基于用户行为记录的云服务隐私保护体系和算法

季正波[1] 白光伟[1,2] 沈 航[2] 曹 磊[1] 朱 荣[1]

(南京工业大学电子与信息工程学院 南京 210009)[1]

(南京理工大学高维信息智能感知与系统教育部重点实验室 南京 210094)[2]

摘 要 针对移动云服务中用户的行为记录影响隐私安全的问题,提出一种基于第三方接入控制的环身份框架。在用户身份注册部分,身份接入控制端为用户提供环身份证书,来确保云服务不能跟踪用户的虚拟身份;在用户数据检测部分,数据接入控制端对数据进行调度和行为记录整合,来防止关键数据存储位置泄露,并且为用户群生成环数字签名,使用户的隐私身份对云服务工作人员保密。对所提出的机制进行了安全性验证与评价,理论分析结果表明,提出的方案能够很好地解决用户行为记录对关键数据位置以及用户身份隐私的泄露问题。

关键词 移动云计算,隐私,身份认证,环签名,接入控制,用户行为

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.8.039

Privacy-preserving Framework for Cloud Services Based on User Behavior

JI Zheng-bo[1] BAI Guang-wei[1,2] SHEN Hang[2] CAO Lei[1] ZHU Rong[1]

(School of Electronic and Information Engineering, Nanjing University of Technology, Nanjing 210009, China)[1]

(Key Laboratory of Intelligent Perception and System for High-dimensional Information of Ministry of Education, Nanjing University of Science and Technology, Nanjing 210094, China)[2]

Abstract In response to the issue that user behaviors threaten security and privacy in mobile cloud computing, a ring-identity mechanism based on the third party was proposed in this paper. The access control of user's identity ensures that it can not be able to track user's virtual identity by providing user with ring identity certificate. The focus of data auditing is on how to schedule data records and generate ring signature so as to avoid leaking position of critical data and to protect user's privacy. Theoretical analysis shows that our framework achieves good security and privacy performance considering the threat of user's behavior records.

Keywords Mobile cloud computing, Privacy, Identity authentication, Ring signatures, Access control, User behavior

移动云计算是继分布式计算、网格计算、对等计算之后的一种新型计算模式,它以资源租用、应用托管、服务外包为核心,迅速成为计算机技术发展的热点[1]。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主要障碍[2]。近年来,随着移动终端的飞速发展,移动云服务越来越受人们的关注。在移动云服务越来越热门的同时,用户的隐私安全需要成了云服务研究人员首先需要解决的问题之一,亟需一个既能保证云端数据安全又能保护用户隐私身份的移动云服务框架。

大多数的移动云服务安全框架主要针对数据加密传输、安全的环境搭建以及用户身份的保密处理等。通过研究,我们发现用户使用移动云服务后留下的行为记录也会对用户的隐私安全产生很大的威胁。例如,面对云端的海量数据,攻击者往往会找不到有价值的窃取目标,但是那些访问频繁或是修改次数多的数据就给了攻击者明确的攻击目标,这些获得用户青睐的数据也通常会是十分重要的数据。如图1所示,云端数据的差异本来是不显著的,但由于用户对关键数据的频繁访问处理,这些关键数据就会因为用户的行为记录而变得特别醒目,从而成为攻击者的目标。同样受到行为记录影响的还有用户的身份隐私,虽然用户A与B为用户的虚拟身份,但是移动云服务端依然可以跟踪这些虚拟身份,把其存储的信息与用户的虚拟身份绑定在一起。更为危险的是:图中用户A在不同时间段留下了与真实身份相关的3个信息,云端会发现这些信息都是A存储的,就可以把这些信息综合起来推测出用户A的真实身份。移动云服务本身对用户隐私

到稿日期:2014-08-19 返修日期:2014-10-13 本文受国家自然科学基金项目(60673185,61073197),江苏省自然科学基金项目(BK2010548),江苏省科技支撑计划(工业)项目(BE2011186),江苏省普通高校研究生科研创新计划项目(CXLX11_0262,CXZZ12_0425),江苏省六大高峰人才基金资助项目(第八批)资助。

