或黑客访问机密信息或资源变得困难或不经济。加密技术就是一个例子。

2.2　隐私

隐私是每个人的基本权利。隐私技术主要用于防止个人数据泄漏或曝光。

2.3　可审计性

可审计性是评估组织、系统、过程、项目或产品的能力。审计是指为了特定目标，对系统或企业的运营、报表、数据、记录和性能进行系统检查的活动。在审计过程中，审计人员收集证据，对其进行评估并做出判断，最终通过审计报告与被审计单位进行沟通。审计一般由独立实体来执行。

2.4　可追责性

可追责性保证个人、系统或进程所执行的所有操作都可以被唯一标识，并能追溯到作者和操作。它又被称为可追溯性。

3　信任类型

从广义上讲，存在着 3 种类型的信任[5]：直接信任、间接信任和混合信任。

3.1　直接信任

如果某个实体通过直接关联或直接通信来信任另一个实体，则我们将此类信任称为直接信任。在图 1 中，实体 X 和实体 Y 直接进行交互。

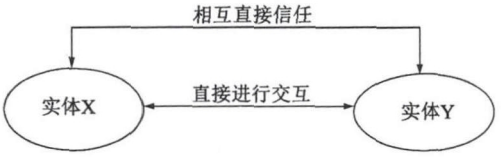

图 1　直接信任

3.2　间接信任

某个实体可以基于其他人的建议来间接信任另一个实体。如果两个实体没有直接关联且通过第三方实体相互了解，则可能产生此类信任。当两个实体先前没有交互时，可能需要间接信任。因此，可以基于观测值和推荐值来计算信任值。在图 2 中，节点 Z 基于可信实体 X 的推荐对 Y 产生了间接信任。

3.3　混合信任

混合信任是基于直接经验和推荐信息来计算的，如图 3 所示。这里，实体 Z 直接信任实体 Y 和实体 X。此外，实体 X 推荐实体 Z 来信任实体 Y。因

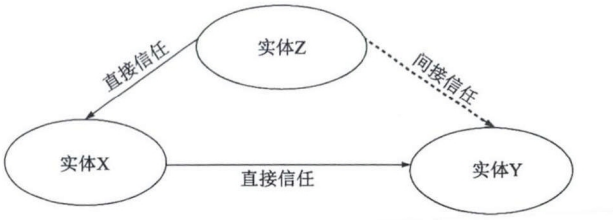

图 2 基于推荐的间接信任

此，实体 Z 也可以间接信任实体 Y。最后，我们可以说实体 Z 对实体 Y 拥有混合信任。

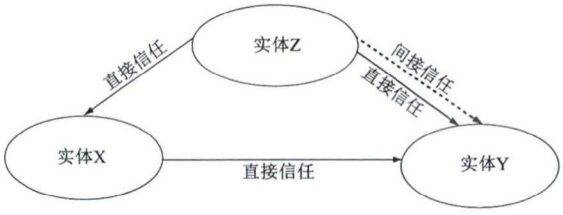

图 3 从实体 Z 到实体 Y 的混合信任

4 信任相关问题

信任难以培养，但很容易丧失。一个简单的错误可能会破坏多年建立起来的信任。声誉和品牌形象都是信任的重要参数。通常，安全性和密码学水平增加了通信系统的可信度。弱信任链、控制和可视化缺失都是与信任相关的问题[6]。

4.1 弱信任链

云服务提供商和客户之间可能还存在着分包商。云服务提供商需要通过这些分包商向客户快速提供所需的服务。这些分包商甚至还有可能与其他人签订合同，这些人的身份、声誉和可信度并未做到核对无误，原因可能是截止日期或时限。然而，在这一分包商链中，可能无法保证协议得到恰当合法的遵守。客户可能不知道所有的分包商，甚至他们可能对服务链一无所知，这就导致了弱信任链的产生。

4.2 控制和可视化缺失

客户不知道谁将处理他们的个人信息，以及他们的数据是否在云中得到了充分的保护。这种控制和可视化缺失会产生不信任，最终客户将自己置于云域之外，尤其是当涉及到敏感信息时。

5 信任建立方法

存在一些能够协助消费者确定可信或可靠云服务提供商的方法。我们可以将这些方法分为服务级协议、审计、测量与评级、自评问卷、信任和声誉模型等类型[7]。

5.1 服务等级协议

服务等级协议是建立对云服务提供商信任的一种方式。服务等级协议能够说明云服务提供商可以提供什么、具备什么特征、采用何种安全机制、能够满足哪些实际担保等内容。在移动云计算环境中，用户对违反服务等级协议的行为进行监控，并可以向云服务提供商申请补偿。遗憾的是，虽然服务等级协议近期已经实现了标准化，但是它们远未实现。云服务提供商充分利用了这一现状。他们采用可以剥夺客户获得赔偿的方式来使用服务等级协议。

