doi:10.3969/j.issn.1000-436x.2013.12.018

移动云服务的数据安全与隐私保护综述

李瑞轩，董新华，辜希武，周湾湾，王聪
（华中科技大学 计算机科学与技术学院，湖北 武汉 430074）

摘 要：移动云服务相比传统云具有移动互联、灵活终端应用和便捷数据存取等特点。然而，丰富的移动云服务应用也带来了更多的安全与隐私泄露问题。在阐述移动云服务的基本概念、应用与安全问题的基础上，给出了其安全与隐私保护体系结构，主要围绕安全协议与认证、访问控制、完整性验证、移动可信计算和基于加密、匿名、混淆的隐私保护等关键技术，分析其研究现状，论述已有技术的优势和不足，并探讨了未来的研究方向。
关键词：移动互联网；云计算；移动终端；数据安全；隐私保护
中图分类号：TP309 **文献标识码：**A **文章编号：**1000-436X(2013)12-0158-09

Overview of the data security and privacy-preserving of mobile cloud services

LI Rui-xuan, DONG Xin-hua, GU Xi-wu, ZHOU Wan-wan, WANG Cong
(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: Compared with the traditional cloud services, the mobi cloud services have the characteristics of the mobile interconnected, flexible end-user applications and convenient data access. However, the rich applications of mobile cloud services bring more security and privacy-leaking problems. The basic concepts, applications and security issues of mobile cloud services were shaded light on, and then describes the architecture of security and privacy-preserving was described, some key technologies were studied in this domain, mainly focusing on the research progress of the security protocols and authentication, access control, integrity verification, mobile trusted computing and the privacy-preserving based on encryption, anonymous and confusion, and the advantages and disadvantages were pointed out respectively. Finally, some future research direction were given at the end.
Key words: mobile internet; cloud computing; mobile devices; data security; privacy preserving

1 引言

随着信息技术的发展，近几年各种类型的移动云服务越来越广泛地被人们所使用，比如远程管理、无线推送、存储备份、在线搜索、在线音乐、移动便签等。据 CNNIC《第 31 次中国互联网络发展状况统计报告》显示[1]，截至 2012 年 12 月底，我国网民规模达 5.64 亿，移动互联网用户数将超过 5.2 亿。预计 2013 年中国移动互联网用户数首次超过传统互联网用户数，中国移动互联网产值将超过 1 000 亿元。进入 2011 年以来，以手机在线存储、手机在线音乐为典型应用的移动云服务呈现出强劲发展势头。国外的苹果 iCloud 云服务和 iOS 终端、谷歌的安卓云服务、微软 Windows Azure 服务等都是著名的移动云服务案例。在国内，华为 Cloud 云和 Vision 手机、阿里云 OS、MIUI 手机金山云服务、中国移动彩云服务等也逐渐呈现。移动云服务除了具备传统云服务的便捷云端数据存储、大量的开放

收稿日期：2013-05-02；**修回日期：**2013-10-15
基金项目：国家自然科学基金资助项目（61300222, 61173170, 60873225）；国家高技术研究发展计划(“863 计划”)基金资助项目（2007AA01Z403）；华中科技大学自主创新研究基金资助项目（2012TS052, 2012TS053, 2013QN120, CXY13Q019）
Foundation Items: The National Natural Science Foundaiton of China (61300222, 61173170, 60873225); The Natiional High Technology Research and Development Program of China (863 Program) (2007AA01Z403); Independent Innovation Fund of Huazhong University of Science and Technology (2012TS052, 2012TS053, 2013QN120, CXY13Q019)

软件服务、无所不在的强大云计算支撑、终端配置要求低等特点，融合了移动通信设备和传统互联网，还具有移动互联、实时在线、便捷灵活实现传统云服务在移动互联网中的扩展和应用等特点，将服务从云端推送至终端，向用户提供自由、方便和灵活的服务，这种新的服务模式将引起业界又一次重大的产业变革，但同时也带来相比于传统云服务更广泛更复杂的安全与隐私保护问题。

在实际应用中，典型的移动云服务公司提供的服务（如苹果的 iCloud，谷歌的安卓云服务和微软的 Windows Azure 等）出现安全漏洞的消息时有所闻。而在移动云环境中，移动智能终端存在隐私泄露、身份盗用、位置定位和手机病毒等安全问题，云端服务存在拒绝服务攻击、信息窃取等问题，内容提供者方面存在不良信息源、有安全漏洞的移动业务应用等问题。第四届迈克菲年度安全峰会（MacFree Focus 11）、2012 中国信息安全高峰论坛、第十三届中国信息安全大会等会议都将移动云服务安全问题与隐私保护列为备受关注的大会日程。移动云安全和隐私保护问题的圆满解决将成为促进移动云服务不断深入发展的推动力，将大力促进国家移动互联网基础设施建设，满足国家信息安全的重大需求，具有重要的理论和实际意义。

2　移动云服务的基本概念、应用与安全问题

2.1　移动云服务的基本概念

所谓“云计算”，是分布式处理、并行处理、网格计算、网络存储及大型数据中心的进一步发展和商业实现，它将数据计算分布在互联网的大规模服务器集群上，用户根据需求访问计算机和存储系统，实现对信息服务进行统一建设和管理，用户按需使用、按量付费。云服务是指采用云计算技术的大规模服务器集群（云端）为用户提供的不必下载、不必安装、上网即用、操作方便、功能丰富、价格低廉的互联网服务。移动云服务是移动互联网和云计算融合发展的最新形态，旨在通过移动互联网络，以移动智能终端为信息接入口，面向最终用户提供云计算的各类综合服务。