季正波(1990—),男,硕士生,主要研究方向为移动云安全,E-mail:jzb_njut@163.com;白光伟(1961—),男,博士,教授,博士生导师,CCF高级会员,主要研究方向为移动互联网、无线传感器网络、网络体系结构和协议、网络系统性能分析和评价、多媒体网络服务质量等;沈 航(1984—),男,博士生,CCF学生会员,主要研究方向为无线网络编码、移动互联网、无线多媒体通信协议等;曹 磊(1980—),男,博士生,CCF会员,主要研究方向为无线网络编码、移动互联网、无线传感器网络;朱 荣(1989—),男,硕士生,主要研究方向为移动互联网室内定位。

身份的威胁是不容忽视的，因为若一个云服务的普通工作人员能够查看用户的行为记录信息，从而轻易地绑定用户的虚拟身份，这会严重威胁到用户的隐私安全。

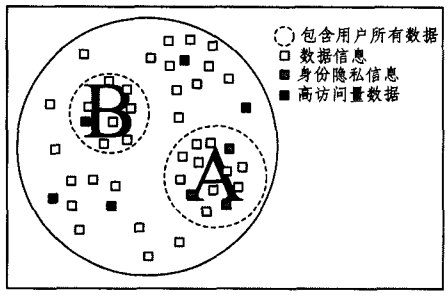

图1　云服务数据存储分布

综上所述，用户使用云服务的行为记录既会暴露关键数据的位置，也影响到用户的隐私安全。为了给用户提供不受行为记录影响的隐私安全保护，本文针对行为记录造成的用户虚拟身份被锁定问题和关键数据位置暴露问题，提出了环身份接入控制框架和数据接入控制框架。

本文第1节研究分析目前安全框架的不足并提出改进的思路；第2节引入网络模型；在此基础上第3节介绍隐私保护框架和算法；第4节为本文框架的安全性分析与评价；最后总结全文。

1　相关工作

为了解决云服务中的隐私安全问题，本文从框架和算法两个方面提出了改进。这里提到的云服务记录对用户的影响，Dou 和 Zhang 对其也有研究，他们发现了云服务记录对判断各个云服务的服务质量和安全系数有很大帮助[3]。本文主要对行为记录给用户隐私安全带来的危害提出解决办法。

在框架结构方面，Dimitris Zissis[4] 在云计算安全的文章中提出了可信赖的第三方接入控制框架，其可以给用户和云端提供方便快捷的对话，通过第三方让用户和云端变成确定的可信任交互对象。但是在这个框架中，当云服务获得较多的用户行为记录时，云端就可以跳过第三方来窥视用户的隐私。而本文的接入控制服务在提供用户与云服务可信赖对话的同时，把多个用户划分到用户组里面，以解决行为记录对于用户隐私身份的破坏问题。

在算法设计方面，Oruta[5] 利用环签名方法来掩盖用户数字签名的不同，使数据完整性检测员不能通过用户的数字签名发现用户隐私身份，但却不能防止云端对用户隐私的窥视。与之相比较，本文在身份接入控制框架中就提供给用户环身份证书，用户凭借统一的用户群身份使用移动云服务，云服务也就不再能够跟踪用户的隐私身份。

本文结合传统的由第三方提供身份证书的服务框架，提出了环身份接入控制框架，来确保云服务不能够跟踪用户隐私身份。在身份接入控制端把用户群组成一个环，环中每个用户利用自己的私钥和环成员的公钥完成身份证书认证。这样，即使用户在使用云服务时不小心留下了与隐私相关的部分信息，攻击者也无法确定这些信息是不是属于同一个用户，也就不能通过综合这些信息来发现用户的真实身份。而且，本文中的环身份证书认证方法结合了零知识验证算法，使得增加或是减少环成员都显得很方便，只需要在客户端更新其他环成员的公钥组。在用户拥有环身份证书的前提下，结合数据接入控制框架的环数字签名算法，使得云服务工作人员也不能根据用户的数字签名推测出用户隐私身份。总的来说，本文结合身份接入控制框架和数据接入控制框架以及环签名算法来处理用户行为记录对隐私安全的影响。

2　网络模型

2.1　框架结构

在本文的框架中主要有5个模块（见图2）：用户群、身份接入控制、云、数据接入控制、云服务工作人员。其中身份接入控制框架模块为：用户群、云服务端和身份接入控制。数据接入控制框架模块为：用户群、云服务端、数据接入控制和云服务工作员。

