Journal of Computer Applications
计算机应用,2014,34(7):1897 - 1901
ISSN 1001-9081
CODEN JYIIDU
2014-07-10
http://www.joca.cn

文章编号:1001-9081(2014)07-1897-05
doi:10.11772/j.issn.1001-9081.2014.07.1897

具有隐私保护功能的移动云服务接入控制

季正波[1*],白光伟[1,2],沈　航[2],张　芃[1]
(1.南京工业大学 电子与信息工程学院,南京 210009;　2.高维信息智能感知与系统教育部重点实验室(南京理工大学),南京 210094)
(*通信作者电子邮箱 jzb_njut@163.com)

摘　要:针对移动云服务中的安全和隐私保护问题,提出一种匿名使用云存储服务的机制。在匿名身份注册部分,零知识验证和数字签名技术简化了移动云用户的密钥验证步骤,同时第三方使用户与自己的身份证书绑定,防止用户对移动云服务的恶意使用;在数据共享部分,系统通过提取共享者账号参数,用于解决因共享密钥丢失导致数据安全性降低的问题。结合理论分析的方法对所提出的机制进行安全性验证与评价,结果表明身份证书和共享密钥生成算法对用户隐私安全有很好的保护作用。

关键词:移动云计算;隐私;身份认证;共享;匿名
中图分类号:TP393　　**文献标志码**:A

Privacy-preserving access control for mobile cloud services

JI Zhengbo[1*], BAI Guangwei[1,2], SHEN Hang[2], ZHANG Peng[1]
(1. *School of Electronics and Information Engineering, Nanjing University of Technology, Nanjing Jiangsu* 210009, *China*;
2. *Key Laboratory of Intelligent Perception and System for High-Dimensional Information of Ministry of Education (Nanjing University of Science and Technology), Nanjing Jiangsu* 210094, *China*)

Abstract: In response to the issue of security and privacy-preserving in mobile cloud computing, an anonymous mechanism using cloud storage was proposed. Zero-knowledge proofs and the digital signature technology were introduced into anonymous registration to simplify the steps of key authentication, building upon which the third party was used to bind users and their identity certificates that avoid legitimate cloud services for malicious purposes. The focus of data sharing is on how to take advantage of account parameters of sharers so as to solve the security issues due to secret key loss. Theoretical analysis shows that the proposed identity certificate and shared key generation schemes contribute to users' privacy.

Key words: mobile cloud computing; privacy; identity authentication; sharing; anonymity

0　引言

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]。移动云计算为移动终端解决了存储量小、计算能力不足、平台搭建困难等一系列问题,让用户可以在移动终端,如手机、IPAD 上享受大型计算机的运算存储能力。因为用户享受服务的同时,需要把数据存储在云服务器端,这就带来了很多的隐私安全保护问题。

随着移动云计算的普及,隐私安全问题变得越来越重要。用户不希望自己的数据被云服务或是其他攻击者窥视,更不希望被跟踪甚至暴露真实身份。在享受移动云服务时,用户希望自己是匿名的;但对于云服务端来说,它们期望获得一些用户的身份信息来确保服务的对象是合法的。原本应用于移动互联网中的隐私保护机制无法直接应用于移动云环境中,我们迫切地需要一个既能保护用户隐私又能确定用户身份的移动云服务框架。

为了给用户提供隐私保护,这里提出一种基于第三方手机身份认证的移动云服务框架(通常用户拥有的手机数量被认为是可控制的)。第三方即为接入控制服务器端,负责给用户签发身份证书,保证其身份的合法性。和通常提供匿名身份的第三方相比,这里把第三方设定为不完全可信状态,因此本文中用户的身份信息对第三方保密。根据用户对安全性的不同需求,对不同用户的安全性进行了区分处理,在保证整个框架安全性的同时,也保证了其灵活性。

1　相关工作

近年来,针对隐私保护问题人们对用户匿名使用互联网服务提出了相应的解决方案。目前,OpenID[2] 的单点登录验证框架,允许用户凭借同样的身份证书去使用不同的网络服务。但是用户的身份却可以被服务器追踪到,即使用户在此之下创建多个虚拟身份,这些虚拟身份也会被联系在一起,甚至 OpenID 可以知道用户创建这些账户时所在的位置。显然,这个框架中第三方参与过多,妨碍了用户的隐私权益。

