# 个人云存储服务安全保障中的信任评估

胡裕阳
（武汉大学信息管理学院，武汉 430072）

摘要：个人云存储服务安全保障日益完善，但用户对安全保障仍存在信任问题。本文以可信云服务认证的评估内容作为基础指标，结合文献调研，对可信云服务认证、云计算安全报告、云计算安全构架与标准进行补充、调整，构建针对个人云存储服务安全保障的信任评估指标，并通过问卷调查分析个人云存储服务安全保障中的用户信任问题，进而提出在现有云服务认证的基础上推进基于信任评估的安全认证建议，以提高个人云存储服务的安全保障水平。

关键词：个人云存储；信息服务；安全保障；信任评估
中图分类号：G203　　DOI：10.3772/j.issn.1673-2286.2021.04.007
引文格式：胡裕阳. 个人云存储服务安全保障中的信任评估[J]. 数字图书馆论坛，2021 (4)：44-50.

随着互联网技术的提升，云存储服务作为一种访问便捷、空间大、易拓展、可共享的在线存储服务，越来越受到广大用户的欢迎。百度云盘、迅雷云盘、腾讯微云、阿里云盘等的出现也说明云存储服务正受到各大企业的重视。虽然云存储服务正在逐步普及，但云存储服务的信任问题仍然存在。邓仲华等[1]指出：当人们把数据存储到云端时，即使得到安全承诺，也仍是抱着怀疑的心理在使用云存储服务，而且安全问题与信任问题在一定程度上可以相互转化，安全问题是信任问题的一种体现，安全问题主要表现在物质上，而信任问题则体现在精神上。如今，人们已经意识到，信任对安全的重要性[2]。在个人云存储服务方面，信任关系影响云存储服务的安全，云存储服务的安全保障反过来又影响人们对云存储服务的信任。信任关系无法在没有任何信任基础的情况下建立，因此首先需要通过奠定安全保障基础以确保信任关系初步搭建，此后借助良好的信任关系进一步推动安全保障的提高。

## 1 信任关系对个人云存储服务安全的影响

### 1.1 个人云存储服务安全保障中的信任问题研究

关于个人云存储服务安全保障中的信任问题，主要有以下研究。Nimgaonkar等[3]提出了一个安全管理应用程序的框架，以保证云计算处理器架构的安全，从而保障执行环境的安全。Canedo等[4]提出私有云数据安全的信任模型，运用过去的推荐和交互记录来计算信任值。Kim等[5]通过进行信任计算来计算资源有效分配实现的可靠性。Yang等[6]提出了一种面向云环境的协同信任模型，信任模型与防火墙兼容，而不影响其性能。Ahmed等[7]提出了一种在访问数据时建立信任和保密性的协议。Tian等[8]在研究中讨论了基于时间，行为异常程度和访问次数的用户行为信任评估。王建亚等[9]提出的个人云存储服务的用户采纳模型显示，用户感知信任是影响用户对个人云存储服务采纳的重要因素之一。杨银波等[10]结合用户等级、资源使用合理性、用户行为、云服务终端安全性、账号异常性对用户云存储服务信任进行评

估，构建了一种基于信任评估的云存储服务模型。综上所述，现有研究主要针对个人云存储服务的使用数据进行安全保障的信任评估，缺少用户对个人云存储服务安全保障的主观信任的研究。

目前，对于个人云存储服务的安全保障已有较为详细的规范标准，客观上可以较好地保证个人云存储服务的安全性，但用户是否对现有安全保障体系完全信任，仍然存在疑问，而用户对个人云存储服务的感知风险将影响其对个人云存储服务的持续使用意愿[11]。本文通过对个人云存储服务链进行解析，分析个人云存储服务安全保障中存在的信任关系，再围绕这些信任关系，以可信云服务认证为基础建立信任评估指标，对用户信任进行评估和分析。

## 1.2 个人云存储服务安全保障中的信任关系

个人云存储服务信任关系的主要参与者由云服务提供方、用户和资源三者构成，监管机构主要负责提供可信的第三方认证，并不参与服务。其中，资源是用户使用云存储服务的主要动机，既是信任关系结构的一部分，同时还是搭建用户和云存储服务提供方之间信任的重要载体，因此资源是个人云存储服务安全保障结构的重要组成部分。