移动云服务除了具备传统云服务大量开放的软件开发与服务、云端与终端设备的自动同步、强大的云计算和云端数据存储和终端硬件配置要求低等特点，还具有永远 24 h 在线的便捷服务，能实现传统云服务在移动互联网的扩展应用等新的特点。

2.2　移动云服务的应用

移动云服务有着广泛的应用，在商业领域常见的应用有工作派遣、日程安排、内部邮件、工作流程等移动企业管理相关服务，也有后勤、库存控制等移动商务应用。同时，政府也在公共服务、军事等领域应用移动云计算，譬如：电子政府、电子健康服务、旅游业(电子地图导航、旅游定位服务)、智能交通、环境监控、战时通信等。个人用户的应用一般是移动网络接入、电子商务(购物、移动支付)、办公、存储、影音、游戏、SNS、娱乐等个性化的需求。其中个人娱乐类移动云服务将会占据主角。

近年来，中国的 3G 用户呈现了规模化发展趋势，庞大的用户基数造就了个人消费类移动云服务的巨量潜在市场，因此未来 3 至 5 年内，个人消费类服务将是移动云服务的主要服务形态。

2.3　移动云服务的安全问题

目前，大多数正在应用的移动云服务仅涉及那些安全性要求相对较低的应用，隐私和安全问题成为阻碍移动云服务发展和广泛应用的重要障碍。相对于传统云服务，移动云服务的优势在于突破终端硬件的限制，移动终端实现了便携式数据存取、智能负载均衡，降低了管理和按需服务的成本。但移动云服务的接入终端由传统桌面机变为移动终端，接入终端的系统复杂程度远超传统终端设备，智能终端设备（如 3G 手机）的带宽不仅受到区域手机发射塔带宽的限制，且计算能力和电池容量有限；承载网络由互联网转换为移动网络叠加互联网，网络连接环境也变得更为复杂。移动云服务中的安全和隐私问题归纳起来主要存在以下 3 个方面。

1) 移动云服务整个生命周期模型中存在的安全问题。由于移动云服务平台的复杂性、资源种类繁多和多终端共享的特征，使得云服务提供商无法保证数据在移动云服务平台中递交、存储、访问、更新和销毁等环节不出现安全问题。

2) 移动云服务的移动互联和资源受限等特性所带来的安全问题。由于移动通信和传统互联网叠加而带来的接入方式多样，移动连接和带宽不稳定，智能终端计算、存储能力和电池容量等方面的限制，使得传统复杂的加密方法和访问控制措施在移动云服务环境中无法适用。

3) 移动云服务中用户隐私数据的泄露。目前，移动云服务中的用户大部分是在没有安全防护的情况下使用云服务，如移动终端设备的用户通讯

录、短信、备忘录等隐私数据默认直接与云平台保持同步，这些隐私数据在云平台中无法得到有效保护。随着移动终端应用的广泛使用，应用程序可以方便地捕捉用户的地理位置信息，而这些信息不仅包括用户目前的地理位置，还可能会推导出用户潜在的位置隐私，这也会对用户的隐私构成威胁。

3 移动云服务安全与隐私保护体系架构

移动云服务可以随时随地按需提供弹性存储、计算等资源，结合当前移动云服务的应用与研究，其体系架构可分为资源层、虚拟层、服务层和移动终端，如图 1 所示。

资源层(IaaS)面临的安全威胁主要有物理安全、网络安全和主机安全等问题。物理安全需要考虑机房选址，做好防火、防雷、防盗、防静电、防电磁泄漏等措施，网络安全和主机安全需要防火墙、入侵防范、恶意代码防范、安全审计等措施来实现。虚拟层主要存在着虚拟化安全问题，虚拟化安全问题一般通过镜像加固、配置管理、虚拟机攻击防护等措施解决。服务层（PaaS 和 SaaS）则存在应用安全、运行安全、接口安全和数据安全等问题，应用安全主要通过 WAF、代码审计、安全开发、应用安全扫描等方式实现，运行安全通过补丁管理、配置管理、安全监控实现，接口安全则主要通过安全审计的方式来保护，数据安全则通过安全协议与认证、私密性与访问控制、完整性验证、DLP、安全审计、加密、数据灾备等措施实现。移动终端则包括终端安全和隐私保护等问题，终端安全包括终端自身的安全和云终端软件安全，前者可通过防恶意代码、防火墙、防入侵、补丁管理等方式保护，后者则主要考虑应用安全和浏览器安全。在终端和移动云平台之间还存在着通信安全问题，通信安全则主要通过通信加密、SSL、安全通信协议等方式来实现。

本文重点讨论安全协议与认证技术、私密性与访问控制技术、完整性验证和移动可信计算等关键技术，这些技术主要是针对移动云平台，解决移动云服务中整个生命周期以及由于移动云服务的特性而带来的数据安全问题，增强云中数据的安全性。然后讨论基于加密、匿名、混淆的隐私保护技术，主要是针对移动终端，在提供移动云服务的同时，对个人隐私数据进行保护。

4 关键技术分析

4.1 数据安全保障

目前，移动云服务的安全性研究主要是将已有的安全技术，如访问控制、加密、完整性等移植到移动云服务环境中。国内学者对云计算及其安全性展开了讨论[2,3]，中国联通研究院对移动互联网环境下的云计算安全问题进行了分析[4]，并给出了安全建议，这些工作为移动云环境下的安全发展提供了参考。