收稿日期:2014-01-26;**修回日期**:2014-03-19。
基金项目:国家自然科学基金资助项目(60673185, 61073197);江苏省自然科学基金资助项目(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。
作者简介:季正波(1990 -),男,江苏南通人,硕士研究生,主要研究方向:移动云安全;　白光伟(1961 -),男,河北玉田人,教授,博士生导师,博士,CCF 高级会员,主要研究方向: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;沈航(1984 -),男,江苏南京人,博士研究生,CCF 会员,主要研究方向:无线网络编码、移动互联网、无线多媒体通信协议;　张芃(1965 -),女,江苏徐州人,副教授,CCF 会员,主要研究方向:无线网络。

Opaak[3]比较详细地讲解了互联网的隐私保护机制,对三方协议进行了一些改动,避免了第三方对用户与服务商的隐私窃取。但是 Opaak 协议主要是针对移动互联网的安全机制,在移动云环境下还是不能适用的。

通常的三方协议中,由于第三方是验证身份的关键,三方会获得大量的用户个人信息,甚至注册使用云服务的频率。第三方可以通过在其注册的用户得知各家云服务的客流量,这不仅仅泄露了用户的隐私,也会泄露移动云服务的商业机密。在本文的框架中,我们把第三方视作半可信状态,仅用它参与用户的身份证书验证和部分虚拟账户注册过程。

从用户角度来讲,隐私和安全是吸引使用者的关键;从云服务端来看,我们在确保用户的隐私安全不受威胁的同时,也希望用户能够遵守协议,规范地使用移动云服务。在文献[4]中,虽然很好地用同态加密技术保护了用户的隐私,但却对用户的身份注册和虚拟账户使用没有加以限制。本文先通过手机验证用户的真实身份,防止攻击者对第三方和移动云服务的恶意攻击,之后又对用户的私钥进行了顺序拆分,来确保身份证书与用户相绑定,这样既能减小用户身份证书被窃取的概率,还能避免用户把自己的身份证书随意外借别人。

在用户共享移动云服务端的数据时,共享者的个人隐私问题没有得到很好的解决。本文中移动云服务生成的共享密钥并不直接发给共享者,而是采用用户间相互转发的方式,这样可以让共享者无需对移动云服务暴露自己的通信地址,同时由于数据所有者需要转发解码密钥给共享者,也没有采用第三方转发共享密钥的方式。这里共享密钥参数由云服务和数据所有者共同生成,主要的计算工作是在移动云服务端进行。针对共享密钥会大大降低云服务端数据安全性的问题,在共享权限验证中用共享密钥与共享者的虚拟账号绑定的方法,来同时解决共享安全和用户的个人隐私保护问题。对于整个云服务框架,有时对安全性提出过高的要求会浪费很多的计算资源和通信资源,在本文部分环节中我们按用户需求对移动云安全进行分级处理,在保护安全性的前提下也能节省开销。

2 移动云服务接入控制框架

2.1 总体框架结构

整个的框架中主要有 3 个参与者(如图 1 所示):用户、第三方(提供匿名身份保护)和移动云服务。其中:用户在共享环节中分为数据所有者和共享者;第三方即为移动云服务的接入控制端,负责通过验证用户的手机信息来给用户一个合法匿名身份。

用户在注册使用云服务之前,首先需要在第三方获得身份证书,之后用身份证书去云服务注册虚拟账户。注册虚拟账户时除了用户自己注册,也可以选择接入控制服务器注册的方式,两种方式的具体描述在 3.2 节有详细的介绍。

2.2 网络模型与算法设计

在介绍具体的云服务接入控制框架前,先引入后面注册登录所需要的密钥验证方法。

1)零知识验证算法。本文中在用户获取身份证书和注册登录云服务环节都需要零知识验证。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。下面举一个事例,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。