根据个人云存储服务链可以把个人云存储服务安全保障中的信任关系归纳为6种：①云存储服务提供方间的信任关系；②用户间的信任关系；③云存储服务提供方对用户的信任关系；④用户对云存储服务提供方的信任关系；⑤云存储服务提供方对资源的信任关系；⑥用户对资源的信任关系。每一种信任关系直接影响到个人云存储服务安全保障中的其他信任关系。

（1）云存储服务提供方间的信任关系。云存储服务尚处在成长期，各云存储服务提供方间缺乏数据交互，但云存储服务提供方间的资源互通是云存储服务发展的可能趋势。目前已有一些中小型云存储服务供应商（飞猫云、巴士云等）通过将资源链接到百度云、腾讯微云等大型云服务提供方的方式来推广自身服务，云存储服务提供方间的信任关系将影响各提供方间的合作及授权。合作双方之间如果没有信任关系，双方将难以进行直接的资源共享，也会影响用户对共享资源的信任。

（2）用户间的信任关系。由于个人云服务资源存在可共享性，使用云存储服务的用户就存在交互和信任关系，如果用户间难以达成信任，共享过程将难以进行。由于云存储服务用户的虚拟性，用户间的信任需要由云存储服务提供方对用户的信任以及用户对云存储服务提供方的信任来保证，只有云存储服务能通过完善的机制确保用户可信，用户相信云存储服务供应商有较为成熟的信用评估体系，用户才能信任其他用户。

（3）云存储服务提供方对用户的信任关系。云存储服务提供方对用户的信任将影响其对用户的授权，只有云存储服务提供方对用户建立了信任关系，确保其行为不会对自身安全及声誉造成影响，才能授权用户的存储、共享行为。云存储服务提供方对用户的信任将直接影响用户间的信任关系。

（4）用户对云存储服务提供方的信任关系。用户最初对云存储服务提供方的信任将直接影响其是否使用云存储服务，只有用户确信自己的资源能得到妥当保存而不会受到损害，才会开始使用该服务。不过，此信任关系难以由云存储服务自身提供，目前已通过第三方的可信云服务认证[12]保证信任关系。当用户开始使用云存储服务后，对服务提供方进一步的信任将会影响用户的深度使用，决定其是否继续使用服务，以及是否要将更为隐私的信息存储到云端等。

（5）云存储服务提供方对资源的信任关系。云存储服务提供方需要信任资源的安全性，确定资源合法安全，不会违反“红旗原则”，不会由于用户进行违法资源的存储、共享行为导致云存储服务提供方的利益损失，才能放心地进行资源的保管。云存储服务提供方对资源的信任将影响用户对共享资源的信任。

（6）用户对资源的信任关系。用户对资源的信任来源于用户对云存储服务提供方的信任以及云存储服务提供方对资源的信任，还会受到用户间信任关系的影响。用户对资源的信任分为用户对自身资源的信任，以及用户对共享资源的信任。用户对自身资源的信任主要受隐私泄露风险、知识产权风险、数据安全风险、服务迁移风险、服务履约风险和服务补偿风险的影响。用户通过共享获取资源时，需要信任资源的合法安全，不会隐藏病毒等有害资源，不会对自身产生危害，才能放心进行资源的获取。

综上所述，用户在使用个人云存储服务的过程中，仍存在亟待解决的信任问题，这些信任问题将严重影响用户的持续使用意愿。现有可信云服务认证体系虽保证了用户的权益，却无法完全保证用户在使用过程中的信任。基于此，本文围绕上述信任关系，以可信云服务认证作为基础进行拓展，构建云存储服务提供方、资

源、用户三者的信任评估指标，设计问卷进行调查，分析用户在使用云存储服务中存在的信任问题，并提出改进建议。

## 2 个人云存储服务的信任评估

### 2.1 评估指标的确定

针对前文提到的信任问题，本文以可信云服务认证的16项评估内容作为基础指标，结合文献调研，对可信云服务认证、云计算安全报告、云计算安全构架与标准进行补充、调整，构建个人云存储安全保障中的信任评估指标（见表1）。