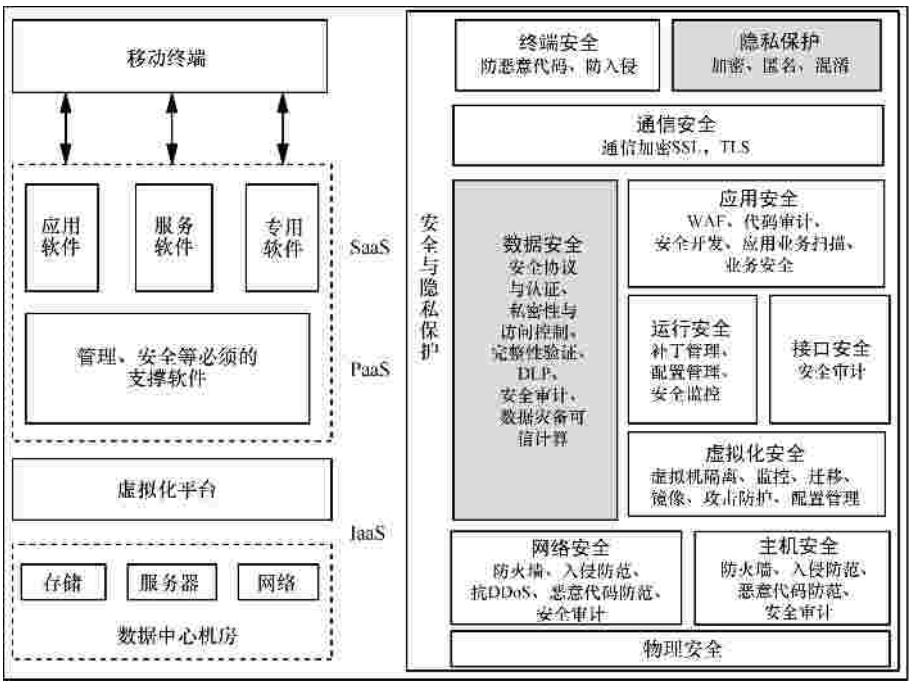

图 1 移动云服务安全与隐私保护体系架构

1) 安全协议与认证技术

用户要使用移动云存储和计算等服务，首先必须经过云服务商 CSP 的安全认证。同时，各级服务提供商之间也需要相互的认证。服务需求者和提供者都需要接受默认的安全协议，因此，安全协议与认证机制是云服务的一个基础研究问题。

吕慧等[5]提出了一种应用于 3G 业务的改进协议，针对第三代移动通信系统中采用的认证与密钥协商(AKA)协议存在安全漏洞和密钥管理困难等问题，采用基于椭圆曲线密码(ECC)和公钥体制协商会话密钥、对称加密算法加密消息的方法。该协议不仅有效克服了 AKA 协议中存在的各种缺陷，避免了复杂的密钥管理难题。傅建庆等[6]提出了一种新的匿名认证协议。该协议基于椭圆曲线加密和代理签名机制，通过让部分移动终端随机共享代理签名密钥对的方式，实现了完全匿名和非法认证请求过滤。Lee 等[7]针对移动卫星通信系统提出了一个简单且高效的认证机制，可以抵挡模拟攻击、拒绝服务攻击和智能卡损失攻击等，且其计算代价很小。Richard 等[8]提出了一种云环境中基于用户行为的移动终端认证框架，结合基于支持认证决策 TrustCube（认证管理基础设施）的灵活框架和基于行为认证（用户行为翻译为认证分数）的隐式认证，通过灵活的决策和动态调整可以权衡可用性和信任之间的平衡。刘宴兵等[9]设计了一种基于云计算的智能手机社交认证系统，在降低终端能耗和增强身份认证安全性的情况下，有效地解决了认证票据有效期短而导致系统性能急剧下降的问题。

当前，研究人员在现有安全协议的基础上，对协议中存在的安全漏洞进行补救，并提出新的灵活、高效和节能的认证方案。借鉴认证方案中的优点，加强移动云应用统一认证技术研究，以保障用户在登录多个业务系统时用户信息的安全。

2) 私密性与访问控制技术

终端用户把个人数据存储于移动云并接受其提供的服务，从用户角度，思想上仍存在顾虑，因为数据不受自己的控制。云服务系统能否保证数据安全，云提供商是否对用户数据在未经授权情况下查看都是未知数。而从云服务商 CSP 的角度，是要确保用户数据安全，提升用户体验。因此，私密性与访问控制是云安全领域最热的研究问题之一。

国内研究者采用基于属性的加密算法[10]和基于代理重加密[11,12]的方法去保护数据的私密性。Victor 等[13]利用基于属性的加密措施设计数据的访问控制方法，以加密形式保存用户数据。在访问控制方面，文献[14]运用 Voronoi 图模型和 quorum 系统的思想，提出了一种移动自组网的动态路径 quorum 系统，设计了动态路径 quorum 的生成算法，并提出了基于 quorum 系统的移动自组网的分布式访问控制机制，与传统的基于单个节点自身的访问控制机制相比，该访问控制机制具有较强的抗攻击能力和较高的可靠性，能够有效地提高移动自组网的资源共享与保护水平。Unal 等[15]针对多域移动网络提出了一个新的安全策略模型 FPM-RBAC，支持移动性、位置限制、角色层次映射、域间服务、域间访问权限和职责分离。同时提出了针对域和域间安全策略的正式的安全策略约束规范语言，使用环境演算和安全策略来说明移动网络的当前状态和行为，并评价访问请求。该策略模型的一个新颖方面就是支持涉及移动性在多个安全域的安全策略的正式和自动化分析。Shin 等[16]提出移动终端在云存储服务下的安全数据访问控制方法 DFCloud，DFCloud 依赖可信平台模块 TPM 去管理所有密钥，并在合法用户中使用密钥共享协议。DFCloud 利用客户端加密技术、远程认证客户平台和基于硬件的密钥管理去构建一个安全访问环境。

