计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2015.20140227
52(6):1362-1377, 2015

弹性移动云计算的研究进展与安全性分析

李鹏伟[1,2] 傅建明[1,2,3] 李拴保[1,2] 吕少卿[4] 沙乐天[5]
[1](武汉大学计算机学院 武汉 430072)
[2](空天信息安全与可信计算教育部重点实验室(武汉大学) 武汉 430072)
[3](软件工程国家重点实验室(武汉大学) 武汉 430072)
[4](综合业务网理论及关键技术国家重点实验室(西安电子科技大学) 西安 710071)
[5](南京邮电大学计算机学院 南京 210046)
(xu_pang@163.com)

Elastic Mobile Cloud Computing: State of the Art and Security Analysis

Li Pengwei[1,2], Fu Jianming[1,2,3], Li Shuanbao[1,2], Lü Shaoqing[4], and Sha Letian[5]
[1](*Computer School, Wuhan University, Wuhan* 430072)
[2](*Key Laboratory of Aerospace Information Security and Trusted Computing* (*Wuhan University*), *Ministry of Education*, *Wuhan* 430072)
[3](*State Key Laboratory of Software Engineering* (*Wuhan University*), *Wuhan* 430072)
[4](*State Key Laboratory of Integrated Services Networks* (*Xidian University*), *Xi'an* 710071)
[5](*School of Compter Science & Technology*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210046)

Abstract Elastic mobile cloud computing (EMCC) enables the seamless and transparent use of cloud resource to augment the capability of mobile devices by off-loading parts of mobile devices' tasks to cloud according to the real-time user requirement. By summarizing the service providing models of EMCC, we divide existing EMCC models into two categories: computing migration-mobile cloud computing(CM-MCC), in which the mobile devices employ the cloud to perform the parts of their computing intensive tasks; and cloud agent-mobile cloud computing(CA-MCC), in which the cloud maintains one or more virtual mobile devices for each mobile device and these virtual mobile devices are synchronized with the mobile device to complete various tasks such as computing, storage, security and communication instead of the mobile device. Then the applicable scenarios, the implementation method, the key issues, and the future research of EMCC models in each category are studied. After that, we analyze the critical security threats of EMCC, including users' error operations or malicious actions, malicious applications, communications security problems, and cloud computing security issues such as the vulnerabilities of virtual system, multi-tenant problems, malicious cloud service providers. The corresponding defenses of these threats are discussed. At last, we point out that security is a key issue for EMCC.

Key words mobile cloud computing (MCC); computing migration (CM); cloud agent (CA); virtual mobile device (VMD); security threats

摘 要 弹性移动云计算(elastic mobile cloud computing, EMCC)中,移动设备按照实时需求将部分任务迁移到云端执行,无缝透明的利用云资源增强自身功能.将现有EMCC方案分为雇佣云端完成部分

收稿日期:2014-03-14;**修回日期**:2014-07-14
基金项目:国家自然科学基金项目(61373168,61202387);高等学校博士学科点专项科研基金项目(20120141110002)
通信作者:傅建明(jmfu@whu.edu.cn)

计算密集任务的计算迁移型移动云计算(computing migration-mobile cloud computing, CM-MCC)和通过云端的虚拟移动设备来辅助或代替移动设备完成多种任务的云端代理型移动云计算(cloud agent-mobile cloud computing, CA-MCC)两类,分别对 CM-MCC,CA-MCC 的适用场景、实现流程、关键技术、存在问题及相应解决方法进行研究并指出其发展方向.对 EMCC 所面临的主要安全威胁,包括用户的错误操作或恶意行为、恶意代码、通信安全以及虚拟系统漏洞、多租户、不安全资源等云安全问题进行分析并研究相应防御方法,指出安全问题将是 EMCC 研究的重点和难点.

关键词 移动云计算;计算迁移;云端代理;虚拟移动设备;安全威胁

中图法分类号 TP393

电子商务、社交网络等传统计算机网络中的任务已经被广泛转移到移动网络,现实增强、移动金融/医疗/教育等新的任务也正在被逐步部署于智能移动设备和移动网络中.这些对计算、存储、安全等要求较高的任务是对现有移动设备的挑战:1)移动设备因受限于便携性、易用性、成本、散热等因素,其计算、存储、网络能力逊色于固定台式设备;2)计算密集型任务过快地消耗掉移动设备的电量,电量对移动设备应用时间和范围的制约日益凸显[1],电源的体积和重量等因素导致电量问题难以解决.

移动云计算(mobile cloud computing, MCC)中,数据处理可以在移动设备之外进行,移动设备作为客户端从云端获得计算、存储、网络、安全等服务,从而突破移动设备的性能、电量瓶颈,极大地扩展其使用范围.现有的 MCC 通常为客户端—服务器(client-server, CS)模式的 CS-MCC[2],由部署在移动设备中的客户端获取本地信息和用户输入,云端的服务器预先安装好相应软件提供各种具体服务.CS-MCC 通常属于软件即服务(software-as-a-service, SaaS),其客户端和云服务是紧耦合的[3],存在以下 2 个缺陷:1)移动设备网络连接的不稳定性可导致任务无法完成;2)云端和移动设备只能以单一的协同方式完成任务,不能满足移动设备性能多样性、用户需求变化性的要求.例如同一任务,有的移动设备需要云端协助,有的移动设备则可自行完成;移动设备用户有不同的服务质量需求,如安全、计算时间、电量和流量等方面的要求.

为了能够更加灵活、高效地利用云端的计算资源,文献[4-16]实现了计算迁移(computing migration, CM)模式的 CM-MCC.类似于网络觅食(cyber foraging)[17],CM-MCC 中移动设备保管完成任务所需要的所有数据和代码.当未连接到云端时,移动设备自行完成计算;当连接到云端时,移动设备将计算量较大的部分任务迁移到云端,雇用云端来完成计算,以节省电量、提高运算速度.云端提供平台即服务(platform-as-a-service, PaaS),为移动设备上传的任务提供执行环境.在计算过程中,移动设备可以依照具体执行环境(网络状况、电量、任务性质、用户模式等)的变化对任务的分配进行实时调整.CM-MCC 主要适用于计算量大、数据交互量小的移动应用,如图像处理、目标识别等.

文献[18-23]实现了云端代理(cloud agent, CA)模式的 CA-MCC.CA-MCC 在云端维持与移动设备同步的一个或多个虚拟移动设备(virtual mobile device, VMD),VMD 作为移动设备的云端代理,协助或代替移动设备完成部分计算、存储、安全、通信等任务.CA-MCC 可以拉近移动设备和云的距离,在节省电量、提高计算能力的同时提供更多种类、更大范围的服务.VMD 由用户管理,云端提供基础设施即服务(infrastructure-as-a-service, IaaS),为 VMD 的运行提供硬件支持.

图 1 描绘了以上 3 种 MCC 模式.CS-MCC 中,用户 U_1,U_2 通过特定移动应用的客户端向云端发出请求,云端进行响应,二者依照一种固定的合作模式完成任务;用户 U_3,U_4 采用 CM-MCC,移动设备将各个任务中的计算密集模块发往云端,雇用云端来完成一部分计算;CA-MCC 用户 U_5,U_6 在云端维持与移动设备同步的 VMD,由 VMD 代替或协助移动设备完成任务.

与 CS-MCC 相比,CM-MCC 和 CA-MCC 能够适应移动设备执行环境的多样性和动态性,由用户需求和运行环境决定任务是由云端还是移动设备来完成、哪些模块需要被分配到云端,并且在执行过程中任务分配可以随用户需求的变化而调整.CM-MCC 和 CA-MCC 中,移动设备对云端资源的索取是按需自助的、弹性可变的,且可以更好地支持并行计算和云端资源共享[6,8].本文称这类具有按需自助服务、高弹性计算、高效资源共享等特性的 MCC

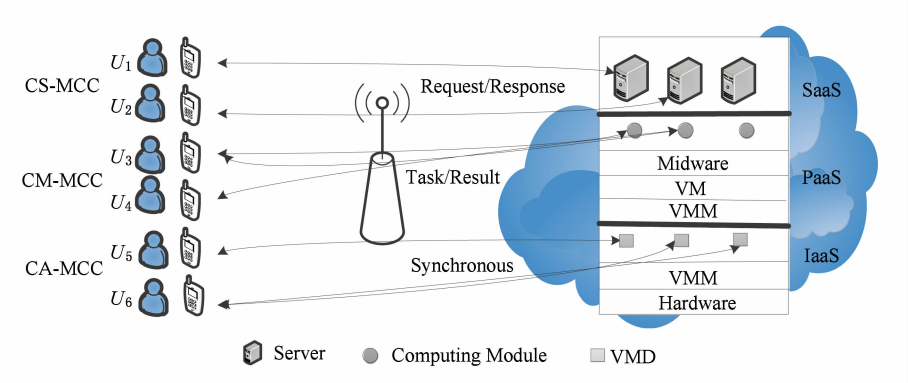


Fig. 1 CS-MCC, CM-MCC and CA-MCC.

图 1 CS-MCC, CM-MCC 和 CA-MCC

为弹性移动云计算(elastic mobile cloud computing, EMCC),其移动设备通过无线网络按需将任务迁移到云端,灵活高效地利用云端的计算、存储、网络等资源来完成任务.

安全问题一直是阻碍云计算发展的主要障碍[24],移动设备的移动性、开放性、不稳定性等使得 MCC 的安全问题比传统云计算更复杂. EMCC 还处于研究阶段,缺乏整体的安全框架[25-26],用户的错误操作和恶意行为、移动设备的系统漏洞和恶意代码、无线信道的脆弱性、云系统漏洞、多租户问题、云服务提供商(cloud service provider, CSP)窃取和出卖信息的行为等都可能会导致 EMCC 的数据处理过程被阻断、拦截或干扰,对当前 EMCC 系统构成安全威胁,阻碍 EMCC 的健康和快速发展.