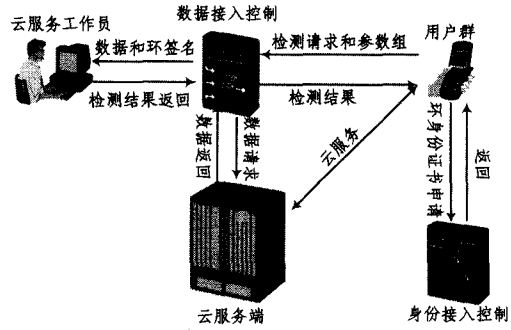

图2　移动云服务的总体结构关系

用户登录使用移动云服务所需要的虚拟身份证书由身份接入控制端生成。在这里，身份接入控制端把 λ 个用户划分为一个用户群体，然后执行本文的环身份证书生成算法，来给用户群提供统一的身份证书。在用户利用环身份证书注册云服务虚拟身份时，结合本文网络模型中的零知识验证算法，使用户不需要传递私钥就能完成验证过程。之后，用户凭借环身份证书使用移动云服务。由于云端的软硬件故障或者工作人员的操作不当，存储在云端的数据或许会遭到破坏，于是用户每次调用数据前都需要检测数据的完整性，这样检测数据的工作人员就能通过用户的数字签名变化推测出用户的行为记录，继而窥视到用户隐私。为了防止上述现象，加入数据接入控制端，数据接入控制在环数字签名协议下可以给用户群提供统一的可验证的数字签名，使用户的检测数据行为不再有差异，也就不会泄露用户隐私。同时，数据接入控制还负责根据用户的行为记录调度数据存储位置，均匀分布关键数据位置。在云服务数据记录被访问时，反馈整合后的数据记录，防止攻击者通过用户行为记录判断出关键数据位置以及用户身份。

2.2　网络模型

1）零知识验证算法。本文中在用户获取环身份证书过程中需要零知识验证。具体是指：A 向 B 证明拥有对应的私钥，却不需要把私钥展示给 B 看的验证方法。下面举一个示例，存在一个公开的密钥验证方法 $\boldsymbol{C}=\boldsymbol{D}_n * \boldsymbol{X}$（其中 $\boldsymbol{C},\boldsymbol{D},\boldsymbol{X}$ 为矩阵），验证者 B 已知 $\boldsymbol{C}$ 与 $\boldsymbol{D}_n$。用户 A 为了向 B 说明有私钥 $\boldsymbol{X}$，只需要向 B 证明能使 $\boldsymbol{C}=\boldsymbol{D}_n * \boldsymbol{X}$ 等式成立，而不需要把 $\boldsymbol{X}$ 的具体值发送给 B。

2)环身份证书生成算法。本文中身份接入控制端给用户提供的身份证书是面向一个用户群体的。这里,密钥证书形式借用 Camenisch 和 Lysyanskaya[6]两人提出的签名框架,定义一个公钥组(A_i,b,c,n),n 是 l_n 的 RSA 模数,$(A_i,b,c)\in QR_n$,$(sk_1',\cdots,sk_\lambda')$是用户群公钥组,$\lambda$ 为一个用户群的总人数;U_j 为任意环成员 j 的公钥环,来源于其他环成员的公钥组合。首先计算出用户 j 的公钥环:

$$sk_i'=H_1(sk_i)(i\in[1,\lambda],i\neq j) \tag{1}$$

$$U_j=\prod_{i=1}^{\lambda}A_i^{k_i'}(i\neq j) \tag{2}$$

然后计算出环证书 Q 的值(m 和 e 是随机数值):

$$Q_j^e\equiv A_j^{sk_j}\cdot U_j\cdot b^m\cdot c \bmod n \tag{3}$$

这个框架有两个部分:数字签名和签名认证。这里使用上面提到的零知识验证方法,用户不需要传输私钥 sk_j,只需要使下列等式成立,就能验证用户拥有合法的环身份证书。

$$SPK\{(e,sk_j,U_j,m):Q_j^e\equiv A_j^{sk_j}\cdot U_j\cdot b^m\cdot c \bmod n\} \tag{4}$$

3)环数字签名算法。用户的数字签名方案由客户端和数据接入控制端的交互来完成。表 1 列出了环签名基本参数。

表 1 环签名参数

G_i	3 个乘法循环组:$G_1,G_2,G_T(g_i\in G_i)$
e	$G_1\times G_2\rightarrow G_T;e(g_1^a,g_2^b)=e(g_1,g_2)^{a*b}$
Φ	双线性映射,$\Phi:G_2\rightarrow G_1$
w_i	用户数字签名公钥($i\in[1,\lambda]$),$w_i=g_2^{ski}$
t	环签名生成时间参数
S	完整环签名
s_i	各个数据块的部分签名,$si=g_1^{ai}$
a_i	随机参数($a_i\in Z_p$)
m′	待签名数据
J	签名用户公钥