传统的加密技术能够实现数据的私密性，但在移动云环境下，利用基于属性的加密和代理重加密能提高访问控制的灵活性。在传统访问控制的基础上，访问控制从单域向自组网络和多域安全发展。

3) 完整性验证技术

由于受存储容量和网络带宽的限制，用户不可能将数据下载后再验证其正确性。因此，终端用户需在取回很少数据的情况下，通过某种知识证明协议或概率分析手段，以高置信概率判断远端数据是否完整。Yun 等[17]提出一个新的基于 MAC 树的加密网络文件系统结构，相比于 Merkle 树的结构有更好的性能，以更低的成本提供了完整性保护。文献[18]通过分析传统的完整性验证机制，借鉴身份认证、携证代码以及反射技术，提出对终端 Agent 进行完整性验证的分级保护机制，实现软件行为的监控，从而提升了移动代码的可信度。其他典型工作包括，面向用户单独验证的数据可检索性证明(POR)[19]方法、公开可验证的数据持有证明(PDP)方法[20,21]。NEC 实验室提出的 PDI(provable data integrity)[22]方法改进并提高了 POR 方法的处理速

度以及验证对象规模，且能够支持公开验证。

在支持随机访问的基础上保证文件的机密性和完整性，当前流行的设计是把 Merkle hash 树和加密的块密码结合。在面向云的数据完整性验证方面，终端用户更希望移动云能支持来自用户的公开验证。

4) 移动可信计算

移动可信计算是在移动终端中加入移动可信计算模块，配合移动云中的可信过程，构建一个从终端到云的可信网络平台。

李涛等[23]基于可信计算思想，通过在现有移动终端中加入移动可信计算模块，并在核心网中加入安全服务提供者和安全软件提供商，构架了面向移动终端的统一安全防护体系。该方案有效利用了移动终端操作系统的特性，将基于角色的访问控制与可信验证相结合，实现了高效的可信链传递，使没有授权证书的非法软件和非法进程不能在系统中运行，保证了系统的安全性。国防科技大学的研究人员对可信计算组织定义的移动可信模块(MTM, mobile trusted module)的结构和特点进行了详细描述，介绍了当前增强移动平台安全的 TrustZone 和 MShield 技术[24]。TrustZone 技术其核心是在微处理器中增加安全功能，以保证微处理器内外的存储空间及外设不受软件攻击。MShield 技术提供了一个基于硬件的安全环境，通过嵌入的安全状态机(SSM)确保应用程序在进入、执行和退出安全环境时遵守系统安全策略。SSM 消除了芯片互连及直接存储访问(DMA)时数据传输的脆弱性，为传输机密、敏感数据（如密钥、证书等）以及整个平台处理提供安全保护。

移动云服务数据安全还包括数据的可用性等方面，鉴于当前数据备份等技术比较成熟没有进一步展开。上述几方面技术能够解决移动云服务整个生命周期中存在的绝大部分安全问题，针对移动云服务提供商和其他用户，移动云服务数据安全的技术手段如表 1 所示。目前的技术基本可以避免来自其他用户的安全威胁，但是对于服务提供商，若要从技术上完全杜绝安全威胁还有一定困难，因此需要非技术手段（如法规等）作为补充。

综上所述，利用基于属性的加密机制来实现数据的加密与访问控制是移动云环境下行之有效的方法，但基于属性的加密方法需要较大的计算量，因此需要研究移动云服务环境中的轻量级数据加密与访问控制方案，实现对数据的细粒度访问控制，大幅降低移动设备的计算、通信和存储开销。鉴于当前云服务商处于不可信或不完全可信状态，提供公开验证方法和有关的验证结构，允许数据拥有者来验证存储在云中数据的完整性也是一个重要研究方向。而从云服务商的角度，则更关注在移动计算中建立可信云计算的基础构架和应用，未来应考虑统一可信平台各部分可信组件的安全协调。

表 1 移动云服务数据安全技术手段

安全性要求	对其他用户	对服务提供商
安全协议与认证技术	非法认证过滤	统一认证、相互认证
数据访问控制	存储隔离、加密	存储加密、文件加密
数据私密性	虚拟机隔离、操作系统隔离	操作系统隔离
数据完整性	数据检验	数据检验、公开验证
移动可信计算	移动可信模块，阻止非法进程	可信链传递

4.2 隐私保护

总体说来，移动云服务中的隐私问题主要包括通信隐私和数据隐私 2 个方面。通信隐私是指通信的双方或多方之间的关联，有不被外界知晓的权利和需求；同时用户具有对云服务端保持身份匿名或查询内容的私密性。数据隐私是指隐私敏感性的数据有不被外界知晓的权利和需求。数据隐私可分为直接数据隐私和间接数据隐私。移动云服务中的隐私保护的技术需要借鉴数据库中的隐私保护技术。比较主流的数据隐私保护技术主要有基于加密的隐私保护技术、基于匿名的隐私保护技术和基于混淆的隐私保护技术。为避免个人数据（通讯录、短信、备忘录等）丢失，移动终端用户在将其同步至云端时，加密技术可以有效保护这些敏感数据不被窃取；用户在享受移动云提供的各类服务时，利用匿名技术和混淆技术可以有效保护个人隐私数据。下面分别对这几类技术进行介绍和分析。