（1）用户信任评估指标。现有云存储服务通常都会通过身份认证以及用户等级行为评估保证用户的可信度。综合相关研究，可以通过以下指标进行用户的信任评估。

表1 个人云存储安全保障中的信任评估指标

| 评估对象 | 评估维度 | 具体指标 | 解释说明 | 指标来源 |
|---|---|---|---|---|
| 用户对用户的信任 | 对用户的信任 | 访问控制 | 用户认证与授权 | [13-15] |
| | | 用户等级评估 | 对用户基于活跃度和付费进行评估 | [16] |
| | | 用户行为评估 | 对用户的操作行为进行评估 | [16] |
| 用户对云存储服务提供方的信任 | 对云存储服务功能的信任 | 服务功能 | 承诺用户提供的服务的具体功能 | [14] |
| | | 服务可用性 | 是否在承诺时间内服务可用 | [14] |
| | | 故障恢复能力 | 对用户数据备份并在需要时恢复 | [13，14，17，18] |
| | 对云存储服务性能的信任 | 网络接入性能 | 服务达到为用户承诺的相应带宽 | [14] |
| | | 服务计量准确性 | 是否按用户的实际购买量计费 | [14] |
| | | 服务变更和终止 | 用户是否担心服务变更和终止 | [14，19] |
| | 对云存储服务安全的信任 | 服务赔偿 | 服务未达承诺进行是否相应赔偿 | [14] |
| | | 网络安全保障 | 云端能否抵挡恶意代码软件攻击 | [19-20] |
| | | 账号异常性评估 | 对用户账号异常进行监测 | [16，19] |
| | | 数据存储持久性 | 数据存储在承诺时间内不丢失 | [14，15，21] |
| 用户对资源的信任 | 对资源安全的信任 | 数据可销毁性 | 数据彻底删除以免用户数据泄露 | [13，14，22] |
| | | 数据可迁移性 | 用户能否随时顺利安全迁移数据 | [14，17] |
| | 对资源隐私的信任 | 数据私密性 | 数据是否私密不可见 | [14] |
| | | 数据安全性 | 分享数据是否有安全保障 | [22] |

访问控制：访问控制主要包括身份认证和授权。身份认证是对访问个人云存储服务的用户身份进行确认。个人云存储系统面向庞大的用户群体，每个用户都有唯一的身份信息，系统需要通过完善的身份认证技术对用户的身份信息进行确认。授权是指对用户或应用程序的权限授予或拒绝的过程，对每个初始用户都应当有相应的授权。

用户等级评估：云存储服务提供方对用户进行等级评估，有利于为不同级别的用户提供差异化和个性化云存储服务。个人云盘中用户等级的主要参考指标为用户经验属性和用户特权属性。用户的经验值是根据用户的活跃度来决定的，系统根据用户对云服务的使用情况评估得到相应的经验值，依据经验值的高低来确定用户等级评估值。用户的特权值是由用户的付费情况来进行评估。

用户行为评估：用户行为评估是指对用户在云存储环境中文件上传、下载和分享等操作行为的评估。对用户分享和上传文件所进行的监控和审计包括图片和视频，有人工审核和自动化分析两种方法。

（2）云存储服务提供方信任评估指标。用户在使用云存储服务初期，并不了解云存储服务，此时由第三方可信云服务认证提供安全保障，构建用户对个人云存储服务的初步信任[23]。可信云服务认证从用户关注的数据安全、服务质量、权益保障3个方面出发，通过对云服务的16个指标进行测评认证，本研究结合可信云服务认证，保留与信任相关的评估指标，并结合现有研究进行拓展。从用户对个人云存储服务功能、服务性能和服务安全3个方面构建指标。

服务功能主要对个人云存储服务提供服务的功能进行评估，通过服务功能、服务可用性、故障恢复能力3个指标对服务功能进行评估。这3个指标决定了云存储服务的基本用途和功能，这些功能的使用性和便利性决定了用户是否愿意使用以及长期使用个人云服务产品。

服务性能主要对个人云存储服务所提供服务的性能进行评估，通过网络接入性能、服务计量准确性、服务变更和终止3个指标对服务性能进行评估。这3个指标决定了用户在使用云存储服务时的用户体验，会影响用户在不同云存储服务供应商间的抉择。

服务安全是对云服务网络安全保障和用户账号安全进行评估。通过服务赔偿、网络安全保障、账号异常性评估、数据存储的持久性4个指标对服务安全进行评估。这4个指标决定了用户使用云存储服务时的基本安全保障以及出现安全问题后如何采取措施，会影响用户的上传、共享、下载等操作行为。

（3）资源信任评估指标。用户在分享资源及通过共享获取资源时，需要信任资源合法安全，不会对自身产生危害；同时要信任自己的隐私不会受到侵犯，才能安心使用云存储服务。因此，资源信任评估指标分为用户对资源安全的信任以及用户对资源隐私的信任。