本文首先总结新一代 MCC 的特性,提出 EMCC 概念,将现有 EMCC 分为 CM-MCC, CA-MCC 两类,提炼出各 CM-MCC 方案所共有的实现环节,分析各个环节面临的关键问题、解决这些问题的思路;然后对 CA-MCC 方案的实现流程、所能提供的各种服务、CA-MCC 与 CM-MCC 的区别与联系等进行总结;最后从数据处理角度分析了 EMCC 面临的主要安全威胁与相应防御方法,并指出下一步发展方向.

1 计算迁移

CM-MCC 实现方法通常可以分为云环境构建、任务分割、模块分配、模块迁移、计算、返回 6 个步骤. 图 2 的简单实例展示了后面的 5 个步骤:任务 Task 被分割为 A,B,C,D,E,F 这 6 个模块. 其中, A,F 被分配到移动设备;B,C,D,E 被分配并迁移到云端. 然后,依次执行各个模块,在执行过程中 E 被重新分配到移动设备执行.

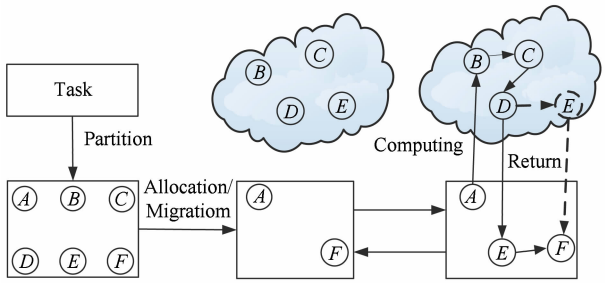


Fig. 2 An example of the computing process of CM-MCC.

图 2 CM-MCC 计算过程示例

1.1 云环境构建

可以利用公有云、本地的私有云或专用云、个人计算机(PC)、附近的移动设备等构建辅助移动设备执行程序的云环境.

公有云(如亚马逊、谷歌、微软、百度、腾讯等)拥有近乎无限的资源,但其 EMCC 服务质量受到 2G/3G/4G 网络与多跳的广域网带宽、延时的影响[27],且存在用户对服务商的半信任问题[28]. 为此,文献[17,20,24]利用本地云服务器或本地 PC 来提供计算服务.

本地云服务器或本地 PC 通常被部署于学校、单位、小区或家庭内,是用户较为信任的资源. 移动设备可以通过 WIFI 直接连接到本地云服务器或 PC 构建的云端,WIFI 的带宽通常要比 3G 高 2 个数量级,其延时、抖动等也可以控制在一定范围内[27],因此本地云端可以提供较高质量的服务. Cloudlet[27]利用本地的一个或者多个计算机构建云环境. 文献[20]中,部署在 PC 上的 Android 虚拟机可以为移动设备提供计算服务. RoseMic[23]利用空闲 PC 为移动设备提供计算支持,其文本搜索、面部识别等任务的实验结果显示本地云的响应速度比 Amazon EC2 云快 3~4 倍. 另外,EMCC 可以采用移动设备、本

地云、公有云的"3级"架构,本地云作为提供EMCC服务的第一选择,当本地云无法满足计算需求时,移动设备也可雇用公有云完成计算任务.

除本地云和公有云外,移动设备用户可以开放自己的移动设备,多个移动设备构成虚拟云平台.这样,每个移动设备都可以连接到虚拟云,通过虚拟云完成计算或存储任务.文献[14-15]利用部署在移动设备上的Hadoop来完成分布式的任务执行和数据存储.MobiCloud[16]利用移动设备构建移动自组织网络,提供传感、存储、计算等服务;同时,MobiCloud提供了风险管理、可信管理、安全路由等功能,但没有考虑机会网络的安全问题[29]以及云端节点可能面临的安全威胁.这种虚拟云模式主要用于数据采集、信息分享.但是,相同区域的用户具有相似的分享需求[16]不足以打动设备用户开放自己的资源,因此,需要研究如何激励移动设备用户加入到虚拟云中.

为移动设备提供云计算支持的可以是多个云服务提供商[30],还可以是多种资源的混合体,将来的发展方向是由公有云、本地云、本地PC、附近移动设备等协同构建动态的资源池,并支持各资源之间的任务迁移、用户信息的共享等.如何高效地构建动态资源池和按需实现任务的动态迁移是一个开放的研究方向.

1.2 任务分割

任务分割即将任务分为若干个可执行模块并分别标注各个模块是否可以被迁移到云端执行.现有研究中的分割方法可分为基于设计的分割、基于改写的分割和基于分析的分割.

1) 基于设计的分割.它是指设计适合在MCC中运行的、可分割的程序架构.文献[4]设计的移动应用由一个或者多个Weblet、用户界面(user interface, UI)和描述程序的声明组成.Weblet是一种可以独立完成特定功能的程序片段,并提供与其他Weblet或者UI交互的接口.Weblet可以在移动设备上执行,也可以在云端执行.MACCHIATO[10]为移动应用开发者提供脚本化的CM-MCC程序开发环境,相应程序可以通过特定中间件将给定的计算任务迁移到云节点执行.

2) 基于改写的分割.它是指改写或微调程序,并按照原移动应用程序的基本结构进行分割并标注模块是否可迁移.Thinkair[6]以Method为粒度对Java程序进行分割,提出面向MCC的Android程序开发方案,程序开发者对可迁移到云端的Method标注"@Remote".Cuckoo[31]可以借助Java虚拟机的支持,通过重写Java程序实现Android组件(如Activity, Service)粒度的分割.

3) 基于分析的分割.它是指对程序进行静态或者动态的分析,寻找合适的分割点.Clonecloud[5]对程序进行静态分析后,自动分割现有程序,可将部分线程迁移到到云端上执行.文献[11]依照Android程序的组件进行分割,可以把Service类组件迁移到云端.

表1列出了各种EMCC方案提供的不同方法、不同粒度的分割.基于设计的分割,其分割粒度较细,所开发程序比较可靠,对计算环境的要求也较为宽松,但短期内难以推广;基于改写的分割相对容易实现,但是云服务器和移动设备的指令集架构可能不同(例如前者通常为x86,后者为ARM),需要在云端提供支持模块执行的环境;基于分析的分割更容易实现,但需要更多的分割时间,有可能出现错误[32],而且需要云端提供执行环境:除了提供基本执行环境外,还需要将移动设备当前的系统状态、被迁移模块可能用到的数据等全部复制到云端.考虑任务的粒度、长度、计算量、包含的敏感信息、拥有的权限、可能计算成本以及各任务之间的数据关联、控制关联等因素,设计支持任务分割的程序开发方法实现最优的任务分割是将来的研究方向.

Table 1 Examples of Task Partition

表1 任务分割示例

Framework	Module	Partition Method	Execution Environment in Cloud
Weblet	Weblet	Redevelop	Linux Server
MACCHIATO	Component	Redevelop	Middleware
Thinkair	Method	Rewrite	Android x86
MAUI[7]	Method	Rewrite	Microsoft .NET Framework
CaaS[8]	Component	Rewrite	Component
μCloud[12]	Component	Rewrite	Component
Clonecloud	Thread	Analyze	Application-Layer VM
Opportunistic Offloading[11]	Component	Analyze	Android x86
Comet[13]	Thread	Analyze	Application-Layer VM

1.3 模块分配

分割后的任务是由一个或者多个模块构成,模块可以在云端或者本地执行.模块分配指确定哪些模块在哪个时间点被迁移到云端的过程.

与固定设备相比,移动设备程序的执行环境更

具动态性和多样性. 不同时间,其网络状况(带宽、信号质量、空闲程度、通信开销)、电量、CPU 利用率等各不相同;不同任务,用户预期的执行时间、执行效果各不相同. 例如象棋游戏中,用户可能会期待最快的响应速度;病毒扫描时,用户可以接受较长的运行时间,但期待能够节省电量. 因此,模块分配应当是随时间变化的,由执行环境、用户期待、模块属性等共同决定具体的分配情况.

图 3 总结模块分配的过程:1)通过监控或者测试得到设备的 CPU、网络、电量等执行环境参数,通过询问用户、分析程序等方式得到整体任务属性、各个模块的属性. 2)根据环境参数、任务属性、模块属性得到最优的执行配置. 其中,模块属性包括执行模块需要消耗的电量、时间、实施和迁移模块的带宽成本等. 分配目标通常为最少的运算时间、电量、消耗、或者费用等,可以由用户指定,如将当前分配模式设定为"最快模式"或者"最省电模式". 同时,还需要考虑到设备参数(如内存或 CPU 上限)的约束. 另外,历史分配记录可用来辅助作出判断. 3)在执行过程中,如果各项输入的变化超过阈值(如用户指定模式改变或者网络带宽、电池电量等的变化超过一定阈值),则重新进行模块分配.

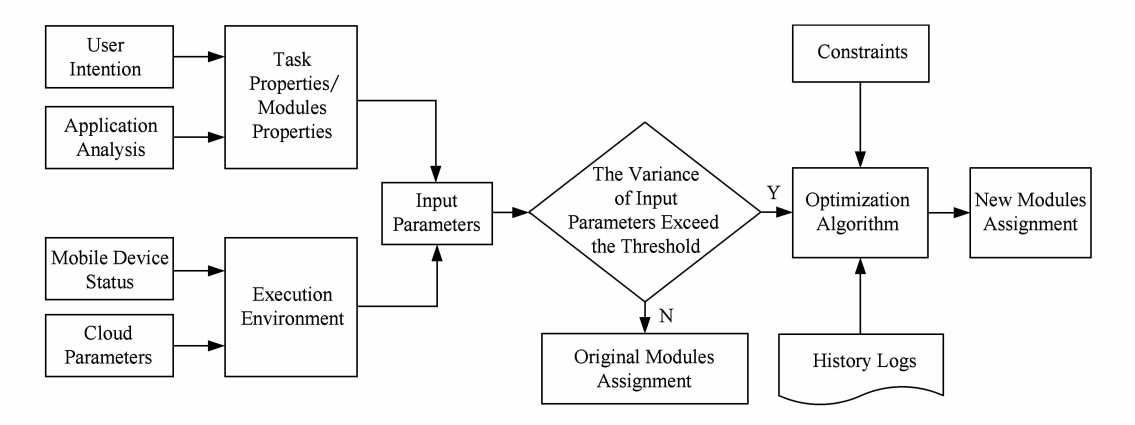


Fig. 3 Modules allocation.