5.2 审计

许多审计标准是可用的，不同的云服务提供商使用不同的审计标准，如 FISMA（联邦信息安全管理法案）、SAS70 II 和 ISO 27001 等。这些审计标准能够为云消费者所得到的服务提供保证。举例来说，审计标准 SAS 70 II 涵盖了系统的运行性能，并依赖于一组特定目标。审计报告并不足以减轻用户的担忧。此外，大多数云服务提供商不想分享其审计报告。这直接导致了透明度的缺乏。

5.3 测量与评级

最近，一个名为 Spot Cloud 的新型云市场已经启动。它提供了一种平台，云消费者可以根据位置、质量和成本来选择潜在提供商。这将支持云消费者来识别可靠的云服务提供商。对云服务提供商的评级是基于当前云消费者填写的问卷得出的。未来，需要制定一项将技术测量与消费者反馈结合起来的规定，以便比较和评估云服务提供商的可信度。

5.4 自评问卷

为确保云服务提供商的安全特性，云安全联盟提供了一种称为 CAIQ（一致性评估计划问卷）的调查问卷。CAIQ 提供了在不同特征（诸如信息安全、管理和合规性等）方面来评估云服务提供商能力和资质的方法。CAIQ 由云服务提供商进行填写。实际上，它是一组云消费者可能希望向云服务提供商提出的问题。这些问题与云服务提供商在其 IaaS、PaaS 和 SaaS 交付模型中的安全性实现有关。然而，CAIQ

评估策略尚未实现标准化。评估对于比较潜在云服务提供商是非常必要的，通过这些评估，我们可以确保云服务提供商提供的服务能够符合行业认可的安全标准、规章和审计。

5.5 信任和声誉模型

第 5.1～5.4 节中提到的方法是耗时和繁琐的。此外，这些趋势缺乏统一方法。所有这些标准可以通过该方法进行组合和评估，以支持客户选择最有效、最可靠的云服务提供商。

为了帮助客户理解差异并选择最值得信赖的云服务提供商，信任和声誉模型代表了一种很有前途、非常必要的基础方法。这些模型拥有一些被称为 QoS+ 参数的参数，以支持客户在与云服务提供商开展实质性交互之前选择最合适的云服务提供商。应当根据这些参数的重要性，来对其进行恰当的测量和分析。

1）信任和声誉模型的 QoS+ 参数

信任和声誉模型中使用的标准参数如下：

服务等级协议：云服务提供商和云消费者之间需要采用服务等级协议。

合规 / 鉴定 / 认证：云服务提供商使用不同的审计标准来证明自己。

可移植性：可移植性意味着能够运行于不同平台和操作系统上。云服务提供商应当为所有平台提供服务。

地理位置：云服务提供商提供与其数据中心地理位置有关的信息。

客户支持：一般来说，云服务提供商需要在服务等级协议中提供与客户支持相关的信息。

性能：通过服务监控技术，可以得到与云服务提供商有关的性能相关数据。性能包括可用性、弹性、时延、带宽和可靠性。

联合身份管理：通过服务等级协议，可以获取联合身份管理信息。

安全措施：云消费者总会担心数据的安全性，而云服务提供商应提供相关信息。安全措施包括加密算法、密钥管理、物理安全支持、数据安全支持和网络安全。

用户反馈：用户反馈、推荐、公开可用的评论等在云市场中非常重要。与云服务提供商有关的反馈可以作为一个整体提供，或者作为单个标准的基础。

服务部署和交付模型：云服务提供商使用的部署模型（如私有云、公共云和混合云）和服务交付模型（如 IaaS、PaaS 和 SaaS）也是非常重要的。

2）前景看好的信任和声誉模型

当前，存在着诸多信任和声誉模型。一些前景看好的模型是 eBay、RFSN（基于声誉的传感器网络框架）、β–声誉、潮汐信任、Buchegger 模型、Epinions、特定信任、Hang 模型、BNTM（基于贝叶斯网络的信任模型）、Unitec，Abawajy 模型、TESM、FIRE、网格特征值信任、特征值信任、社交 REGRET 和 Billhardt 模型等。

6 信任评估

信任模型主要涉及到信任表示、信任度量和信任评估。信任评估是信任模型的核心。信任评估方法有多种，主要包括：黑盒方法、由内向外的方法以及由外向内的方法等[7]。

6.1 黑盒方法

在黑盒方法中，实体的可信度仅是通过输出观测值进行评估的，不需要知道系统或服务的内部架构。例如，可以仅仅通过考虑用户反馈来进行评估。采用此种方法来评估信任和声誉模型的可信度时，通常将云服务提供商看作是黑盒子。