1) 加密技术

加密是一种有效地保护隐私的方法，传统的加密算法包括对称加密算法（如 DES、3DES、ADES）和非对称加密算法（如 RSA、Diffe Hellman、ECC），但加密后的数据往往失去可操作性，对数据处理性能有较大影响，因此提高密文处理效率和密文检索速度是现阶段数据隐私保护的研究热点。在密文处理方面，建立公共云平台基础上的安全数据服务模

块 CSS[25]，可通过加密和令牌服务保证用户数据隐私，但涉及数据值操作时，需要解密数据。传统的同态加密仅支持某一类型或特定的操作，如针对同态乘法的 RSA、针对同态加法的 Paillier 等。IBM 研究员 Gentry 利用“理想格”的数学对象构造隐私同态算法[26]，可充分操作加密状态的数据，虽在理论上取得了一定突破，但效率太低，还不适合应用在具体应用中。在密文检索方面，文献[27~30]针对云中数据隐私保护展开研究，分别提出了在云中进行密文检索的解决方案。基于矩阵和向量运算的可计算加密方案 CESVMC[31]，支持对加密字符串的模糊检索和对加密数值数据的加减乘除运算，并保证数据存储和运算过程的隐私安全性。但其中的乘除法运算的性能仍需改进，不支持多次乘除法运算。

从密钥管理和终端节能方面，Wang[32]和 Zhou[33]对移动云环境下数据的加密存储和授权进行了研究，并提出数据块加密和密钥管理的方法。Tysowski 等[34]提出基于动态重加密原理的密钥分布模型应用于云计算系统，去满足移动设备环境的需求，包括客户端无线数据使用、存储容量、处理能力和电池寿命的限制。该模型要求密钥由客户端管理，密集型数据重加密由云提供商处理，密钥重新分配机制能使移动设备通信开销最小化。Yongjoo 等[35]针对移动设备轻量级的自加密算法（SE）的缺点，提出了基于随机排列和比特翻转的自加密机制，既能从明文中派生密钥流，又能从随机过程中有效地去除统计相关性。算法克服了原先的 SE 机制和复杂性，满足密钥和密码流的 0/1 的均匀性，比 AES、RC4 更快，更高效节能。

2) 匿名技术

匿名技术是对信息进行处理以隐匿其敏感属性，而共享其他属性的过程。随着基于位置服务的快速发展，在移动云环境下的位置和轨迹隐私保护越来越受到关注。匿名技术主要包括假名匿名、空间匿名、时空匿名、k-匿名、L-diversity 匿名、T-closeness 匿名技术等。假名匿名技术是用户在发送服务请求信息时，给出的不是自己真实的位置数据，而是与真实数据有一定差距的假数据，其保护强度由真假数据之间的差距来决定。空间匿名是使用一个空间区域来代替用户的准确位置，以此降低用户的空间分辨率。时空匿名在空间匿名的基础上增加了一个时间轴，在用空间区域代替具体位置后，同时延长匿名的时间，将位置服务请求信息的匿名时间延长，在这个时间段里会有更多的信息出现在这个空间区域，以寻找合适的匿名群。对于空间匿名和时空匿名，空间的大小决定了匿名的强度。P.Samarati 等在 PODS 会议上提出的 k-匿名技术[36]最早使用在关系数据库的隐私保护中，后来被引入移动环境下的位置隐私和轨迹隐私保护中。k-匿名可以保证每个个体的敏感属性隐藏在规模为 k 的群体中，使得个体被确认的几率不会超过 $1/k$。k-匿名技术的隐私保护强度取决于 k 值的大小。k-匿名尽可能的保持数据的可统计性，但没有对敏感数据做任何约束，攻击者可以利用一致性攻击和背景知识攻击来确认敏感数据与个人的联系，导致隐私泄露。(α,k)-匿名原则[37]在此基础上进行了改进，其在保证发布的数据满足 k-匿名化原则的同时，还保证发布数据的每一个 k 群体中，与任一敏感属性值相关的记录的百分比不高于 α。L-diversity 匿名[38]保证每一个群体的敏感属性至少有 L 个不同的值，使得攻击者最多以 $1/L$ 的概率确认某个体的敏感信息。T-closeness 匿名[39]在 L-diversity 匿名基础上，考虑了敏感属性的分布问题，它要求群体中敏感属性及其值的分布差异不超过 T。在隐私保护实践中，上述匿名技术均适用于移动云环境。

3) 混淆技术

混淆技术通常通过扰乱、添加随机变量或随机偏移值、增加错误数据或噪声、替换等方法对原始数据集中的敏感信息进行替代，生成加入扰乱信息的模糊数据集，以进行公示和计算等操作。攻击者通过发布的混淆数据不能重构出原始的真实数据，而经混淆后的数据仍能保持某些性质不变，从而保证了某些应用的可行性。