图 3 模块分配

表 2 列出了现有 CM-MCC 中的动态分配方案的目标、输入、求解方法. 现有分配方案主要存在以下 5 个问题:1)现有各方案目标、输入(考虑的条件)、实验方法各不相同,缺乏标准化. 2)现有研究往往忽视了模块的计算成本. 3)难以准确获取能源消耗情况. 移动设备方面,文献[33]认为目前 EMCC 研究中对系统中特定负载引起的能量消耗的估计是不准确的;云端由于虚拟化层的存在,同样难以精确获得硬件的能耗数据[34]. 4)网络不稳定可能会大幅度增加分配成本. 每次网络状态的变化都可能会导致重新分配,导致大量额外的电量消耗. 5)安全性也应作为模块分配的一个目标,应减少安全要求较高的模块被迁移到云端. 模块分配是一个优化问题,其解取决于输入(刻画执行环境、目标、任务属性等的参数)和约束条件(为安全而进行的限制、资源上限等),文献[35]对该问题进行了基本的形式化描述. 针对特定的程序和用户需求生成具有对环境的自适应能力的最优分配方案是一个开放的研究方向.

Table 2 Examples of Modules Assignment

表 2 CM-MCC 分配方案示例

Framework	Objectives	Resource Monitoring	Optimization Algorithm
Weblet	Energy Saving, High Speed, Low Cost	Application Workload, Connection Quality, Device Loads	Machine Learning Techniques
MAUI	Energy Saving	Network Bandwidth, Battery Level	Linear Optimization
Clonecloud	Energy Saving, High Speed	Network Bandwidth, CPU Level	Linear Optimization
Thinkair	Energy Saving	Network Bandwidth, Hardware Status	PowerTutor Model[36]
Calling the Cloud[37]	High Speed	Data Exchange, Memory Cost, Code Size	ALL/K-Step Algorithm
CaaS	Max Throughput	CPU Level, Network Bandwidth	Genetic Algorithm
Code Offloading[38]	Energy Saving, High speed, Cloud Computing Cost	Network Bandwidth, Cloud Parameters, Mobile Device Parameters	Fuzzy Logic Decision Model

1.4 模块迁移

将一个或多个被分配到云端的模块从移动设备迁移到云端通常包括以下5个步骤:1)暂停模块,保存当前状态;2)将模块压缩并加密;3)将加密数据通过无线网,以TCP,HTTP,HTTPS等方式传到云端;4)云端解密、解压接收到的数据;5)重新运行模块.

模块迁移主要解决迁移的效率、成本和安全问题.无线网络的不稳定性和随机性直接影响模块迁移的时间/电量成本.对此,文献[39]提出了一种基于李雅普诺夫优化的数据传输策略,通过改进网络连接利用方式减小模块迁移时的电量消耗.模块在迁移过程中可能被窃听、劫持、修改等,因此需要对安全要求较高的模块进行加密和签名.

1.5 模块执行

模块执行即依次执行被分配到移动设备和云端的各个模块,可以通过并行计算来提高计算速度,通过资源共享来提高资源利用率.

Weblet设计了分离、聚合等执行模式,并通过实验证明并行执行可显著提高计算效率;Thinkair可以通过同时征用多台虚拟机进行并行计算提高计算速度.另外,移动终端还可以将同一任务同时发往不同云,通过并行执行实现错误/攻击容忍和延时控制.

CM-MCC既可以共享计算资源,也可以共享数据资源.Thinkair的模块被封装到应用层的Dalvik虚拟机,这种情况下来自不同用户的多个Dalvik虚拟机可以共享同一台Android虚拟机.在文献[8]所述CM-MCC方案中,云端保存常用的公共模块,节约了移动终端上传模块的成本.在MobiCloud中,同一区域的移动设备可以共享GPS等信息.

当来自多个用户的模块访问共享资源时,可能会出现网络拥塞、资源占用、隐私泄露、多租户问题等.对于物理资源访问拥塞,文献[40]设计了虚拟机迁移方案,通过虚拟机在不同云间的迁移来平衡负载.其他安全和隐私问题在第3节介绍.

1.6 结果返回

云端模块执行完毕后,将结果返还给移动设备.其返回的结果可以是阶段性的,也可以是最终的.

云端计算环境或者传输信道可能会出现故障或遭受攻击而导致计算结果出错,因此EMCC需要错误容忍、结果校验机制.文献[41]为EMCC设计了容错机制,通过资源状态的历史记录预测其变化情况,从而制定恰当的分割分配策略,减小结果出错的可能.目前对分布式计算结果进行检验的方法很多[42-43],但这些方法往往计算量较大、实现成本较高,不易部署到EMCC中.

现有CM-MCC在节省电量、提高计算速度方面取得了良好的实验效果,证实了CM-MCC的可行性.但由于未能准确获取移动用户需求[44],各方案的目标各不相同,难以进行精确比较.实行计算转移本身,如数据传输、加密解密、分析分割等都需要消耗电量,代码迁移需要消耗带宽,云端的计算服务通常需要付费,现有研究往往没有对实施计算迁移本身的电量消耗、资费消耗进行全面考虑[35,45-46].

2 云端代理

云端代理式移动云计算CA-MCC利用部署在云端的移动设备虚拟机VMD减轻移动设备负载、透明地扩展其功能.CA-MCC的基本实现过程可分为云代理构建、同步维持、代理服务、结果返回4个步骤.

2.1 云代理构建

这里的云代理构建包括云计算资源构建和云代理生成.其中,云计算资源的构建与1.1节中CM-MCC的云计算资源构建相同.

云代理生成方面,CA-MCC需要在云端部署与用户移动设备相匹配的VMD,即将移动设备中的系统状态、应用程序、用户信息等都复制到VMD.这一复制过程只需要进行一次,可以通过无线网络实现,也可以通过有线连接实现.

2.2 同步维持

移动设备中的信息是不断变化的,需要按照一定时间间隔对VMD和移动设备进行同步.增量同步是现有EMCC方案中较好的同步方法[1]:移动设备预先计算并保存各文件的Hash值,同步时利用Hash值找出该时间间隔内文件发生改变的部分;然后将该部分数据进行压缩、加密并通过无线网络传送到VMD;最后由VMD解密、解压接收到的信息,并依照这些数据对自身文件进行相应修改.增量同步虽然避免了在文件发生变化时传送整个文件或目录,但由于移动终端系统文件数据较为庞大,维持同步仍然需要消耗较多的流量和电量.

移动设备的状态变化通常由用户输入或者网络输入引发.文献[47]中的实验证实,对于初始状态相同的移动设备MD_1,MD_2,对MD_2重放MD_1所接收的用户输入和网络输入即可使MD_2与MD_1保持同步.因此可以研究基于事件重放的高效同步机制.

2.3 代理服务

VMD 相当于一个移动设备克隆体,可代替或协助移动设备参与计算服务、存储服务、安全服务、通信服务等.

计算服务的整个实现流程与 CM-MCC 中的 Clonecloud, Thinkair 类似. CA-MCC 在云代理构建时迁移了所有模块,节约了 CM-MCC 中模块的动态迁移开销.因此,各模块更倾向于在云端执行,更好地节省移动设备的电量、提高计算速度.

CA-MCC 可以提供多种类型的、个性化的存储、缓存服务,具体如下:

1) 基本信息存储.例如可以将智能手机中的大文件、通讯录等拷贝到 VMD 中,手机丢失/损坏后,能够通过口令拷贝出这些信息.由于虚拟机提供的隔离机制,在 VMD 中储存文件比传统移动云存储更为安全[48].

2) 状态存储.由于虚拟机具有重放功能[49],VMD 可以用来保存多个移动设备状态,例如可保存当前打开的多个程序或文档、游戏进度、常用的某个移动设备状态等.

3) 信息缓存. VMD 可以在同步时将多次接收的数据一次同步到移动设备,减少加密解密和建立网络连接的次数,从而减少移动设备的电量/流量消耗.

"安全即服务"是将安全服务放在云端进行,能够在增强安全服务更新能力和处理能力、提高安全服务质量的同时减少客户的计算代价.因移动设备计算能力相对较差,该服务在 MCC 中得到了非常广泛的应用[50],是未来移动设备安全软件的一个发展趋势.目前已有的"安全即服务"研究包括安全检测、版权保护、取证、认证等.例如,文献[51-52]将反病毒作为一项云服务,提供多个异构检测引擎,实现了高复杂度、可进化的反病毒系统;针对移动应用,文献[53]设计了基于云计算的数字版权管理系统;文献[54]为移动设备设计了基于云计算的取证工具;文献[55]提出了一个基于 MCC 的隐式认证框架.这些安全服务的主要特点是移动设备只需要维护一个负责信息收集与传输的客户端,而把反病毒引擎等计算密集的模块放在云端计算.

由于 VMD 是现实终端的镜像,VMD 可以方便地代替移动设备进行安全检测、病毒扫描等. CA-MCC 中,文献[51-55]等所述的安全服务可省去部署在移动设备的客户端信息收集和网络传输的开销. Secloud[56]在与移动设备同步的 VMD 中进行安全分析; Paranoid Android[57]利用多个 VMD 来实现多版本漏洞挖掘和攻击检测.另外,由于 VMD 的计算能力高于移动设备,而且可以实施 Android 强制访问控制机制[58-59]等高计算量的安全措施,VMD 安全性高于物理移动设备.