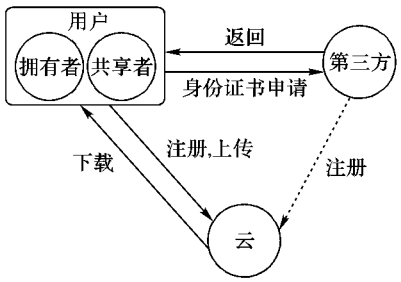

图 1 移动云服务的总体结构关系

2)数字签名认证算法。用户在第三方获得身份证书时使用数字签名技术,这里借用 Camenisch 等[5]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,$(A_i,b,c)\in QR_n$,$(sk_1,sk_2,\cdots,sk_\lambda)$ 是用户私钥的顺序截取,首先计算出 Q 的值(m 和 e 是随机数值):

$$Q^e\equiv\prod_{i=1}^{\lambda}A_i^{sk_i}\cdot b^m\cdot c \bmod n \tag{1}$$

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,用户不需要传递私钥 sk,只需要使下列等式成立,就能验证用户拥有接入控制端的身份证书。

$$SPK\left\{(e,sk_1,\cdots,sk_\lambda,m):Q^e\equiv\prod_{i=1}^{\lambda}A_i^{sk_i}\cdot b^m\cdot c \bmod n\right\} \tag{2}$$

3)云服务虚拟账户生成算法。本文中用户不可以直接凭身份证书登录移动云服务,而是利用一个身份证书对应多个虚拟账户的方式来使用移动云服务,用户注册虚拟账户既保护了用户隐私也能让攻击者失去攻击的目标。用户从第三方获得身份证书后可以按需创建 j 个令牌来表示不同账号。每个用户的令牌参数都不相同,即使是同一用户的不同账号的参数也是不一样的,这样确保云服务端不能够把同一个用户的不同账号联系起来,只能够限制一个用户创建账户的最大数量。下面是虚拟账户令牌 T 的生成算法($H()$ 是哈希函数,a 是云服务地址,j 为同一个用户注册账户次数,n 和 α 由 l_n 和 l_α 的长度决定):

$$\rho=H(a\|j)^{(n-1)/\alpha};\ 1\leqslant j\leqslant k \tag{3}$$

$$T=\rho^{sk}\cdot e \bmod n \tag{4}$$

上面这种生成虚拟账户的方法和通常的身份匿名验证方法十分地类似,但这里为了使零知识验证算法更简便,对参数作了简化工作。我们把上述的 ρ 作为公开的参数,用户登录云服务时只需要输入私钥 sk 使得式(4)成立,而不需要转发私钥,同时公开 ρ 也简化了零知识验证的步骤。

3 移动云服务隐私保护机制

隐私保护的框架分为注册、登录以及数据存储和共享。注册主要是第三方的身份证书注册和移动云服务端的虚拟账

户注册。用户从第三方注册获得身份证书,接下来凭身份证书注册云服务虚拟账户,之后用户就可以使用移动云服务的存储和共享功能。

3.1　第三方身份证书注册

在这个过程中用户和第三方完成身份证书认证协议,第三方返回用户证书参数值(云服务端不参与其中)。首先,第三方需要确定用户是合法用户而不是一段恶意攻击程序,本文中用户把手机信息和用户的其他私人基本信息(如:身份证、住址、Email 等)一起上传给第三方。这里手机信息作为确认用户真实存在的依据,第三方通过返回短信来判断本次申请是否来自合法用户。身份证书注册框架中,把第三方作为半可信状态,用户需要在客户端把自己的其他私人信息加密之后存储在第三方。下面是身份证书注册的具体步骤:

1)用户把注册请求、手机信息和加密后的其他基本信息发送给第三方。

2)第三方比对此手机信息,如果注册次数超过次数上限 r,返回用户失败。

3)第三方返回用户核实信息,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)第三方确认了用户的合法身份。用户与第三方利用式(1)执行数字签名协议,之后用户注册云服务虚拟账户时,客户端用式(1)通过零知识验证算法来证明用户拥有合法的身份证书。

5)客户端保存随机参数对 (e,m) 和计算结果 Q 的值。

3.2　移动云服务账户注册

用户从第三方获得了合法的身份证书后可以凭借此身份证书在云服务端注册多个虚拟账户。根据用户和移动云服务对安全程度需求的高低,可以选择两种不同的注册云服务方式:

1)云注册由用户去实现。用户发送给云服务器所需信息和身份证书来完成注册。这种方式下,在用户获得了身份证书之后,第三方就处于断开状态,完全不参与接下来的任何流程。用户注册的方式适合安全级别较高的用户和云服务,与通常保护用户隐私的三方协议相比,这个流程中第三方不能获得用户与云服务的任何隐私。