黄铠教授基于李德毅院士提出的正态云模型，设计了一种支持数据染色的隐私保护方法，可用来保护文档、图像、视频、软件及其他类型的数据，其计算复杂度要远远低于传统加解密计算的复杂度。移动云服务中的基于假数据的轨迹隐私保护技术，通过添加假轨迹对原始数据进行干扰，同时保证被干扰的轨迹数据的某些统计属性不发生严重失真[40]。Zhang 等[41]利用掺沙子技术，通过加入一定量的伪造数据，来保护数据处理过程中的隐私。Heng[42]提出的基于虚拟信息的 PSIUM 干扰模型，通过隐私敏感信息稀释机制，实现了用户位置隐私的保护，但该干扰模式仅局限于稀疏用户环境。倪

表 2 隐私保护技术的对比分析

代表技术	通用性	计算开销	数据缺损	隐私保护度
加密技术（DES、3DES、ADES、RSA、Diffe Hellman、ECC）	高	高	低	高
匿名技术（*k*-匿名、*L*-diversity 匿名、*T*-closeness 匿名）	高	中	中	高
混淆技术（添加随机变量、随机偏移值、错误数据、噪声）	中	低	高	中

巍伟等人[43]针对隐私保护聚类问题，提出一种隐私保护数据干扰方法 NETPA，对原始数据中数据点的领域主属性值用其 k 邻域集内数据点在该属性上的均值进行替换，能够在较好地维持原始数据 k 邻域关系的情况下达到保护原始数据隐私的目的。徐小龙等人[44]提出一种基于数据分割与分级的云存储数据隐私保护机制，先将数据合理分割为大小数据块，再分别将小块数据和大块数据部署在本地和异地，按数据不同的安全级别需求，联合采用数据染色和不同强度的数据加密技术进行数据染色或加密，以在保护云存储用户数据隐私的同时，提高灵活性，降低系统开销。可以将上述技术引入到移动云环境中，来增强隐私保护。

每类隐私保护技术都有不同的特点，在不同应用需求下，它们的适用范围、性能表现等不尽相同。从表 2 可以看出，当关注于对隐私的保护甚至要求实现完美保护时，基于加密的隐私保护技术比较合适，但需要较高的计算开销，尤其在分布式环境下还会增加通信开销。当针对特定数据实现隐私保护且对计算开销要求比较高时，则考虑基于混淆的隐私保护技术。而基于匿名的隐私保护技术可平衡各方面指标，能以较低的计算开销和信息缺损实现隐私保护。

在移动云环境中需要根据不同的需求考虑运用不同的隐私保护技术，而目前有关移动云服务中隐私保护的研究工作主要关注于从云服务提供商的角度建立隐私保护策略，却忽视了用户对云服务环境中隐私安全的个性化需求和隐私保护需求的动态特性。运用加密和访问控制策略等安全保障机制一般只能保护用户数据的直接隐私，然而可能导致隐私泄露的因素有很多，终端用户隐私保护需求千差万别，单纯依靠传统安全验证和管理策略还无法满足用户的潜在隐私保护需求。

5 结束语

本文从移动云服务及其在数据安全和隐私保护方面的研究进展进行了阐述和分析，虽然移动云服务的安全与隐私保护研究已经取得了一定的进展，但还有广阔的研究空间。笔者认为，今后的研究工作可侧重于以下几个方面。

1) 移动云服务质量与隐私保护之间的矛盾。在移动云服务中，用户使用基于云计算的服务时，需要提供自己的一些数据，数据的精确度越高，服务质量越好，而隐私度则越低，隐私保护和服务质量之间的平衡是一个挑战性问题。

2) 动态数据的安全与隐私保护。移动设备在社交网络上实时产生着大量的动态数据，数据模式和数据内容时刻都在发生着变化，而现有隐私保护技术主要基于静态数据集。鉴于攻击者利用数据的累积性、关联性去抽取、整合、分析、挖掘用户隐私数据的情况，如何在移动云环境下实现对动态数据的安全保障和隐私保护将更具挑战。

3) 建立完善的移动云安全技术框架、移动云服务安全标准及其测评体系。移动云安全框架必须在资源层、虚拟层、服务层、应用层考虑各种安全和隐私保护问题。保证数据从产生到消亡的全生命周期安全，应该包括安全递交、安全存储、安全共享与访问、安全更新和安全销毁等阶段。建立安全指导标准及其测评技术体系也是实现移动云服务安全的一个重要支柱。

参考文献：

[1] 中国互联网络信息中心.第 31 次中国互联网络发展状况统计报告[R]. 北京: 中国互联网络信息中心, 2012.4-5.
China Internet Network Information Center. The 31th Statistical Report of China Internet Network Development State[R]. Beijing: China Internet Network Information Center, 2012.4-5.

[2] 吴吉义, 沈千里, 章剑林等. 云计算：从云安全到可信云[J]. 计算机研究与发展, 2011, 48(Suppl): 229-233.
WU J Y, SHEN Q L, ZHANG J L, *et al*. Cloud computing: cloud security to trusted cloud[J]. Journal of Computer Research and Development, 2011, 48(Suppl): 229-233.

[3] 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.
FENG D G, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2011, 22(1):71-83.

[4] 房秉毅, 张云勇, 徐雷. 移动互联网环境下云计算安全浅析[J].移

动通信, 2011, 9: 25-28.
FANG B Y, ZHANG Y Y, XU L. Briefly discuss on the secu ity of cloud computing in the mobile internet environment[J]. Mobile Communications, 2011, 9: 25-28.