VMD 可以收集、存储大量的传感数据和用户行为数据,这些数据可以用来增加 EMCC 系统的安全性.例如,可以设置上下文相关的访问控制策略进行细粒度的访控[60]、利用用户行为数据进行异常检测[61]、身份认证[62]、可信扩展[63]等.基于 CA-MCC 的安全服务降低了移动设备的计算/能耗开销,提高了服务质量,也会产生新的安全应用和安全服务.

迁移到云端的任务模块可以直接通过云端的高速网络连接传输信息,实现网络通信服务.文献[64]在计算迁移、存储迁移的基础上更进一步提出了"通信迁移".每个移动设备拥有一个移动设备克隆体(clone),类似于 VMD,在这些克隆体之间建立 P2P 网络.这样,云端的 clone 之间可以进行端对端(clone to clone, C2C)的网络通信.该 C2C 架构得到了初步利用,如构建实时合作系统[65]、实现不需要可信第三方的位置信息保护系统[66].

VMD 还可以代替移动设备完成其他的数据处理工作. CDroid[19]利用云端的 VMD 提供应用安装、计算迁移、Cookie 保存、敏感信息保护、广告过滤、推送信息管理等服务.文献[67]提出虚拟手机屏幕设想,将手机屏幕渲染的部分工作转移到云端.文献[68]描述的移动设备虚拟桌面基础架构(virtual desktop infrastructure, VDI)场景中,云端的 VMD (Android x86)代替移动设备执行所有操作,移动设备只需显示云端传回的显示信息.

2.4 结果返回

VMD 完成计算任务后,将全部或者部分结果返还给移动设备.例如,VMD 处理完一组图片后,可以直接将这些图片上传到社交网,而不必下载到移动设备后再进行上传,从而节省移动设备的流量和存储空间.

与 CM-MCC 只需在有计算需求时向云端索取资源不同,CA-MCC 需要在云端维持一个与移动设备同步的 VMD.建立和管理 VMD 是较为复杂的[69],会给移动设备使用者带来较重的额外负担[70],而且 VMD 的运行和同步需要消耗较多的云端资源与移动设备电量、流量.文献[1]通过截获 Android 组件间通信数据、设置监控器等方式记录移动终端的数据变化,并通过增量同步方式同步到

云端,对同步维持的流量、电量成本进行考察,其结果显示:如果同步频率为 30 min/次,计算转移会增加移动设备 11%的电量消耗,数据备份会增加移动设备 8%的电量消耗.

CA-MCC 研究的关键内容如下:1)成本度量.对维持 VMD 的成本进行有充足数据支持的统计分析.2)同步优化.探究如何设定最优的同步间隔、同步方式与同步内容.3)多云合作.CA-MCC 可引入本地云,减少流量开销、上传到云端的敏感信息,实现快速的、可信的响应.4)服务扩展.用户拥有一个或多个 VMD,可以对现有 CA-MCC 中的计算、存储、安全、通信服务进行扩展,充分利用具有近乎无限的计算、存储、通信能力的 VMD.

现有文献[71-73]在对 MCC 进行总结时,均未区分计算迁移和云端代理.本文对这 2 种 MCC 模式加以区分:CM-MCC 是对 CS-MCC 的一种改进,适用于计算密集型任务;CA-MCC 则可代理计算、存储、安全、通信服务,适用于多种场景,但成本较高.

CM-MCC 和 CA-MCC 性能的比较如表 3 所示:

Table 3 The Performance Differences Between CM-MCC and CA-MCC

表 3 CM-MCC 和 CA-MCC 性能的比较

Performance Parameters	CM-MCC	CA-MCC
Main Goal	Energy Saving, High Speed Computing	Comprehensive Capability Augment
Cost	Low(Use Cloud Resource on Demand)	High(Maintain Mobile Device-Synchronized VMD)
Main Type of Cloud Service	PaaS	IaaS
Tasks	Computing Intensive Tasks	All Kinds of Tasks
Service Type	Computing	Computing, Storage, Communications, etc
Security of Computing	Low	High(Protected by Isolation Mechanism of VMD)
Uploaded Privacy Information	Less(Information in Uploaded Modules)	More(Almost all Information in the Mobile Device)
Sharing Resource	Share Execution Environment and Sharable Modules	Exclusive Execution Environment
Computing Speed	Lower(Need to Upload Modules before Computing)	Higher(In Most Cases, Does not Need to Upload Modules in the Process of Computing)

3 EMCC 的安全威胁

从数据处理角度,本节对在 EMCC 场景下危害更为凸显的安全问题、可能出现的针对 EMCC 的新威胁进行分析.限于篇幅,本文不全面介绍特定 EMCC 方案的安全缺陷[25]、传统移动网络[74-75]或者云计算[76]安全、数据存储安全[77]等.图 4 列出了 EMCC 面临的多种安全威胁,包括用户错误操作与恶意行为、移动设备恶意代码、云端安全等.

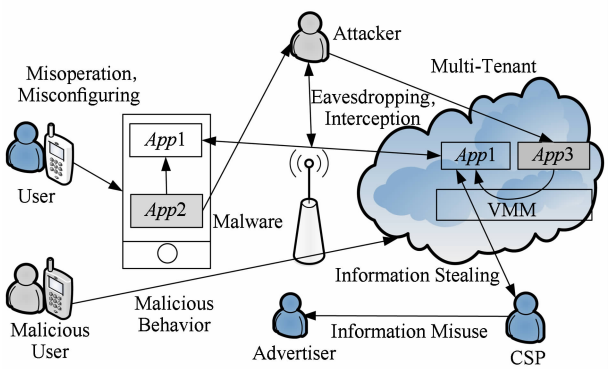


Fig. 4 Security threats of EMCC.

图 4 EMCC 面临的安全威胁

3.1 用户错误操作与恶意行为

移动用户安全意识较差且移动设备丢失或被借用的可能性较大,因此 MCC 中用户引发的安全问题比较多.同时,相对于 CS-MCC,EMCC 中用户所进行的操作、配置较多,所占用的资源也较多,更容易出现错误操作和恶意行为.

3.1.1 用户错误操作

移动设备用户的错误决策、配置、管理等有可能导致信息泄露、服务不可用等.例如,在安装移动应用时,Android 权限系统依托用户完成授权工作,是将授权与否的最终决策权交予没有专业知识的广大用户,降低了系统的安全性[78].在云计算环境中,用户往往需要通过设定配置文件来管理虚拟机,错误的配置有可能会造成敏感信息泄露[79].另外,用户在进行虚拟机镜像发布时,有可能泄露自身敏感信息;下载并使用镜像时,有可能会获得包含恶意代码或者敏感信息的镜像[80].

因此,EMCC 系统需要引导用户进行正确操作、消减用户错误操作带来的危害.例如,文献[81-82]等试图通过分析权限的具体使用方式、设计新的

访问控制方案等方法改善用户缺乏对权限理解导致的安全威胁.文献[79]提出一种基于信息流图的配置审计方法,该审计方法可以分析出用户的配置疏漏.文献[80]设计了一个云端虚拟机镜像管理系统,提供访问控制、镜像过滤、镜像追踪和镜像维护等一系列安全服务.

3.1.2 用户恶意行为

用户恶意行为包括2类:1)移动设备用户通过在云端执行恶意代码发起攻击、进行过量资源占用、利用云端资源非法牟利等.对此,防御方法主要是对用户行为进行监控和审计.例如,文献[61]在移动设备和云端分别设置监测点,在云端记录平均访问时间、资源使用情况、访问和认证方式等;在移动设备记录访问认证方式、流量电量等,依据这些数据来判断当前访问是否为异常.2)移动设备丢失或被盗后,别人可能会利用移动设备窃取云端的隐私信息、对云端数据进行恶意的损坏、随意消费云端资源或在利用云中C2C网络实施诈骗等,可通过身份认证来防御该威胁.相对于密码,在移动设备中用户更容易进行基于生物特征或者行为特征的认证[83],例如通过声纹、指纹、面部特征等从生理特征角度对用户进行认证或利用GPS信息、加速度信息、通话/游戏/网络行为等进行基于行为特征的身份认证[84].

3.2 移动设备恶意代码

移动设备的硬件[85]、操作系统[86]、应用程序[87]、通信链接[88]等各层次都存在安全缺陷.EMCC场景下,传统移动终端恶意代码可能会造成更大危害,同时有可能出现面向EMCC的新型恶意代码.

3.2.1 传统的移动设备恶意代码

移动应用的集中分发机制提高了其安全性[62],但移动设备仍面临预装恶意程序[85]、移动应用篡改等威胁.恶意代码被安装到移动设备后,有可能绕过权限机制直接进行信息窃取、扣费攻击、后门植入,也可能通过其他程序间接发起攻击.

由于EMCC程序具有网络通信和使用云资源的权限,很可能会成为恶意代码的攻击目标.移动设备通常为Android系统,而Android组件间通信缺少对信息流的监控,存在权限泄露、组件劫持等安全风险[89-90].同时,当前云服务也缺乏组件间的身份验证[91].如果将Android组件作为任务分割的模块(如文献[8,12]所述场景),则整个EMCC系统面临权限泄露和组件劫持威胁.如图5所示,程序1中组件A负责接收云端组件C返回的结果,如果A为公开组件,则恶意组件X有可能通过组件A间接调用云端组件B,C,实现数据窃取或控制流攻击;如果C通过隐式Intent返回信息,则存在恶意组件Y冒充A接收C信息的可能.因此,以组件或类似结构为模块的EMCC方案需要设计模块间验证机制或扩展现有研究中的组件劫持检测方案[90],将其部署到整个EMCC中.