用户对资源安全的信任具体从数据可销毁性、数据可迁移性两个方面进行评估。数据可销毁性是指云存储服务提供方承诺在用户要求删除数据或设备在弃置转售前必须将其所有数据彻底删除，并无法复原。数据可迁移性是指云存储服务提供方承诺用户能够控制数据或主机镜像的迁移，保证弃用或启用该云服务时，数据能迁出和迁入。

用户对资源隐私的信任具体通过数据私密性和数据安全性两个方面进行评估。数据私密性是指云存储服务提供方承诺用户应有加密或隔离等手段保证同一资源池用户数据互不可见，且在用户授权的情况下，云存储服务提供方才能获取数据。数据安全性体现为云存储服务平台应当对分享文件的安全提供保障，在用户得到分享资源时，资源安全、可靠、无病毒，不会对用户造成损害。

## 2.2 问卷设计和调查

本次调研共发放了两轮问卷：第一轮问卷为量表问卷，用于进行统计分析；第二轮问卷以第一轮问卷的数据为基础设计问题，为非量表问卷。为保证问卷可信度，第一轮问卷主要由笔者校友及亲友等进行填写（共收到92份）。第二轮问卷采用线上随机发放问卷的方式收集数据，历时2个月，最终收集到问卷391份，前后逻辑矛盾和连续10题以上选项相同的问卷视为无效问卷，经过清理，最终得到364份有效问卷。

为保证调查有效，问卷在个人云存储服务（百度网盘、115网盘等）用户群进行发放。所有调查用户均有云存储服务使用经验，其中使用时限在一年以上的用户占74.7%，71.4%的用户每月使用云存储服务的次数在3次以上，其中29.7%的用户为常用服务的付费会员。

本研究通过SPSS23.0软件对第二轮问卷进行数据处理，得到各变量的Cronbachs $\alpha$系数来验证研究量表的信度。总量表的$\alpha$系数为0.941（大于0.800），所有维度的Cronbachs $\alpha$值均大于0.700，说明量表具有良好的信度[24]。效度即有效性，表现量表能在多大程度上有效地表示出所要表达的含义，主要作用是测量指标的有效性。本文使用Amos21软件进行验证性因子分析，所得结果显示：各维度的平均提取方差值均大于0.500，CR值均大于0.700，说明问卷各题项间内部一致性较高。

# 3 基于信任评估的个人云存储服务安全保障

## 3.1 个人云存储服务安全保障的信任关系现状

首先，在对用户的信任评估上，问卷结果表明，访问控制、用户等级评估、用户行为评估3个指标均存在信任问题。第一轮问卷的李克特七级量表得出的中位数均为5，平均数也均在5左右，表示用户在这3个方面较为信任，但离完全信任其他用户仍有一定距离。第二轮问卷结果显示，在访问控制方面，57.6%的用户认为身份认证及授权保障了分享文件来源的安全；21.7%的用户认为这会造成没必要的隐私泄露，对自身带来不利影响。在用户等级评估方面，67.6%的用户认为等级制度保证了其他用户的可信，但有19.6%的用户认为这会造成他们对其他用户不准确的信任。这说明访问控制和用户等级评估在保障用户信任的同时，也带来了一些新的信任问题。在用户行为评估方面，仅有19.6%的用户认为云服务在对用户的不当操作上不存在任何问题，33.6%的用户认为云服务存在正当操作被误判、对不当操作的界定存在问题、不当操作不会被审核到等问题。

其次，在对云存储服务提供方的信任评估上，问卷结果显示，网络接入性能、服务变更和终止、网络安全保障、服务计量准确性、服务赔偿、数据存储持久性6个指标存在信任问题。第一轮量表问卷中服务功能、服务可用性、故障恢复能力、账号异常性评估4个指标的中位数与平均数均在6以上，表示用户对个人云存储服务持信任态度。网络接入性能、服务变更和终止、网络安全保障3个指标的中位数和平均数均在5左右，服务计量准确性、服务赔偿、数据存储持久性3个指标的中位数和平均数均在4左右，表示用户在这些指标上仍存在一定的信任问题。第二轮问卷结果显示，有32.6%的用户认为个人云存储服务会真正提供其承诺的带宽。在服务变更和终止方面，60.9%的用户表示担心使用的云存储服务突然终止，导致资源丢失。在网络安全保障方面，33.7%的用户认为所使用的云存储服务无法抵御黑客及恶意代码的攻击，不能保障数据的安全。在服务赔偿方面，45.6%的用户并不相信云存储服务会对于其造成的损失进行赔偿。在数据存储持久性方面，42.7%的用户表示担心自身资源会因为云存储服务的审查计划导致数据遗失。