[5] **吕慧**, **袁杰**, **肖悦等**. **改进的基于椭圆曲线加密的** 3G **认证与密钥协商协议**[J]. **计算机应用** 2012, 32(1): 58-60.
LV H, YUAN J, XIAO Y, *et al*. Improved ECC-based authentication and key agreement protocol for 3G communication[J]. Journal of Computer Applications, 2012, 32(1): 58-60.

[6] **傅建庆**, **陈健**, **范容等**. **基于代理签名的移动通信网络匿名漫游认证协议**[J]. **电子与信息学报** 2011, 33(1): 156-162.
FU J Q, CHEN J, FAN R, *et al*. A delegation-based protocol for anonymous roaming authentication in mobile communication network[J]. Journal of Electronics & Information Technology, 2011, 33(1): 156-162.

[7] LEE C, LI C, CHANG R. A simple and efficient authentication scheme for mobile satellite communication systems[J]. ternational Journal of Satellite Communications and Networking, 2012, 30(1): 29-38.

[8] CHOW R, JAKOBSSON M, MASUOKA R, *et al*. Authentication in the clouds: a framework and its application to mobile sers[A]. Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop (CCSW)[C]. Chicago, USA, 2010.1-6.

[9] **刘宴兵，刘飞飞**.**基于云计算的智能手机社交认证系统**[J].**通信学报**, 2012, 33(Z1): 28-34.
LIU Y B, LIU F F. Cloud computing based smartphone social authentication system[J]. Journal on Communications, 2012, 33(Z1): 28-34.

[10] YU S, WANG C, REN K, *et al*. Attribute based data sharing with attribute revocation[A]. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASI
Beijing, China, 2010.261-270.

[11] LI J, ZHAO G, CHEN X, *et al*. Fine-grained data access control systems with user accountability in cloud computing[A]. Proceedings of the 2th International Conference on Cloud Computing (C udCom)[C]. Indianapolis, USA, 2010.89-96.

[12] **邵俊**. **代理重密码的研究**[D]. **上海**: **上海交通大学，** 2007.
SHAO J. Proxy Re-cryptography Revisited[D]. Shanghai: Shanghai Jiaotong University, 2007.

[13] ECHEVERRIA V, LIEBROCK L M, SHIN D. Permission management system: permission as a service in cloud computin A]. The 34th Annual IEEE Computing Software and Applications Conference Workshops (COMPSAC)[C]. Seoul, South Korea, 2010. 371-375.

[14] **熊庭刚，卢正鼎，张家宏**. **移动自组网的访问控制技术研究**[J]. **计算机科学**. 2011, 38(4): 72-75.
XIONG T G, LU Z D, ZHANG J H. Research on access control technology on mobile ad-hoc networks[J]. Computer Science, 2011, 38(4): 72-75.

[15] UNAL D, CAGLAYAN M U. A formal role-based access control model for security policies in multi-domain mobile networks[J]. Computer Networks, 2013, 57(1): 330-350.

[16] SHIN J, KIM Y, PARK W, *et al*. DFCloud: a TPM-based secure data access control method of cloud storage in mobile devices[A]. The 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings (CloudCom)[C]. 2012.

[17] YUN A, SHI C, KIM Y. On protecting integrity and confidentiality of cryptographic file system for outsourced storage[A]. Proceedings of the first ACM Cloud Computing Security Workshop (CCSW)[C]. Chicago ,USA,2009. 67-76.

[18] **杨翠**, **谭成翔**. **远端非可信平台** agent **完整性保护机制研究与设计**[J]. **计算机应用**, 2009,(11): 3001-3004.
YANG C, TAN C X. Research and design of agent integrity protection mechanism on remote untrusted platform[J]. Journal of Computer Applications, 2009,(11): 3001-3004.

[19] JUELS A, KALISKI J B S. Pors: proofs of retrievability for large files[A]. ACM Conference on Computer and Communications Security (CCS)[C]. Virginia, USA, 2007.584-597.

[20] ATENIESE G, BURNS R, CURTMOLA R, *et al*. Provable data possession at untrusted stores[A]. ACM Conference on Comp and Communications Security (CCS)[C]. Virginia, USA ,2007. 598-609.

[21] ATENIESE G, DIPIETRO R, MANCINI L V, *et al*. Scalable and efficient provable data possession[A]. Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (SecureComm'08)[C]. ACM: NewYork, NY, USA, 2008. 1-10.

[22] ZENG K. Publicly verifiable remote data integrity[A]. 10th International Conference on Information and Communication Securit (ICICS)[C]. Birmingham, UK, 2008. 419-434.

[23] **李涛**, **胡爱群**. **可信模块与强制访问控制结合的安全防护方案**[J]. **东南大学学报**:**自然科学版**, 2011, 41(3): 513-517.
LI T, HU A Q. Security protection scheme using mobile usted module and mandatory access control[J]. Journal of Southeast University (Natural Science Edition), 2011, 41(3): 513-517.

[24] **李磊**, **侯方勇**, **陈建勋**. **移动可信平台的发展与研究**[J]. **电脑知识与技术**, 2010(8): 1833-1835.
LI L, HOU F Y, CHEN J X. The development and research f mobile trusted platform[J]. Computer Knowledge and Technology, 2010(8): 1833-1835.

[25] SENY K, KRISTIN L. Cryptographic cloud storage[A]. Proceedings of the 14th International Conference on Financial cryptograpy and Data Security[C]. Canary Islands, Spain, 2010.136-149.

[26] CRAIG G. Fully homomorphic encryption using ideal lattices[A]. Proceedings of the 41th Annual ACM Symposium on Theory of Computing (STOC)[C]. Bethesda, MD, USA, 2009.169-178.