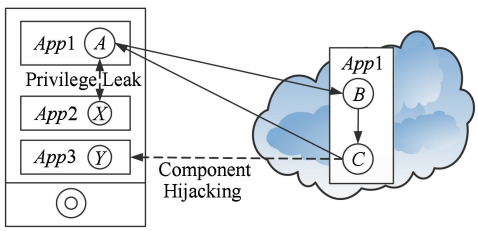


Fig. 5 Component hijacking and privilege leak of EMCC.

图5 EMCC中的权限泄露和组件劫持

云端的恶意代码有可能会对迁移到云端的模块或信息流进行修改,破坏程序执行过程的完整性.例如,假设模块A生成一系列参数,模块B利用这些参数对移动终端中的系统状态或者用户信息进行修改,如果A被迁移到云端后被修改,则可能导致B对移动终端系统或用户信息的修改是错误的.此类攻击可能会导致病毒蠕虫传播、系统状态和用户信息被破坏、网络钓鱼、扣费攻击、电子诈骗等.

3.2.2 EMCC恶意代码

由于EMCC程序动态迁移的特点,具有恶意功能的EMCC程序在移动终端执行可以绕过部分现有的Android权限机制,实现信息窃取、电子诈骗、病毒传播、拒绝服务攻击等.

通过恶意程序窃取信息通常包含信息获取与信息上传2个步骤.相应地,隐私保护的主要手段是控制信息获取和信息传输.例如,Android系统设置了控制信息获取、控制对外通信2类权限;现有研究通过权限组合判断是否存在隐私泄露的风险[92],跟踪敏感信息的传播过程从而检测信息泄露[93]等.对于EMCC程序来说,控制其信息获取与传统移动程序类似,但模块的迁移会带来突破权限限制的信息外传:包含敏感信息的模块一旦被迁移到云端,则可通过侧信道、共享文件等多种方法传出信息,上述敏感信息保护方法不再有效.被上传到云端的恶意EMCC模块带有移动设备用户的身份标识且具有通信能力,可以进行网络诈骗、病毒传播等.

另外,恶意 EMCC 程序有可能针对 EMCC 实现机制进行攻击,例如可以通过构造特殊代码,使得分割、分配需要非常大的计算量,从而大量消耗移动设备的电量/流量,实现拒绝服务攻击.

EMCC 恶意代码可以绕过传统访问控制,但是其恶意行为仍然具有"自动执行而非用户触发"的特点.因此,可将基于用户行为的资源访问控制方案[94-95]扩展、迁移到 EMCC 中,实现对 EMCC 程序恶意行为的检测和抑制.

3.3 通信安全

移动设备通常通过无线网络进行通信,其通信媒介(如 3G、WIFI、蓝牙等)容易被监听[96]或干扰抑制[97],攻击者可以进行信息窃取、信息屏蔽、拒绝服务等攻击.

EMCC 的云端 C2C 网络已具有社会网络的属性,需要从社会网络角度考虑其安全问题:1)组成社会网络图的各个元素均可能涉及到隐私信息,需要对结点隐私、边隐私、图性质隐私进行保护[98];2)移动网络病毒、蠕虫在社会网络中以指数速率迅速传播[99],整个社交网络会在很短时间内就被感染.安全防御方面,补丁分发可以采用 C2C 网络的传播方式,缩短漏洞的暴露时间[100].

3.4 云安全

大多数 EMCC 方案都建立在"云环境是安全的"假设之上[45].但是,相比 CS-MCC,EMCC 云端更为复杂、底层资源也更具多样性和动态性,其恶意 CSP 出现的可能性也更大,因此 EMCC 面临来自云端的虚拟系统漏洞、多租户、不安全资源、CSP 恶意行为等多种安全威胁.

3.4.1 虚拟系统漏洞

EMCC 中用户在云端运行自定义代码的权利为恶意用户或恶意软件攻击云端提供了便利.虚拟机管理器(virtual machine monitor,VMM)的漏洞可能会导致一个恶意用户控制其他用户的虚拟机.例如,2009 年 5 月网络上曾经曝光 VMware 虚拟化软件的 Mac 版本中存在一个严重的安全漏洞,别有用心的人可以利用该漏洞通过 Windows 虚拟机在 Mac 主机上执行恶意代码[28].相应防御措施主要有可信计算、VM 完整性验证等.在可信计算中,用户可以使用可信平台模块(trusted platform module,TPM)保证启动安全,但此类基于 Hash 的验证方法很难验证依赖输入或外部数据的程序,所以不能保证运行时安全.运行时安全防御可以通过监视系统信息、代码执行或者分析代码的控制流实现[26].但 EMCC 中的 VMD 与传统 VM 结构不同,且同步机制会对完整性验证造成干扰,将来需要为 EMCC 量身定制可信检验与 VMD 完整性验证机制.

3.4.2 多租户问题

资源的共享在实现服务成本下降和可扩展性提高的同时也带来巨大安全挑战:1)共享系统为安全威胁的快速蔓延提供了条件;2)多租户共享的特征给恶意租户攻击其他租户或自私租户恶意抢占资源提供了便利.多租户问题引发的旁路攻击往往能够利用共享资源绕开系统隔离,例如,Cache 因为位于 CPU 内核,通常不受 VMM 的直接控制,成为发起旁路攻击的常见媒介.

EMCC 中的多租户问题更为严重.特别是 PaaS 类 EMCC 中,迁移到云端的模块不仅需要和来自其他用户的模块共享 CPU、内存、时钟等云服务的底层资源,还需要共享 Android 系统底层的 Linux 内核、库、应用框架等为迁移到云端的模块营造执行环境而铺设的资源.对于攻击者,以上所有层次资源均可作为发起攻击的旁路通道[101-102].例如,文献[86]通过 Android 系统底层的进程文件、系统文件、流量统计等看似无害的共享资源推断出用户的真实身份、兴趣爱好、行车路线等隐私信息.如图 6 所示,移动设备 MD_1,MD_2 共享云端提供的 Android 虚拟机,则 MD_1 有可能利用模块 A 通过硬件、VMM、Linux 内核、库等各个层次的共享资源对 MD_2 的模块 N 进行信息窃取或拒绝服务攻击[103].现有防御方法,例如将共享细节模糊化、随机化[104]等,都仅作用于云服务器底层资源,不能防御 EMCC 中更上层的旁路攻击.

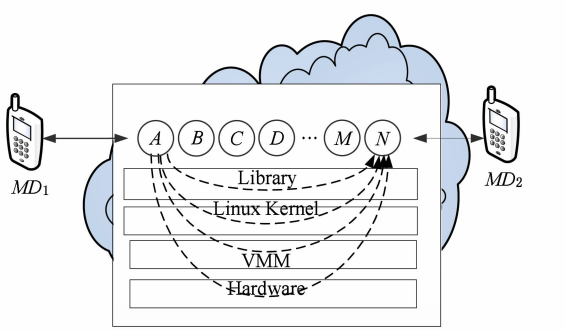


Fig. 6 Multi-tenant problem of EMCC.

图 6 EMCC 中的多租户问题

3.4.3 云端不安全资源

EMCC 中,CSP 既可以是公有云、本地云服务商,也可以是本地 PC、移动设备的拥有者,恶意 CSP 会出卖或窃取用户的信息.

用户使用基于 GPS/摄像/传感信息的服务时,

CSP 可能将移动设备所上传的信息出卖给广告商或进行其他非法利用[105]. 其相应防御方法主要有加密、隔离、设置特定的访问控制机制、过滤掉冗余信息或者设计新的服务模式[106]等. Mobicloud 将移动设备作为感知服务节点,引入可信第三方,实施基于身份的加密和基于属性的访问控制来保护用户信息. 文献[107]考虑电信商和 CSP 的串谋窃取信息的场景,设计了一种匿名的 MCC 业务模式. 文献[108-109]的研究证实,移动设备所提交的传感信息大部分是可以取代的. 因此,移动设备可以在上传信息前去除数据的敏感部分,尽可能减少隐私泄露的机会,例如 GPS 信息在用于天气预报时可以隐去细节信息,用于测定跑步距离时则可以隐去城市信息,设备号可以用随机数代替等[110].

由于移动设备保存有较多社会关系信息(如联系人、通话记录)、个人隐私信息(例如照片、短信)等,CSP 可能会试图窃取用户存储在云端或者在云端进行计算时所涉及的敏感信息. 加密、隔离等方法可以防止信息泄露. 全同态加密是云端信息泄露问题的一个有效解决方法,但目前软件算法还无法做到使用密文进行所有复杂计算. 虚拟机可以为用户提供一个完整的、隔离的个人计算环境,包括自定义的操作系统、软件、设置、数据等,可以提高用户数据的安全性,但同时会带来隐私数据的生命周期完整性[111]难以保证等安全问题. EMCC 中,由于移动设备和个人生活的强关联性,很多情况下移动应用的名称(例如反映用户健康状况、性取向的应用程序)和移动应用行为的相关细节(例如发微博的精确时间,攻击者有可能利用该时间得知用户的真实身份[86])也属于隐私信息. 若移动应用的计算模块在 CSP 所提供的计算平台执行(如图 6 所示场景),恶意 VMM 可轻易获取移动应用名称及其行为. 即使计算在隔离的 VMD 中进行,不同用户的移动应用和库不再共享 Linux 内核、库之类的信息,恶意的 VMM 仍然有可能通过监控 VMD 的网络流、CPU/内存使用情况推测出移动应用名称及其行为[86]. 为了防止迁移后代码的执行造成信息泄露,现有 EMCC 方案对本机数据的使用进行了限制,例如涉及本地数据的 Weblet 只能在本地执行[4]、在用到本机数据时将线程切换回移动设备[5],但这些限制会造成额外的开销;而且即使包含敏感信息的模块没有被迁移到云端,云端攻击者仍有可能通过关联模块中的特征数据推断出敏感信息.