最后，在对资源的信任评估上，问卷结果表明，数据可销毁性、数据私密性、数据安全性3个指标存在信任问题。数据可迁移性方面，量表问卷平均数为5.9，中位数为6，表示用户比较信任资源能在云端随时迁入迁出。数据可销毁性、数据私密性、数据安全性的平均数与中位数均在4左右，说明用户在这3个指标上存在一定的信任问题。第二轮问卷结果显示，在数据可销毁性方面，25.0%的用户相信云服务方会在用户删除数据后立即删除数据，44.6%的用户认为云服务提供存储方会将数据再保存一段时间，而28.3%的用户认为云存储服务提供方会筛选留存有价值的数据加以利用。在数据私密性方面，仅39.2%的用户认为云存储服务提供方仅会在法律允许范围内对用户的资源进行审查，说明用户对自身数据的安全存储以及隐私泄露持不信任的态度。在数据安全性方面，47.8%的用户表示他们并不相信资源安全可靠无病毒，并表示会小心审查文件的安全后使用。

## 3.2 个人云存储服务安全保障的信任关系改进

针对当前个人云存储服务在个体用户安全保障方面的问题，本文从用户感知的信任视角出发，将用户的感知信任通过信任关系分为用户间的信任、用户对云存储服务提供方的信任和用户对资源的信任3个方面，以可信云服务认证为基础，提出基于信任关系的个人云存储服务安全认证体系（见图1），以提升个人云存储服务的安全保障水平。

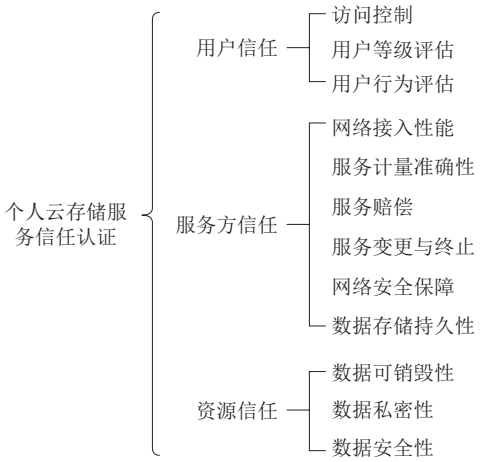


图1 个人云存储服务安全认证体系

（1）针对用户的信任认证。在访问控制方面，用户相信身份认证确实对其他用户的安全可信提供帮助，但与此同时，用户也担心身份认证会导致隐私泄露对自身造成影响。对此，可通过第三方监管，通过联网责任监督、技术责任监督和法律责任监督三方联动，在验证层、应用层和信息层上进行有效监管[25]，确保访问控制在保证用户信任的基础上不会产生其他的信任问题。

在用户等级评估方面，用户等级评估会影响用户对其他用户的信任，仅基于用户付费情况和活跃度的等级制度也让部分用户认为，会造成他们对其他用户不准确的信任。在对用户的行为评估上，用户认为个人云存储服务在对用户的不当操作上进行的处理存在各种各样问题。大部分用户认为云存储服务并不能保证其他用户可信，也无法信任其他用户。因此，为保障用户间信任，个人云存储服务应当对用户进行信用认证：云存储服务提供方应当根据用户的使用行为，建立完善的用户信任认证体系。当发现用户进行违规操作时（分享违法或病毒资源等），降低其信用等级，同时根据用户的信用等级，进行不同级别的授权。此外，要确保其他用户在获取资源时，能直接获取资源分享者的信用等级。

（2）针对个人云存储服务提供方的信任认证。在网络接入性能和服务计量准确性方面，用户认为云存储服务提供方并未根据用户所购买的服务精准提供其

应有的带宽。在服务赔偿方面，用户并不认为使用的云服务会对其违约行为进行赔偿。需要通过设立具有一定独立性和权威性，值得市场主体信任的监管机构，政府参与其中，结合云存储下的ISP和ICP进行评估审查，加强监管，促进云产业健康发展。