先计算签名用户公钥 J,再生成用户环签名主要部分 s_j:

$$J=H_2(sk_j\parallel t) \tag{5}$$

$$a=g_1^{m'}\cdot H'(Q\parallel e\parallel m)(a\in G_1) \tag{6}$$

$$s_j=(a/\phi(\prod_{i\neq j}w_i^{a_i}))^{1/J}\in G_1 \tag{7}$$

通过上面的计算生成了环数字签名:

$$S=(s_1,\cdots,s_\lambda)\in G_1^\lambda \tag{8}$$

由数据接入控制端把环签名 S 发送给用户群的每个用户。用户使用环签名进行数据检测服务时,云服务工作员就不再能根据其数字签名的不同区分各个数据块差异。

3 隐私保护框架和算法

为了解决用户行为记录对隐私安全的影响,本文框架加入了身份接入控制和数据接入控制来解决用户身份隐私和关键数据位置泄露问题。用户利用从身份接入控制端获得的环身份证书去云服务端注册虚拟账户,数据接入控制端整合数据的行为记录发送给云服务工作人员,并且提供给用户环数字签名来完成数据完整性检测。

3.1 环身份接入控制

用户在长期使用移动云服务过程中,有时会不可避免地留下自己的隐私信息,如:家庭住址、手机号码,甚至真实的身份信息等。除去上面这些因素,对攻击者来说,还可以通过用户上传或修改数据的频率来判断出某个项目的主要负责人,也可以通过数据被修改的频率猜测出关键数据的位置所在。上面暴露出的这些隐私安全问题,主要原因在于用户的身份证书在长期的验证登录之后容易被攻击者绑定,攻击者可以把不同的用户区分出来,再通过用户的行为习惯判断想要窃取的信息。

为了解决上述隐私安全问题,本文在身份接入控制端为用户群提供环身份证书。把有限数量的用户划分在一个群里面,用户在身份接入控制端注册的身份证书只能表明其属于这个合法的群体,攻击者不能把身份证书与集群中的用户一一对应起来。下面是用户在身份接入控制端注册的详细过程:

1)客户端把注册请求、手机信息发送给身份接入控制端;

2)身份接入控制端对比此手机信息,如果注册次数超过次数上限 r,则返回用户失败;

3)身份接入控制端返回用户核实,验证此手机信息是否有效,如果验证失败,则返回用户失败;

4)验证成功后,客户端利用式(1)生成此用户的公钥 sk_i',并发送给身份接入控制端;

5)身份接入控制端按用户需求发送其他环成员的公钥信息组$\{sk_1',\cdots,sk_{j-1}'\}$和$\{sk_{j+1}',\cdots,sk_\lambda'\}$到客户端,客户端存储此公钥组;

6)客户端利用式(2)、式(3)生成环身份证书;

7)客户端存储随机参数对(e,m)并把与用户对应的 Q 值发送给身份接入控制端。

之后用户在移动云服务注册虚拟账户时,只需要利用零知识验证算法执行式(4)就能完成云服务账户注册。利用环身份证书作为可信的合法用户凭证可以有效地解决用户被攻击者跟踪的问题,甚至云服务端也不能区分某个特定的用户。对于移动云服务来说,用户不论在上传、修改或是进行完整性验证的时候,都只是环成员中不确定的一个,云服务不能根据用户的长期行为记录去区分出其中的关键人物。特别地,对于一个工作团队来说,由于频繁的数据修改,用户会使用自己的数字签名来验证数据的完整性,这样用户的虚拟身份和数字签名会很容易地被绑定在一起。而在本文提出的环身份认证算法中,一个用户的身份证书会对应多种不同的数字签名方案,数据完整性检测人员也就不能够通过数字签名的差异来跟踪并发现用户的真实身份。但是,用户数字签名的行为记录依然会暴露关键数据位置所在,这个问题在3.3节环签名算法中得到了很好的解决。