不同的云资源,其安全性各不相同;不同移动任务的安全需求不同. 当云端的安全性无法满足任务的安全需求时,会引发安全威胁. 因此,应当避免将敏感信息传输到不安全的云端. 文献[112]针对多个终端的多种计算任务同时向云端迁移的场景,将计算迁移按迁移目的(节省电量、提高性能)、安全要求(用户隐私、企业隐私、非隐私)进行分类,并研究如何将这些任务分配到云端不同类型的计算提供者(安全的、不安全的). 文献[113]将云服务分为高危服务和常规服务,设计了基于 Semi-Markov 决策过程的安全服务管理模型来进行安全的服务分配. 对 EMCC 应用进行风险评估与安全分级,并在此基础上制定不同级别的安全防护策略是当前的一个研究热点.

当云服务的安全性难以得到保证时,可以引入信任评估机制[114],根据历史记录、反馈信息等帮助用户选择较为安全的云服务.

总之,CM-MCC 的主要安全威胁是难以保证各模块,特别是被迁移到云端的模块的安全性,这是因为其数据处理经历多个环节、模块之间共享多个层次的资源,攻击者具有宽广的攻击面,可以在多个层次、多个环节、通过多种手段发起攻击. CA-MCC 的主要问题是云端的 VMD 中包含有大量的用户隐私信息,CSP 难以保证并向用户证明这些信息的安全性. Gartner2009 年的调查结果显示,70%以上受访企业的 CTO 认为近期不采用云计算的首要原因在于存在数据安全性与隐私性的顾虑[28]. EMCC 中,如果不能妥善应对数据处理过程被阻断/拦截/干扰、敏感数据被泄露/非法利用等威胁,则用户可能因安全顾虑而放弃使用 EMCC. 因此,在研究云端资源池构建、EMCC 的程序设计、动态任务分配和协调的同时,移动设备、无线信道、云端的安全加固和安全协同防御是 EMCC 研究的关键内容之一.

4 总结与展望

EMCC 能够按需动态为移动设备提供云服务,透明、高效地利用云计算所提供的强大计算、存储能力能够弥补移动设备计算存储能力不足、电池电量有限等缺陷,拉近移动设备和云端的距离. 本文对各 EMCC 方案进行了总结、分类,并对其关键研究问题、发展方向进行研究;分析了 EMCC 面临的来自多个信息处理点(用户、移动设备、信道、云服务器、CSP)的多种类型(错误/恶意行为、漏洞、恶意代码、旁路攻击)威胁,指出安全问题是当前 EMCC 研究的重点和难点.

将来的工作中,需要研究面向 EMCC 的资源池构建、各类资源之间的协同、程序开发的标准和工具、成本模型、云端间数据交互与同步、服务扩展等.同时,需要根据 EMCC 所面临的各种安全威胁及其终端(性能电量有限的移动设备)、信道(稳定性安全性较差的无线信道)、云端(在多种资源基础上构建移动程序执行环境)的特点,设计具有较高安全性的 EMCC 方案以及 EMCC 安全加固方法.

参 考 文 献

[1] Barbera M V, Kosta S, Mei A, et al. To offload or not to offload? The bandwidth and energy costs of mobile cloud computing [C] //Proc of IEEE INFOCOM'2013. Piscataway, NJ: IEEE, 2013: 1285-1293

[2] Huang D, Xing T, Wu H. Mobile cloud computing service models: A user-centric approach [J]. IEEE Network, 2013, 27(5): 6-11

[3] De S, De S. Uncoupling of mobile cloud computing services: An architectural perspective [G] //AISC 243: Intelligent Computing, Networking, and Informatics. Berlin: Springer, 2014: 233-239

[4] Zhang X, Kunjithapatham A, Jeong S, et al. Towards an elastic application model for augmenting the computing capabilities of mobile devices with cloud computing [J]. Mobile Networks and Applications, 2011, 16(3): 270-284

[5] Chun B G, Ihm S, Maniatis P, et al. Clonecloud: Elastic execution between mobile device and cloud [C] //Proc of the 6th Conf on Computer Systems. New York: ACM, 2011: 301-314

[6] Kosta S, Aucinas A, Hui P, et al. Thinkair: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading [C] //Proc of IEEE INFOCOM'2012. Piscataway, NJ: IEEE, 2012: 945-953

[7] Cuervo E, Balasubramanian A, Cho D, et al. MAUI: Making smartphones last longer with code offload [C] //Proc of the 8th Int Conf on Mobile Systems, Applications, and Services. New York: ACM, 2010: 49-62

[8] Yang L, Cao J, Yuan Y, et al. A framework for partitioning and execution of data stream applications in mobile cloud computing [J]. ACM SIGMETRICS Performance Evaluation Review, 2013, 40(4): 23-32

[9] Rellermeyer J S, Riva O, Alonso G. AlfredO: An architecture for flexible interaction with electronic devices [C] //Proc of the 9th ACM/IFIP/USENIX Int Conf on Middleware. Berlin: Springer, 2008: 22-41

[10] Petitprez N, Rouvoy R, Filip K, et al. Opportunistic offloading of mobile applications in pervasive environments [C] //Proc of the 29th Symp on Applied Computing(SAC). New York: ACM, 2014: 1-6

[11] Chen E, Ogata S, Horikawa K. Offloading Android applications to the cloud without customizing Android [C] //Proc of IEEE PERCOM'2012. Piscataway, NJ: IEEE, 2012: 788-793

[12] March V, Gu Y, Leonardi E, et al. μCloud: Towards a new paradigm of rich mobile applications [J]. Procedia Computer Science, 2011, 5: 618-624

[13] Gordon M S, Jamshidi D A, Mahlke S, et al. Comet: Code offload by migrating execution transparently [C] //Proc of OSDI'2012. Berkeley, CA: USENIX Association, 2012: 93-106

[14] Huerta-Canepa G, Lee D. A virtual cloud computing provider for mobile devices [C] //Proc of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond. New York: ACM, 2010

[15] Marinelli E E. Hyrax: Cloud computing on mobile devices using MapReduce, CMU-CS-09-164 [R]. Pittsburgh, PA: Carnegie Mellon University, 2009

[16] Huang D, Zhang X, Kang M, et al. Mobicloud: Building secure cloud framework for mobile computing and communication [C] //Proc of SOSE'2010. Piscataway, NJ: IEEE, 2010: 27-34

[17] Balan R, Flinn J, Satyanarayanan M, et al. The case for cyber foraging [C] //Proc of the 10th ACM SIGOPS European Workshop. New York: ACM, 2002: 87-92

[18] Barbera M V, Kosta S, Mei A, et al. CDroid: Towards a cloud-integrated mobile operating system [C] //Proc of IEEE INFOCOM'2013. Piscataway, NJ: IEEE, 2013

[19] Barbera M V, Kosta S, Mei A, et al. Mobile offloading in the wild: Findings and lessons learned through a real-life experiment with a new cloud-aware system [C] //Proc of IEEE INFOCOM'2014. Piscataway, NJ: IEEE, 2014

[20] Chen E Y, Itoh M. Virtual smartphone over IP [C] //Proc of WoWMoM'2010. Piscataway, NJ: IEEE, 2010: 1-6

[21] Izumi M, Horikawa K. Toward practical use of virtual smartphone [C] //Proc of APSITT'2012. Piscataway, NJ: IEEE, 2012: 1-5

[22] Zhao B, Xu Z, Chi C, et al. Mirroring smartphones for good: A feasibility study [G] //Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 73: Mobile and Ubiquitous Systems: Computing, Networking, and Services. Berlin: Springer, 2012: 26-38

[23] Hassan M A, Chen S. An investigation of different computing sources for mobile application outsourcing on the road [G] //Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 93: Mobile Wireless Middleware, Operating Systems, and Applications. Berlin: Springer, 2012: 153-166

[24] Ren K, Wang C, Wang Q. Security challenges for the public cloud [J]. Internet Computing, 2012, 16(1): 69-73

[25] Khan A N, Mat Kiah M L, Khan S U, et al. Towards secure mobile cloud computing: A survey [J]. Future Generation Computer Systems, 2013, 29(5): 1278-1299

[26] Gu Q, Guirguis M. Secure mobile cloud computing and security issues [G] //High Performance Cloud Auditing and Applications. Berlin: Springer, 2014: 65-90

[27] Satyanarayanan M, Bahl P, Caceres R, et al. The case for vm-based cloudlets in mobile computing [J]. IEEE Pervasive Computing, 2009, 8(4): 14-23

[28] Feng Dengguo, Zhang Min, ZhangYan, et al. Study on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83 (in Chinese)
(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)

[29] Wu Yue, Li Jianhua, Lin Chuang. Survey of security and trust in opportunistic networks [J]. Journal of Computer Research and Development, 2013, 50(2): 278-290 (in Chinese)
(吴越, 李建华, 林闯. 机会网络中的安全与信任技术研究进展[J]. 计算机研究与发展, 2013, 50(2): 278-290)

[30] Kaewpuang R, Niyato D, Wang P, et al. A framework for cooperative resource management in mobile cloud computing [J]. IEEE Journal on Selected Areas in Communications, 2013, 31(12): 2685-2700

[31] Kemp R, Palmer N, Kielmann T, et al. Cuckoo: A computation offloading framework for smartphones [G] // Mobile Computing, Applications, and Services. Berlin: Springer, 2012: 59-79

[32] Ma X, Zhao Y, Zhang L, et al. When mobile terminals meet the cloud: Computation offloading as the bridge [J]. IEEE Network, 2013, 27(5): 28-33

[33] Yoon C, Kim D, Jung W, et al. Appscope: Application energy metering framework for Android smartphone using kernel activity monitoring [C] //Proc of USENIX'2012. Berkeley, CA: USENIX Association, 2012: 387-400