[27] ANANTHI S, SENDIL M S, KARTHIK S. Privacy preserving keyword search over encrypted cloud data[A]. Advances in Computing and Communications[C]. 2011.480-487.

[28] HU H, XU J, REN C, *et al*. Processing private queries over untrusted data cloud through privacy homomorphism[A]. Proc of the 27th IEEE International Conference on Data Engineering (ICDE)[C]. Hannover, Germany,2011.

[29] CAO N, WANG C, LI M, *et al*. Privacy-preserving multi-keyword ranked search over encrypted cloud data[A]. Proc of the 30th IEEE International Conference on Computer Com munications (INFOCOM)[C]. Shanghai, China, 2011.829-837

[30] **侯清铧**, **武永卫**, **郑祎民等**.**一种保护云存储平台上用户数据私密性的方法**[J]. **计算机研究与发展**.2011, 48(7):1146-1154.
HOU Q H, WU Y W, ZHENG W M, *et al*. A method on protection of user data privacy in cloud storage platform[J]. Journa of Computer Research and Development, 2011, 48(7): 1146-1154.

[31] **黄汝维，桂小林，余思等**. **云环境中支持隐私保护的可计算加密方法**[J]. **计算机学报**, 2011, 34(12): 2391-2402.
HUANG R W, GUI X L, YU S, *et al*. Privacy-preserving computable

encryption scheme of cloud computer[J]. Chinese Journa of Computers, 2011, 34(12): 2391-2402.

[32] WANG W, LI Z, OWENS R, *et al*. Secure and efficient access to outsourced data[A]. Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW)[C]. Chicago, USA, 2009.55-65.

[33] ZHOU Z, HUANG D. Efficient and secure data storage operations for mobile cloud computing[A].2012 8th International Conference on Network and Service Management (CNSM)[C]. Las Vegas, USA, 2012. 37-45.

[34] TYSOWSKI P K, HASAN M A. Re-encryption-based key management towards secure and scalable mobile applications i clouds[R]. IACR Cryptology ePrint Archive, 2011.

[35] SHIN Y, SHIN S, KIM M, *et al*. A secure self-encryption scheme for resource limited mobile devices[A]. Proc of the International Conference on IT Convergence and Security[C]. Pyeong Chang, Korea, 2013. 121-129.

[36] SAMARATI P, SWEENEY L. Protecting privacy when disclosing information: *k*-anonymity and its enforcement through generalization and suppression[J]. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002, 10(5):557-570.

[37] WONG R C, LI J, FU A W, *et al*. (*α*, *k*)-anonymity: an enhanced *K*-anonymity model for privacy-preserving data publishing[A]. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining(SIGKDD)[C]. Philadelphia, PA, USA, 2006.754-759.

[38] MACHANAVAJJHALA A, GEHRKE J, KIFER D, *et al*. *L*-diversity: privacy beyond k-anonymity[J]. ACM Trans on Knowledge Discovery from Data (TKDD), 2007, 1(1):24-33.

[39] NINGHUI L, TIANCHENG L, VENKATASUBRAMANIAN S. *t*-closeness: privacy beyond k-anonymity and l-diversity[A]. Proceedings of the 23rd International Conference on Data Engi (ICDE)[C]. Istanbul,Turkey, 2007.106-115.

[40] LUPER D, CAMERON D, MILLER J A, *et al*. Spatial and temporal target association through semantic analysis and GPS data mining[A].Proceedings of the 2007 International Conference on Information & Knowledge Engineering (IKE)[C]. Las Vegas, 2007.251-257.

[41] ZHANG G, YANG Y, YUAN D, *et al*. A trust-based noise injection strategy for privacy protection in cloud[J]. Software: Practice and Experience, 2012, 42(4): 431-445.

[42] CHENG H S, ZHANG D, TAN J G. Protection of privacy in pervasive computing environments[A]. IEEE Computer Society[C]. Las Vegas, USA, 2005.

[43] **倪巍伟, 徐立臻, 崇志宏. 基于邻域属性熵的隐私保护数据干扰方法**[J]. **计算机研究与发展**, 2009, 46(3):498-504.
NI W W, XU L Z, CHONG Z H, *et al*. A privacy-preserving data perturbation algorithm based on neighborhood entropy[J]. urnal of Computer Research and Development, 2009, 46(3):498-504.

[44] **徐小龙, 周静岚, 杨庚. 一种基于数据分割与分级的云存储数据隐私保护机制**[J]. **计算机科学**, 2013, 40(2):98-102.
XU X L, ZHOU J L, YANG G. Data privacy protection mechani m for cloud storage based on data partition and classificati [J]. Computer Science, 2013, 40(2):98-102.

作者简介：

李瑞轩（1974-），男，湖北宜昌人，博士，华中科技大学教授、博士生导师，主要研究方向为系统安全、分布式计算、信息检索。

董新华（1976-），男，河南信阳人，华中科技大学博士生，主要研究方向为云计算和大数据管理、信息检索。

辜希武[通信作者]（1967-），男，湖北武汉人，博士，华中科技大学讲师，主要研究方向为系统安全、服务计算。E-mail: guxiwu@hust.edu.cn。

周湾湾（1989-），女，湖北宜昌人，华中科技大学硕士生，主要研究方向为云计算、大数据安全。

王聪（1991-），男，湖北武汉人，华中科技大学硕士生，主要研究方向为大数据安全、大数据管理。