3.2 数据记录整合及调度

对于攻击者来说,大多数时候只想窃取存储在移动云服务端的关键数据。事实上,存储在云端的数据量十分庞大,攻击者也很难找到对其有价值的数据信息。通常认为被用户修改频繁或者是受检测次数多的数据会比较重要,这些数据就会成为攻击者的攻击目标。另一种情况下,用户存储在移动云服务端的数据文件通常被分成很多小的数据块,这样一方面便于分布式存储,另一方面也减少了整个数据文件被窃取的几率。但是,用户长期留下的行为记录却会增加文件被完全窃取的可能性。例如,一个具体的图像文件 P 被分割成$\{p_1\cdots p_n\}$这样小的数据块,然后存储在云端,这些数据块往往有相同的行为记录,如:下载次数、修改次数、完整性检测次数

等，这些行为记录都会很明确地告诉攻击者它们属于同一个图像文件。

为了解决上面提到的用户行为记录次数暴露数据位置的问题，在云服务数据接入控制端加入了行为记录整合以及数据调度功能。在数据接入控制框架中，云服务数据检测人员并不能直接获取各个数据块的行为记录。数据接入控制端负责把一个存储阵列中的存储内容记录总地呈现给云服务工作人员，这样既保护了用户数据信息的安全，也不妨碍工作人员管理云服务；并且，数据接入控制端会周期性地把访问频次较高的数据块与相邻阵列中的低访问量数据交换物理存储位置，达到一个存储阵列中数据访问均衡的目的，这样既使数据安全隐私得到保障，也使云服务的资源能够得到更合理的分配，不会出现部分存储阵列访问过高而有些存储阵列基本闲置的状况。

3.3 针对数据检验的环签名算法

由于云服务可能因为软硬件出错、管理员操作不当等引起存储数据错误，用户通常在使用云端数据时都需要进行数据的完整性检测。云服务的数据量十分庞大，逐一检测数据完整性是不切实际的，这里针对其通常使用的数字签名算法中的安全隐患提出新的框架结构和算法。

在处理多人参与的共享数据时，若使用通常的云服务身份注册方案，移动云服务的工作人员可以通过其数据检测记录推测出数据库的主要数据部分所在，同时能够锁定项目组的主要负责人。下面通过一个实际的案例予以说明，如图 3 所示。

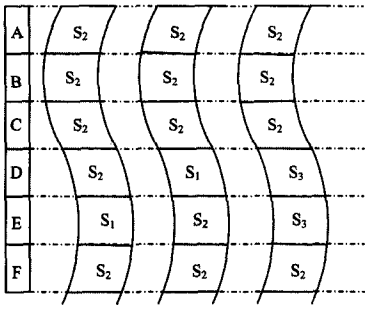

图 3 用户 S_1，S_2，S_3 在 A 到 F 数据块上的数字签名状况

在图 3 显示的数字签名记录下，当用户使用各自不同的数字签名时，能够很容易地看到大部分的数据修改和检验工作都是由 S_2 来完成的，看到签名记录的攻击者就可以推测出 S_2 是这个工作最主要的负责人。同时也可以发现，D 和 E 这两个数据块是工作组中所有人员共同参与的部分，这样也暴露了 D 和 E 的重要性。在身份接入控制部分提到的环身份证书算法下，虽然云服务数据检测员不能够根据数字签名变化来锁定用户在用户群中的具体身份，但是却依然可以发现 D 和 E 为关键数据块。为了保护关键数据位置隐私，这里又在数据接入控制框架中引入了环签名算法。环签名方法使得同一个工作组的成员使用相同的数字签名（即环签名），这样云服务工作人员就只能检测数据完整性却不能分辨这些签名的不同，从而确保了关键数据位置的隐私安全。下面是数据接入控制框架下环签名算法的具体实现：

1）客户端利用式(5)生成用户公钥 J，然后发送云服务数据地址和参数组(e,m)以及公钥 J 到数据接入控制端；

2）数据接入控制端访问云服务，取出待检测数据 m'和用户环签名参数 Q，之后使用式(6)－式(8)计算出此用户环签名 S；

3）数据接入控制把签名 S 和数据 m'以及参数组$(a,g_1,g_2,a_i,w_i)(i\in[1,\lambda])$发送给云服务工作员；

4）工作员验证签名的合法性，若合法，则继续检测数据的完整性；

5）检测结果由数据接入控制端返回给用户。

在本文的数据接入控制框架和环签名算法下，一个工作组的用户每次修改文件后都使用同样的环签名，这样云服务检测人员就看不到签名的变化，也就不能够获取用户隐私及关键数据位置。