6.2 由内向外的方法

在由内向外的方法中，我们通过考虑系统内部架构及其子系统的可信度来评估实体的可信度。

6.3 由外向内的方法

由外向内的方法结合了黑盒方法和由内向外的方法。在这一方法中，基于对其组件内部架构的认识以及所观察到的整体服务行为来评估实体的可信度。

7 结束语

对于云用户来说，云服务提供商的可信度评估是非常重要的。它可以帮助客户在多个云服务提供商之间做出选择，并帮助客户访问云服务，而无需考虑数据安全隐患。关于云服务提供商，用户行为的

可信度评估是非常必要的。它有助于云服务提供商鼓励实际用户，并将恶意用户从系统中删除，这对于实现系统的完整性和可靠的服务交付是非常重要的。

参考文献

1 郎为民，张锋军，周 正．移动云计算：架构、算法与应用[M]．北京：机械工业出版社，2016.

2 郎为民． 大话云计算 [M]． 北京：人民邮电出版社，2012.

3 A K Singh. Trust and trust management models for ecommerce & sensor network [J]. International Journal of Engineering Research and Applications, 2012, 2(6): 585-619.

4 R K L Ko, P Jagadpramana, M Mowbray, et al. TrustCloud: A framework for accountability and trust in cloud computing [C]. Proceedings of IEEE World Congress on Services, Washington, DC, 2011:584-588.

5 K Govindan, P Mohapatra. Trust computations and trust dynamics in mobile ad hoc networks: A survey [J]. IEEE Communications Surveys & Tutorials, 2012, 14(2):279-298.

6 S Pearson, A Benameur. Privacy, security and trust issues arising from cloud computing [C]. Proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, 2010:693-702.

7 S M Habib, S Hauke, S Ries,M Muhlhauser. Trust as a facilitator in cloud computing: A survey [J]. Springer Journal of Cloud Computing,2012,1(1):1-18.

郎为民(1976—)，男，教授，硕士生导师，博士，教研室主任，主要研究方向为物联网、无线认知传感器网络和下一代移动通信系统。

收稿日期：2017-02-03

面向未来的智能工厂

智能工厂是在数字化工厂的基础上，利用物联网技术和监控技术加强信息管理和服务，提高生产过程可控性、减少生产线人工干预、合理计划排程，同时集智能手段和智能系统等新兴技术于一体，构建高效、节能、绿色、环保、舒适的人性化工厂。

作为智能制造的重要载体，智能工厂是构成未来工业体系的一个关键所在。智能工厂的发展，是智能工业发展的新方向。打造智能工厂，是推进信息化和工业化“两化融合”及企业转型升级的必然结果。

智能工厂具有生产设备网络化、生产数据可视化、生产文档无纸化、生产过程透明化、生产现场无人化等五大特征。通过上述先进技术应用的实现及纵向、横向和端到端的集成，实现优质、高效、低耗、清洁、灵活、精细的生产，从而建立基于工业大数据和互联网的智能工厂。

智能工厂基于信息物理系统，通过计算、自主控制和联网将人、机器、应用系统和信息互相联接，融为一体，其本质是人机交互。在智能工厂里，人、机器和资源如同在一个社交网络里自然地相互沟通协作，高效便捷地完成繁重的生产任务。

智能工厂是当今工厂在设备智能化、管理现代化、信息计算机化的基础上达到的新阶段。除了智能设备和自动化系统的集成，还涵盖了企业管理信息系统的全部内容，包括人事系统、财务系统、销售系统、调度系统等方面。

为使工厂“智能化”，智能工厂要实现信息流、物资流和管理流合一，需构建强大的信息收集和分析体系，全面、有效地管理信息，并创造性地使用信息。

智能工厂涉及多个层面和技术领域，智能生产过程中的生产决策、供应链优化等问题的解决需要借助无处不在的快速互联网基础设施和仿真系统。随着信息通信新技术的持续发展，智能工厂将越来越多地利用物联网、云计算、大数据、虚拟现实、增强现实、人工智能、机器人、3D 打印、无人驾驶运输、超宽带、精确定位等多种尖端技术及智能制造解决方案，实现更自然、更多维的人机交互。

智能工厂既是一项系统工程，也是企业需要去逐步建设的能力。对不同行业、不同外部市场竞争格局、不同发展阶段和不同企业能力的企业来说，其建设智能工厂的重点和着手点也不尽相同，应根据自身情况有的放矢、循序渐进，以更好实现建设智能工厂的既定目标。

张力平