2)云注册由第三方去实现。用户发给第三方云服务地址和云服务对个人身份信息的需求,由第三方去完成云服务的注册。这里由于本文把第三方作为半可信状态,为了使用户存储的私人信息对第三方不可见,本文采用 Wang 等的部分同态加密算法[4]加密用户其他私人信息,第三方可以从加密的信息里检索出云服务所需求的私人信息,而不能够知道信息的具体内容。

这种方式对用户和云服务安全性要求都不高,但是却能减轻客户端的开销,方便用户注册。从用户来看,第三方可以跟踪用户注册云服务过程,推测出用户使用云服务的情况;对云服务来讲,第三方能够从用户的注册量上得到云服务的客流量,从而窃取到移动云服务的商业机密。但是由于云服务账号注册还有用户注册的方式,于是第三方就只能得到部分数据,并不能够推测出云服务的客流量信息。

两种注册方式的流程是类似的,下面是由用户注册的步骤:

1)用户向云服务发送注册账户请求。

2)云服务返回注册次数上限 k 和地址参数 a。

3)客户端使用式(2)执行零知识验证,并把验证结果和注册次数 j 发送给云服务。

4)云服务验证零知识验证结果和 j 的值($1 \leqslant j \leqslant k$),如果验证不成立,则终止协议返回用户失败。

5)客户端使用式(3)和(4)创建假名账户 T,创建成功之后向云服务端发送 T 和昵称。

6)云服务检测数据库里是否存在同样的 T,若存在则返回失败;否则把 T 和随机数 e 加入数据库并绑定此昵称,返回用户注册账户成功。

3.3　数据上传与存储

用户在获得了云服务注册账号之后,就可以在云服务端存储自己的数据。这边第三方也不再参与其中。本文在考虑安全隐私的基础上,也按用户需求做了一些安全分级处理,可以节省客户端的开销又不影响用户的基本安全。

客户端首先用零知识验证算法,通过式(4)验证虚拟账户,验证成功之后登录云服务。用户上传的数据可以根据内容类别等进行分区处理,把数据分成 $(D_1,D_2,\cdots,D_N)$ N 个分区,然后根据用户不同情况(内容是否需要对云服务端保密)选择加密方式:

1)把数据加密之后上传到云服务端。这种方法解码密钥只在客户端中,适合安全要求较高的存储文件和可信度不高的云服务端。

2)用户直接上传数据,数据加密由移动云服务端进行。在这种方式下,用户的此数据信息对云服务端是可见的。此方法适合用户存储非重要信息时使用,主要为了减少移动客户端的计算开销。由于用户存储的数据信息实际上并不总是需求那么高的安全性,并且用户得到解码密钥的同时也可以随时查询数据的使用次数,特别是用户存储以及修改数据会变得十分方便,所以这种方法很适合用户存储安全性较低的数据。

3.4　共享密钥生成

由于用户间合作完成项目或者处理数据的需求,用户存储在移动云服务端的数据需要共享出去,而且通常上传的文件会有多个共享者存在。

在上面上传存储部分提到,用户存储自己数据时可以对数据进行分区处理。用户根据自己需要和共享考虑把数据分成 N 个分区,共享者访问用户的共享数据时,只能访问特定分区而不能下载阅读其他部分数据。共享环节的结构如图 2 所示。

下面是共享者获取共享权限的详细流程:

1)共享者向数据所有者发送共享请求和自己的地址;

2)数据所有者同意之后,把共享者需求数据的分区数 β 发送给云服务端;

3)下面是共享密钥的生成,其中 (u,v) 是随机参数对,t 为当前时间;

$$k_\beta^m = u \cdot (\beta \| m \| t)^2 + v \tag{5}$$

4)云服务端把此分区数的共享次数 m 和共享密钥 k_β^m 返回给数据所有者(若 β 区是由云服务加密的共享数据,则带上解码密钥);

5)数据所有者转发给共享者共享密钥 k_β^m 以及此共享分区的解码密钥;