4 安全性分析与评价

针对移动云服务中用户行为记录对隐私安全的影响，本文提出了身份接入控制框架和环身份证书算法来确保云服务不能锁定用户隐私身份；在此基础上，在云服务端加入数据接入控制，并结合环签名算法，来确保云服务工作员既不能窥视用户隐私，也不能够获得关键数据存储位置信息。下面先分析本文框架结构的安全性，再通过环签名算法验证过程来说明其在用户隐私保护中的作用。

4.1 结构安全性分析

对本文框架的评价从两部分来阐述，即身份接入控制框架和数据接入控制框架。

1）身份接入控制框架不会威胁用户以及云服务隐私。本文的身份接入控制框架给用户提供的身份证书为环身份证书，使用户能够很好地对移动云服务保密自己的隐私身份。但是完全可信赖的第三方（即身份接入控制）是不存在的，为了防止在用户使用云服务时，身份接入控制端跟踪用户并获取用户使用云服务的情况以及云服务本身的业务状况信息，本文框架使身份接入控制不与云服务直接联系。而且在本文框架下，身份接入控制端一般处于对用户关闭状态，用户的环身份证书只需要认证一次就能让用户与云服务正常交互信息。只有在环成员有变动的情况下，身份接入控制端才需要获取新用户的公钥，再发送给用户群的各个客户端，来重新生成环身份证书。所以，这不仅保护了用户对移动云服务的隐私安全，也限制了身份接入控制端参与云服务过程，从而防止了其窃取用户隐私和云服务的商业机密。

2）数据接入控制框架在保护用户隐私的同时也节省了客户端功耗，并维护了云服务的利益。在数据接入控制部分，本文把生成环数字签名的主要过程从客户端移到了数据接入控制端，通过式(5)对用户的私钥进行处理，使得数据接入控制端可以取代客户端的签名过程，却不会泄露用户的私钥。与 oruta[4] 方案相比，本文方案节省了客户端计算参数以及生成签名的功耗。在本文框架下，用户不能够把待检测的数据直接发送给云服务工作员，而是由数据接入控制端先从云服务下载数据后再发送给检测员，这样就可以确保所有被检测的数据只能来自于云服务端本身。所以数据接入控制框架既防止了云服务工作员窃取用户隐私，也保护了云服务本身的利益。

4.2 算法安全性分析

1)云服务工作员能够验证签名来自特定用户群,并且验证数据的完整性。

从本文环签名的生成过程得知,要证明这个论点,即是证明:在已知全部用户签名公钥 w_i、被签名数据 m' 和环签名 S 的情况下,①α 的值是否正确;②$e(\alpha,g_2)$ 和 $\prod_{i=1}^{\lambda}e(s_i,w_i)$ 是否相等。若①②都成立,则能证明环签名属于此用户群,并且数据完整。证明过程如下:

$$①\alpha=g_1^{m'}\cdot H(Q\|t)(\alpha\in G_1)$$

$$②\prod_{i=1}^{\lambda}e(s_i,w_i)$$

$$=[\prod_{i\neq j}e(s_i,w_i)]\cdot e(s_j,w_j)$$

$$=[\prod_{i\neq j}e(g_1^{a_i},g_2^{*_i})]\cdot e((\alpha/\phi(\prod_{i\neq j}w_i^{a_i}))^{1/J},g_2^{J})$$

$$=[\prod_{i\neq j}e(g_1^{a_i\cdot *_i},g_2)]\cdot e(\alpha/\phi(\prod_{i\neq j}g_2^{*_i\cdot a_i}),g_2)$$

$$=e(\prod_{i\neq j}g_1^{*_i\cdot a_i}\cdot(\alpha/\prod_{i\neq j}g_1^{*_i\cdot a_i}),g_2)=e(\alpha,g_2)$$

2)云服务工作员不能确定签名来自用户群的哪个用户,其正确猜测出签名用户的概率不会超过 $1/\lambda$(λ 为一个用户群的总人数)。

对于任意的 $\alpha\in G_1$,$1\leqslant j\leqslant\lambda$,签名用户的环签名分布形式为:

$$M\leftarrow\{g_1^{a_1},\cdots,g_1^{a_\lambda}:a_i\xleftarrow{R}Z_p,a_j\leftarrow\prod_{i=1}^{\lambda}g_1^{a_i}=\alpha\}(i\neq j)$$