[34] Ye Kejiang, Wu Chaohui, Jiang Xiaohong, et al. Power management of virtualized cloud computing platform [J]. Chinese Journal of Computers, 2012, 35(6): 1262-1285 (in Chinese)
(叶可江, 吴朝晖, 姜晓红, 等. 虚拟化云计算平台的能耗管理[J]. 计算机学报, 2012, 35(6): 1262-1285)

[35] Chun B G, Maniatis P. Dynamically partitioning applications between weak devices and clouds [C] //Proc of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond. New York: ACM, 2010

[36] Zhang L, Tiwana B, Qian Z, et al. Accurate online power estimation and automatic battery behavior based power model generation for smartphones [C] //Proc of the 8th IEEE/ACM/IFIP Int Conf on Hardware/Software Codesign and System Synthesis. New York: ACM, 2010: 105-114

[37] Giurgiu I, Riva O, Juric D, et al. Calling the cloud: Enabling mobile phones as interfaces to cloud applications [G] //LNCS 5896: Middleware 2009. Berlin: Springer, 2009: 83-102

[38] Huber F, Srirama S. Adaptive code offloading for mobile cloud applications: Exploiting fuzzy sets and evidence-based learning [C] //Proc of the 4th ACM Workshop on Mobile Cloud Computing and Services. New York: ACM, 2013: 9-16

[39] Shu P, Liu F, Jin H, et al. ETime: Energy-efficient transmission between cloud and mobile devices [C] //Proc of IEEE INFOCOM'2013. Piscataway, NJ: IEEE, 2013: 14-19

[40] Gkatzikis L, Koutsopoulos I. Migrate or not? Exploiting dynamic task migration in mobile cloud computing systems [J]. IEEE Wireless Communications, 2013, 20(3): 24-32

[41] Park J S, Yu H C, Chung K S, et al. Markov chain based monitoring service for fault tolerance in mobile cloud computing [C] //Proc of WAINA'2011. Piscataway, NJ: IEEE, 2011: 520-525

[42] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers [G] //LNCS 6223: Advances in Cryptology-CRYPTO. Berlin: Springer, 2010: 465-482

[43] Xu G, Amariucai G, Guan Y. A lightweight argument system with efficient verifier [C] //Proc of CNS'2013. Piscataway, NJ: IEEE, 2013: 163-171

[44] Meng Xiangwu, Wang Fan, Shi Yancui, et al. Mobile user requirements acquisition techniques and their applications [J]. Journal of Software, 2014, 25(3): 439-456 (in Chinese)
(孟祥武, 王凡, 史艳翠, 等. 移动用户需求获取技术及其应用[J]. 软件学报, 2014, 25(3): 439-456)

[45] Rahimi M R, Ren J, Liu C H, et al. Mobile cloud computing: A survey, state of art and future directions [J]. Mobile Networks and Applications, 2014, 19(2): 133-143

[46] Shiraz M, Ahmed E, Gani A, et al. Investigation on runtime partitioning of elastic mobile applications for mobile cloud computing [J]. The Journal of Supercomputing, 2014, 67(1): 84-103

[47] Gomez L, Neamtiu I, Azim T, et al. RERAN: Timing-and touch-sensitive record and replay for Android [C] //Proc of the 2013 Int Conf on Software Engineering. Piscataway, NJ: IEEE, 2013: 72-81

[48] Huang D, Zhou Z, Xu L, et al. Secure data processing framework for mobile cloud computing [C] //Proc of INFOCOM WKSHPS'2011. Piscataway, NJ: IEEE, 2011: 614-618

[49] Flinn J, Mao Z M. Can deterministic replay be an enabling tool for mobile computing? [C] //Proc of the 12th Workshop on Mobile Computing Systems and Applications. New York: ACM, 2011: 84-89

[50] Yu Nenghai, Hao Zhuo, Xu Jiajia, et al. Review of cloud computing security [J]. Acta Electronica Sinica, 2013, 41(2): 371-381 (in Chinese)
(俞能海, 郝卓, 徐甲甲, 等. 云安全研究进展综述[J]. 电子学报, 2013, 41(2): 371-381)

[51] Oberheide J, Veeraraghavan K, Cooke E, et al. Virtualized in-cloud security services for mobile devices [C] //Proc of the 1st Workshop on Virtualization in Mobile Computing. New York: ACM, 2008: 31-35

[52] Khan A N, Kiah M L M, Madani S A, et al. Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing [J]. The Journal of Supercomputing, 2013, 66(3): 1687-1706

[53] Zou P, Wang C, Liu Z, et al. A cloud based SIM DRM scheme for the mobile Internet [C] //Proc of CCS'2010. New York: ACM, 2010: 759-761

[54] Lai Y, Yang C, Lin C, et al. Design and implementation of mobile forensic tool for Android smart phone through cloud computing [G] //Convergence and Hybrid Information Technology. Berlin: Springer, 2011: 196-203

[55] Chow R, Jakobsson M, Masuoka R, et al. Authentication in the clouds: A framework and its application to mobile users [C] //Proc of the 2010 ACM Workshop on Cloud Computing Security Workshop. New York: ACM, 2010: 1-6

[56] Zonouz S, Houmansadr A, Berthier R, et al. Secloud: A cloud-based comprehensive and lightweight security solution for smartphones [J]. Computers & Security, 2013, 37: 215-227

[57] Mansfield-Devine S. Paranoid Android: Just how insecure is the most popular mobile platform? [J]. Network Security, 2012, 2012(9): 5-10

[58] Bousquet A, Briffaut J, Clévy L, et al. Mandatory access control for the Android dalvik virtual machine [C] //Proc of ESOS'2013. Berkeley, CA: USENIX Association, 2013

[59] Smalley S, Craig R. Security enhanced (SE) Android: Bringing flexible MAC to Android [C] //Proc of NDSS'2013. Reston: Internet Society, 2013: 20-38

[60] Conti M, Nguyen V T N, Crispo B. CRePE: Context-related policy enforcement for Android [G] //Information Security. Berlin: Springer, 2011: 331-345

[61] Kim H J, Kim J Y, Kim J H, et al. A study on mobile cloud anomaly detection model [G] //Advanced Methods, Techniques, and Applications in Modeling and Simulation. Berlin: Springer, 2012: 210-216

[62] Gilbert P, Chun B G, Cox L P, et al. Vision: Automated security validation of mobile apps at app markets [C] //Proc of the 2nd Int Workshop on Mobile Cloud Computing and Services. New York: ACM, 2011: 21-26

[63] Kim M, Park S O. Trust management on user behavioral patterns for a mobile cloud computing [J]. Cluster Computing, 2013, 16(4): 725-731

[64] Kosta S, Perta V C, Stefa J, et al. Clone2Clone(C2C): Peer-to-Peer networking of smartphones on the cloud [C] //Proc of HotCloud'13. Berkeley, CA: USENIX Association, 2013

[65] Kosta S, Perta V C, Stefa J, et al. CloneDoc: Exploiting the cloud to leverage secure group collaboration mechanisms for smartphones [C] //Proc of IEEE INFOCOM'2013. Piscataway, NJ: IEEE, 2013

[66] Zhang H, Wen Y, Yu N, et al. Privacy-preserving computation for location-based information survey via mobile cloud computing [C] //Proc of ICCC'2013. Piscataway, NJ: IEEE, 2013: 100-105

[67] Lu Y, Li S, Shen H. Virtualized screen: A third element for cloud [J]. MultiMedia, 2011, 18(2): 4-11

[68] Nguyen T D, Huynh C T, Lee H W, et al. An Efficient Video Hooking in Android x86 to Reduce Server Overhead in Virtual Desktop Infrastructure [M] //Ubiquitous Information Technologies and Applications. Berlin: Springer, 2014: 107-114

[69] He S, Guo L, Guo Y. Elastic application container [C] //Proc of GRID'2011. Piscataway, NJ: IEEE, 2011: 216-217

[70] Shiraz M, Abolfazli S, Sanaei Z, et al. A study on virtual machine deployment for application outsourcing in mobile cloud computing [J]. The Journal of Supercomputing, 2013, 63(3): 946-964

[71] Fernando N, Loke S W, Rahayu W. Mobile cloud computing: A survey [J]. Future Generation Computer Systems, 2013, 29(1): 84-106

[72] Khan A, Othman M, Madani S, et al. A survey of mobile cloud computing application models [J]. IEEE Communications Surveys & Tutorials, 2013, 16(1): 393-413

[73] Dinh H T, Lee C, Niyato D, et al. A survey of mobile cloud computing: architecture, applications, and approaches [J]. Wireless Communications and Mobile Computing, 2013, 13(18): 1587-1611

[74] Yuan Jiabin, Wei Lili, Zeng Qinghua. Delegation based cross-domain access control model under cloud computing for mobile terminal [J]. Journal of Software, 2013, 24(3): 564-574 (in Chinese)
(袁家斌, 魏利利, 曾青华. 面向移动设备的云计算跨域访问委托模型[J]. 软件学报, 2013, 24(3): 564-574)

[75] Luo Junzhou, Wu Wenjia, Yang Ming. Mobile Internet: Terminal devices, networks and services [J]. Chinese Journal of Computers, 2011, 34(11): 2029-2051 (in Chinese)
(罗军舟, 吴文甲, 杨明. 移动互联网: 终端, 网络与服务[J]. 计算机学报, 2011, 34(11): 2029-2051)

[76] Modi C, Patel D, Borisaniya B, et al. A survey on security issues and solutions at different layers of cloud computing [J]. The Journal of Supercomputing, 2013, 63(2): 561-592

[77] Fu Yingxun, Luo Shengmei, Shu Jiwu. Survey of secure cloud storage system and key technologies [J]. Journal of Computer Research and Development, 2013, 50(1): 136-145 (in Chinese)