在服务变更与终止方面，由于有360云盘停止服务的经历，用户担心常用的云存储服务突然停止服务对自身造成不便。对此，建议通过以下方式改善用户对服务终止的信任问题：云存储服务提供方应承诺在停止服务前给予用户足够的时间进行数据迁移，并无偿开放一定带宽保证用户数据的成功迁移；云存储服务方亦可考虑与其他可信云服务提供方进行合作，在服务终止前进行数据迁移以保证用户数据不会丢失。

在网络安全保障方面，部分用户认为所使用的云服务不能完全抵御来自黑客和恶意代码的攻击，对此，云存储服务提供方应加强网络监控，确保自身服务器安全且对用户数据进行备份。对于小型的云存储服务提供方，可以与提供网络保护服务的第三方进行合作，以保障服务器安全。为保障用户的信任关系，在以上操作中最重要的是应将采取的对策行为对用户公示，让用户感知到安全保障措施的实施。

在数据存储持久性方面，应结合后文对资源的信任审核措施以保证用户数据存储的持久性。

（3）针对资源的信任认证。在数据可销毁性方面，由于云存储服务会采用文件指纹技术，分享的资源不会被完全销毁，但用户仍会担心个人的隐私数据未被删除。与服务赔偿类似，在数据可销毁性方面，需要更为可信可靠的第三方监管机构参与其中，进行数据销毁的审查监管，保证资源的及时销毁。

在数据数据私密性和安全性方面，用户担心私密资源会被云服务方获取，同时还担心分享的文件是否安全。对此，建议通过以下措施改善用户对资源的信任：个人云存储服务提供方结合用户信用等级评估机制保证资源分享过程的透明性；为保障用户感知的私密性和数据存储的持久性，存储服务提供方对用户上传到云端的资源不进行审核，而对用户分享的资源进行安全审核；当资源出现被压缩等情况无法保证文件透明时，则根据用户信用等级进行分级授权，对于低信用等级的用户，在分享资源时必须保证资源的透明性，对于高信用等级的用户，可适当放宽分享权限。在分享资源不透明，安全性无法保证时，应当对获取资源的用户进行提醒。

## 4 结语

基于用户的感知风险会对个人云存储服务的持续使用造成影响，本文从信任关系出发，研究个人云存储服务安全保障中存在的信任问题。本文的贡献在于：①指明云存储服务提供方在提供服务时，不仅要要考虑安全保障是否全面，还应考虑用户是否对这些安全保障产生确实的信任；②结合现有安全保障体系，根据信任关系构建用户在使用个人云存储服务中的信任评估指标，并设计问卷找出个人云存储服务安全保障中存在的信任问题；③根据用户在个人云存储服务使用过程中存在的信任问题提出相应的建议，以保证用户持续和深入使用的意愿。然而，本研究还存在继续深入研究的空间。一方面，由于样本数量有限导致结论存在局限性，这可以通过更广泛的调查来解决；另一方面，信任是一种主观感受，当问卷提出相关问题时，有可能对用户的信任感知带来影响，从而可能导致问卷的回答有所偏差，这可以通过结合云存储服务的用户日志分析来缩小这一偏差。

### 参考文献

[1] 邓仲华，涂海燕，李志芳，等. 基于SLA的图书馆云服务参与方的信任管理[J]. 图书与情报，2012(4)：16-20.

[2] CONCHIE S M，DONALD I J，TAYLOR P J. Trust：Missing piece(s) in the safety puzzle[J]. Risk Analysis An Official Publication of the Society for Risk Analysis，2010，26(5)：1097-1104.

[3] NIMGAONKAR S，KOTIKELA S，GOMATHISANKARAN M. CTrust：A Framework for Secure and Trustworthy Application Execution in Cloud Computing[C]//Proceedings of 2012 ASE International Conference on Cyber Security. IEEE，2012.

[4] CANEDO E D，SOUSA R，CARVALHO R，et al. Trust model for private cloud[C]//International Conference on Cyber Security. IEEE，2012.

[5] KIM H，LEE H，KIM W，et al. A Trust evaluation model for QoS guarantee in cloud systems[J]. International Journal of Grid & Distributed Computing，2010，3(1)：1-10.

[6] YANG Z M，QIAO L X，LIU C，et al. A collaborative trust model of firewall-through based on Cloud Computing[C]// International Conference on Computer Supported Cooperative

Work in Design. IEEE，2010.