而在移动云服务工作员看来,任意一个用户的签名表示为:

$$N\leftarrow\{g_1^{a_1},\cdots,g_1^{a_\lambda}:\prod_{i=1}^{\lambda}g_1^{a_i}=\alpha\}$$

可以清楚地看到 M 和 N 是等价的。所以对于任意的环签名 $S=(s_1,\cdots,s_\lambda)$,攻击者都不能够确定具体用户,其正确推测出签名者的概率只能是 $1/\lambda$。

结束语 针对用户行为记录会泄露关键数据位置并且暴露用户身份隐私的问题,提出了身份接入控制与数据接入控制相结合的框架结构。身份接入控制框架给用户群提供环身份证书,使得用户间的身份证书差异不能被云服务端察觉,云服务也就不能根据用户的行为特征跟踪用户的虚拟身份。同时,为了防止云服务工作员根据用户数字签名的不同识别用户隐私身份并发现关键数据位置的情况,利用数据接入控制框架帮助用户生成环数字签名。数据接入控制端也负责整合数据记录并调度数据块位置,来保护用户数据位置的安全。综上,为了防止用户使用移动云服务后留下的行为记录被识别,导致攻击者能够跟踪用户虚拟身份并发现关键数据位置,本文提出新的框架结构和算法来保护移动云用户的隐私安全。

参 考 文 献

[1] 林闯,苏文博,孟坤,等. 云计算安全:架构,机制与模型评价[J]. 计算机学报,2013,36(9):1765-1784
Ling Chuang, Su Wen-bo, Meng Kun, et al. Cloud Computing Security: Architecture, Mechanism and Modeling [J]. Journal of Computers, 2013, 36(9): 1765-1784

[2] 李瑞轩,董新华,辜希武,等. 移动云服务的数据安全与隐私保护综述[J]. 通信学报,2013,34(12):158-166
Li Rui-xuan, Dong Xin-hua, Gu Xi-wu, et al. Overview of the data security and privacy-preserving of mobile cloud services [J]. Journal of communications, 2013, 34(12): 158-166

[3] Dou W, Zhang X, Liu J, et al. HireSome-II: Towards privacy-aware cross-cloud service composition for big data applications [J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 26(2): 455-466

[4] Wang B, Li B, Li H. Oruta: Privacy-preserving public auditing for shared data in the cloud[C]// Proc. of IEEE 5th International Conference on Cloud Computing(CLOUD). 2012: 295-302

[5] Zissis D, Lekkas D. Addressing cloud computing security issues [J]. Future Generation Computer Systems, 2012, 28(3): 583-592

[6] Camenisch J, Lysyanskaya A. A signature scheme with efficient protocols [M]// Security in communication networks. Springer Berlin Heidelberg, 2003: 268-289

[7] Wang C, Chow S S M, Wang Q, et al. Privacy-preserving public auditing for secure cloud storage [J]. IEEE Transactions on Computers, 2013, 62(2): 362-375

[8] Wang C, Cao N, Ren K, et al. Enabling secure and efficient ranked keyword search over outsourced cloud data [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(8): 1467-1479

[9] Sundareswaran S, Squicciarini A, Lin D. Ensuring distributed accountability for data sharing in the cloud [J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(4): 556-568

[10] Liu X, Zhang Y, Wang B, et al. Mona: secure multi-owner data sharing for dynamic groups in the cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191

[11] Bohli J, Gruschka N, JensenM, et al. Security and Privacy Enhancing Multi-Cloud Architectures[J]. IEEE Transactions on Dependable and Secure Computing, 2013, 10(4): 212-224

[12] Zhu Y, Xu R, Takagi T. Secure k-NN computation on encrypted cloud data without sharing key with query users [C]// Proceedings of 2013 International Workshop on Security in Cloud Computing. ACM, 2013: 55-60

[13] Ren K, Wang C, Wang Q. Toward secure and effective data utilization in public cloud [J]. IEEE Networks, 2012, 26(6): 69-74

[14] Wang C, Wang Q, Ren K, et al. Toward secure and dependable storage services in cloud computing [J]. IEEE Transactions on Services Computing, 2012, 5(2): 220-232

[15] Wang H, Wu S, Chen M, et al. Security protection between users and the mobile media cloud [J]. IEEE Communications Magazine, 2014, 52(3): 73-79

[16] Liu C, Zhang X, Yang C, et al. CCBKE—Session key negotiation for fast and secure scheduling of scientific applications in cloud computing[J]. Future Generation Computer Systems, 2013, 29(5): 1300-1308