(傅颖勋, 罗圣美, 舒继武. 安全云存储系统与关键技术综述[J]. 计算机研究与发展, 2013, 50(1): 136-145)

[78] Felt A P, Ha E, Egelman S, et al. Android permissions: User attention, comprehension, and behavior [C] //Proc of the 8th Symp on Usable Privacy and Security. New York: ACM, 2012

[79] Bleikertz S, Schunter M, Probst C W, et al. Security audits of multi-tier virtual infrastructures in public infrastructure clouds [C] //Proc of the 2010 ACM Workshop on Cloud Computing Security Workshop. New York: ACM, 2010: 93-102

[80] Wei J, Zhang X, Ammons G, et al. Managing security of virtual machine images in a cloud environment [C] //Proc of the 2009 ACM Workshop on Cloud Computing Security. New York: ACM, 2009: 91-96

[81] Hornyack P, Han S, Jung J, et al. These aren't the droids you're looking for: Retrofitting Android to protect data from imperious applications [C] //Proc of CCS'2011. New York: ACM, 2011: 639-652

[82] Au K W Y, Zhou Y F, Huang Z, et al. Pscout: Analyzing the Android permission specification [C] //Proc of CCS'2012. New York: ACM, 2012: 217-228

[83] Furnell S, Clarke N, Karatzouni S. Beyond the pin: Enhancing user authentication for mobile devices [J]. Computer Fraud & Security, 2008, 2008(8): 12-17

[84] Al Ridhawi Y, Al Ridhawi I, Karmouch A, et al. A context-aware and location prediction framework for dynamic environments [C] //Proc of WiMob'2011. Piscataway, NJ: IEEE, 2011: 172-179

[85] Wu L, Grace M, Zhou Y, et al. The impact of vendor customizations on Android security [C] //Proc of CCS'2013. New York: ACM, 2013: 623-634

[86] Zhou X, Demetriou S, He D, et al. Identity, location, disease and more: Inferring your secrets from Android public resources [C] //Proc of CCS'2013. New York: ACM, 2013: 1017-1028

[87] Wang R, Xing L, Wang X F, et al. Unauthorized origin crossing on mobile platforms: Threats and mitigation [C] //Proc of CCS'2013. New York: ACM, 2013: 635-646

[88] Kim S H, Han D, Lee D H. Predictability of Android OpenSSL's pseudo random number generator [C] //Proc of CCS'2013. New York: ACM, 2013: 659-668

[89] Chin E, Felt A P, Greenwood K, et al. Analyzing inter-application communication in Android [C] //Proc of the 9th Int Conf on Mobile Systems, Applications, and Services. New York: ACM, 2011: 239-252

[90] Fu Jianming, Li Pengwei, Yi Qiao, et al. A static detection of security defects between inter-components' communication [J]. Journal of Huazhong University of Science and Technology: Nature Science Edition, 2013, 11(2): 259-264 (in Chinese)
(傅建明, 李鹏伟, 易乔, 等. 一种 Android 组件间通信的安全缺陷静态检测方法[J]. 华中科技大学学报: 自然科学版, 2013, 11(2): 259-264)

[91] Wu Jiyi, Shen Qianli, Zhang Jianlin, et al. Cloud computing: Cloud security to trusted cloud [J]. Journal of Computer Research and Development, 2011, 48(1): 229-233 (in Chinese)
(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(1): 229-233)

[92] Enck W, Ongtang M, McDaniel P. On lightweight mobile phone application certification [C] //Proc of CCS'2009. New York: ACM, 2009: 235-245

[93] Enck W, Gilbert P, Chun B G, et al. TaintDroid: An information flow tracking system for real-time privacy monitoring on smartphones [J]. Communications of the ACM, 2014, 57(3): 99-106

[94] Roesner F, Kohno T, Moshchuk A, et al. User-driven access control: Rethinking permission granting in modern operating systems [C] //Proc of SP'2012. Piscataway, NJ: IEEE, 2012: 224-238

[95] Lei Lingguang, Jin Jiwu, Wang Yuewu, et al. A behavior-based system resources access control scheme for Android [J]. Journal of Computer Research and Development, 2014, 51(5): 1028-1038 (in Chinese)
(雷灵光, 荆继武, 王跃武, 等. 一种基于行为的 Android 系统资源访问控制方案[J]. 计算机研究与发展, 2014, 51(5): 1028-1038)

[96] Geneiatakis D, Kounelis I, Loeschner J, et al. Security and privacy in mobile cloud under a citizen's perspective [G] //Cyber Security and Privacy. Berlin: Springer, 2013: 16-27

[97] Pelechrinis K, Iliofotou M, Krishnamurthy S V. Denial of service attacks in wireless networks: The case of jammers [J]. Communications Surveys & Tutorials, 2011, 13(2): 245-257

[98] Liu Xiangyu, Wang Bin, Yang Xiaochun. Survey on privacy preserving techniques for publishing social network data [J]. Journal of Software, 2014, 25(3): 576-590 (in Chinese)
(刘向宇, 王斌, 杨晓春. 社会网络数据发布隐私保护技术综述[J]. 软件学报, 2014, 25(3): 576-590)

[99] Dantu R, Cangussu J W, Patwardhan S. Fast worm containment using feedback control [J]. IEEE Trans on Dependable and Secure Computing, 2007, 4(2): 119-136

[100] Barbera M V, Kosta S, Stefa J, et al. CloudShield: Efficient anti-malware smartphone patching with a P2P network on the cloud [C] //Proc of P2P'2012. Piscataway, NJ: IEEE, 2012: 50-56

[101] Marforio C, Ritzdorf H, Francillon A, et al. Analysis of the communication between colluding applications on modern smartphones [C] //Proc of ACSAC'2012. New York: ACM, 2012: 51-60

[102] Lalande J F, Wendzel S. Hiding privacy leaks in Android applications using low-attention raising covert channels [C] //Proc of ARES'2013. Piscataway, NJ: IEEE, 2013: 701-710

[103] Ristenpart T, Tromer E, Shacham H, et al. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds [C] //Proc of CCS'2009. New York: ACM, 2009: 199-212

[104] Li P, Gao D, Reiter M K. Mitigating access-driven timing channels in clouds using StopWatch [C] //Proc of DSN'2013. Piscataway, NJ: IEEE, 2013: 1-12

[105] De Cristofaro E, Soriente C. Extended capabilities for a privacy-enhanced participatory sensing infrastructure (PEPSI) [J]. IEEE Trans on Information Forensics and Security, 2013, 8(12): 2021-2033

[106] Wang S, Wang X S. In-device spatial cloaking for mobile user privacy assisted by the cloud [C] //Proc of MDM'2010. Piscataway, NJ: IEEE, 2010: 381-386

[107] Ardagna C A, Conti M, Leone M, et al. Preserving smartphone users' anonymity in cloudy days [C] //Proc of ICCCN'2013. Piscataway, NJ: IEEE, 2013: 1-5

[108] Jana S, Narayanan A, Shmatikov V. A scanner darkly: Protecting user privacy from perceptual applications [C] //Proc of SP'2013. Piscataway, NJ: IEEE, 2013: 349-363

[109] Jana S, Molnar D, Moshchuk A, et al. Enabling fine-grained permissions for augmented reality applications with recognizers [C] //Proc of USENIX'2013. Berkeley, CA: USENIX Association, 2013: 415-430

[110] Han Jin, Yan Qiang, Gao Debin, et al. Comparing mobile privacy protection through cross-platform applications [C] //Proc of NDSS'2013. Reston: Internet Society, 2013

[111] Garfinkel T, Rosenblum M. When virtual is harder than real: Security challenges in virtual machine based computing environments [C] //Proc of HotOS'2005. Berkeley, CA: USENIX Association, 2005

[112] Gember A, Dragga C, Akella A. ECOS: Practical mobile application offloading for enterprises [C] //Proc of the 2nd USENIX Workshop on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services. Berkeley, CA: USENIX Association, 2012

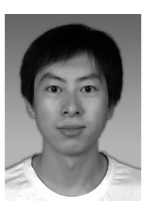
[113] Liang H, Huang D, Cai L X, et al. Resource allocation for security services in mobile cloud computing [C] //Proc of INFOCOM WKSHPS'2011. Piscataway, NJ: IEEE, 2011: 191-195

[114] Zhang Shibin, Xu Chunxiang. Study on the trust evaluation approach based on cloud model [J]. Chinese Journal of Computers, 2013, 36(2): 422-431 (in Chinese)
(张仕斌, 许春香. 基于云模型的信任评估方法研究[J]. 计算机学报, 2013, 36(2): 422-431)

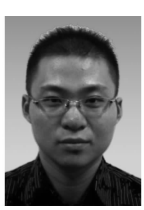
Li Pengwei, born in 1987. PhD candidate. Received his BSc degree from Sourthwest Jiaotong University. Member of China Computer Federation. His research interests include mobile cloud computing security and Android security.

Fu Jianming, born in 1969. Received his BSc and MSc degrees from Huazhong University of Science and Technology in 1991 and 1994 respectively, and received his PhD from Wuhan University in 2000, Hubei, China. Professor in Wuhan University. Senior member of China Computer Federation. His main research interests include software security and network security.

Li Shuanbao, born in 1972. PhD candidate. Received his BSc and MSc degrees from Information Engineering University of PLA in 1995 and 2002 respectively. Member of China Computer Federation. His main research interests include big data, cloud computing and information security.



Lü Shaoqing, born in 1987. PhD candidate. Received his BSc degree from Tianjin Polytechnic University. Member of China Computer Federation. His research interests include network security and social network security.



Sha Letian, born in 1985. Received his PhD degree from Wuhan University. Lecturer in Nangjing University of Posts and Telecommunications. Member of China Computer Federation. His main research interests include software security, reverse engineering, WSN security and sensitive information processing.