[7] AHMED M，XIANG Y，ALI S. Above the Trust and Security in Cloud Computing：A Notion Towards Innovation [C] //IEEE/IFIP International Conference on Embedded & Ubiquitous Computing. IEEE，2010.

[8] TIAN L Q，LIN C，YANG N. Evaluation of user behavior trust in cloud computing [C] //International Conference on Computer Application & System Modeling. IEEE，2010.

[9] 王建亚，罗晨阳. 个人云存储用户采纳模型及实证研究 [J]. 情报资料工作，2016（1）：74-79.

[10] 杨银波，唐会军，石晓虹. 一种基于信任评估的云存储服务模型 [J]. 电子科学技术，2015，2（1）：69-75.

[11] 胡昌平，李霜双，冯亚飞. 感知风险对个人云存储服务持续使用意愿的影响——转换成本的调节作用分析 [J]. 现代情报，2019，39（5）：64-73.

[12] 丁滟，王怀民，史佩昌，等. 可信云服务 [J]. 计算机学报，2015，38（1）：133-149.

[13] 程慧平，彭琦. 个人云存储服务的技术安全风险关键影响因素识别与分析 [J]. 图书情报工作，2019，63（16）：43-53.

[14] 栗蔚. 可信云服务认证体系 [J]. 电信网技术，2014（4）：5-7.

[15] MIRSAEID H S，AMIR M R，AMIR S. An iterative mathematical decision model for cloud migration：a cost and security risk approach [J]. Software practice & experience，2018，48（6）：449-485.

[16] 程慧平，彭琦. 个人云存储服务安全风险及治理策略 [J]. 图书馆理论与实践，2018（1）：54-60.

[17] MYEONGGIL C，CHANGHAN L. Information Security Management as a Bridge in Cloud Systems from Private to Public Organizations [J]. Sustainability，2015，7（9）：12032-12051.

[18] SAURABH S，YOUNG-SIK J，HYUK P A. survey on cloud computing security：Issues，threats，and solutions [J]. Journal of Network and Computer Applications，2016，75（Nov.）：200-222.

[19] 周耀林，黄玉婧. 感知风险对科研人员云存储服务持续使用行为的影响——基于扎根理论的探索性研究 [J]. 现代情报，2020，40（8）：82-88，97.

[20] Missing cloud security awareness：investigating risk exposure in shadow IT [J]. Journal of Enterprise Information Management，2017.

[21] CSA. ‘The treacherous twelve’ cloud computing top threats in 2016 [EB/OL]. [2020-07-05]. https://www.prnewswire.com/news-releases/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016-300227806.html.

[22] ENISA. Cloud computing benefits，risks and recommendations for information security：cloud computing security risk assessment [EB/OL]. [2020-07-17]. https://www.Enisa.Europa.eu/publications/cloud-computing-risk-assessment.

[23] 郭丰，栗蔚. 公共云服务认证进展研究 [J]. 电信科学，2014，30（6）：108-110，117.

[24] LIU S，XIA F，ZHANG J，et al. Exploring the trends，characteristic antecedents，and performance consequences of crowdsourcing project risks [J]. International Journal of Project Management，2016，34（8）：1625-1637.

[25] 阮晨欣. 法益衡量视角下互联网可信身份认证的法律限度 [J]. 东方法学，2020（5）：45-55.

## 作者简介

胡裕阳，男，1998年生，硕士研究生，研究方向：信息服务与用户，E-mail：260803978@qq.com。

Trust Evaluation in the Security Assurance of Personal Cloud Storage Service

HU YuYang
( School of Information Management, Wuhan University, Wuhan 430072, China )

Abstract: The security of personal cloud storage service is improving day by day, but there are still trust problems for users. Based on the evaluation content of trusted cloud service authentication as the basic index, combined with literature research, this paper supplements and adjusts the trusted cloud service authentication, cloud computing security report, cloud computing security architecture and standards, constructs the trust evaluation index for personal cloud storage service security, and analyzes the user trust in personal cloud storage service security through questionnaire survey, Then, it proposes to promote the security authentication based on trust evaluation on the basis of existing cloud service authentication, so as to improve the security level of personal cloud storage services.

Keywords: Personal Cloud Storage; Information Service; Safety Guarantee; Trust Evaluation

（收稿日期：2021-04-01）