6)共享者根据共享密钥 k_β^m 和虚拟账户的公钥 T,执行下列算法,形成完整的共享密钥验证:

$$G = H(k_\beta^m \| T)^{(n-1)/\alpha} \tag{6}$$

之后,云服务端存储公钥 G 和参数对 (n,α),并返回共享者 β 区可共享确认;

上面的流程之后,共享者需要访问 β 区的数据时,只需要登录云服务,输入 k_β^m,云服务端提取共享者的假名账户公钥 T,若共享密钥验证公式成立,则共享者可以访问共享数据区 β。

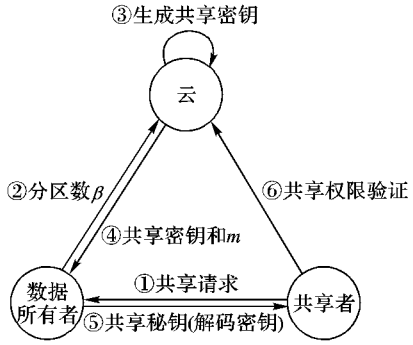

图 2 共享框架

4 安全性分析与评价

4.1 安全性分析

本文移动云计算的隐私保护机制是建立在三方协议基础上的,为了保护用户与云服务隐私,把第三方作为半可信状态,第三方只提供用户的身份证明和低安全性要求下的云服务注册功能。在密钥验证过程中,除了使用零知识验证方法外也对密钥进行了巧妙的绑定,解决了身份认证密钥和共享密钥的泄露问题。下面对本文框架的改进部分作具体的安全评估:

1)第三方无法通过追踪用户来获取移动云服务的商业隐私。本文提出的移动云计算框架在传统的第三方协议框架上作了改善。在身份证书注册过程中,本文利用部分同态加密算法使用户的基本信息对第三方保密但又不影响第三方对用户信息的直接检索。同时在本文协议下,把用户的手机作为认证用户真实身份的凭据,并对注册次数进行限制 $(1 \leqslant j \leqslant k)$,来防止用户对第三方与云服务的恶意攻击。

针对第三方对用户使用云服务的追踪,本文协议在高安全性要求下,第三方不参与用户与云服务的注册登录,也就不能够跟踪了解用户使用云服务的情况。第三方只能获得低安全性要求下的用户注册信息,也就无法准确推断出云服务的商业隐私。因此,用户的个人隐私和云服务的商业机密对第三方保密。

2)降低因密码泄露引起的身份证书丢失的概率。在保护用户隐私的同时本文也兼顾考虑到用户对移动云服务的合法使用。在注册第三方协议时使用式(2)的身份证书验证方式。从式(2)可以看出我们在客户端对用户的私钥进行了简单的拆分,把密钥 sk 按顺序拆分成 $(sk_1, sk_2, \cdots, sk_\lambda)$,同时保存其拆分规律,用户也不能确切地知道 sk_i 取自密钥 sk 的哪一段,因此即使用户被窃取了自己的身份密钥,攻击者也无法直接完成身份证书的认证过程,同时也可以有效防止用户对自己身份证书的外借,保证身份证书与用户的对应。下面是发现拆分方法的概率 p 的计算(s 为可验证次数,u 为密钥长度,$u \geqslant \lambda$):

$$s = p \cdot \sum_{i=2}^{u} C_{u-1}^{i-1} \tag{7}$$

可以看出 p 与用户的密钥长度 u 和验证次数 s 有关,密钥越长,就可以更好地将身份证书与用户绑定。若用户 s(参数 s 的值由第三方设定)次认证失败,则身份证书需要手机号来重新激活。这里我们没有对用户的私钥采用传统的哈希加密方法,直接的拆分可以节约用户注册身份证书和云服务虚拟账户的时间。

3)攻击者不能够通过窃取共享密钥 k_β^m 的方法来获取用户数据。共享者和普通用户一样首先需要从第三方获得身份证书,之后的共享过程与第三方无关。本文的数据共享过程需要确保三方面的安全性:① 共享者 X_i 只能获得数据所有者希望其获取的部分,而不能获得其他共享数据;② 数据所有者随时可以关闭共享者 X_i 对特定数据的共享权限(而不是关闭共享者 n_i 的所有共享权限);③ 只有共享者 X_i 能够使用共享密钥 k_i 获取共享数据。

首先用户对自己的共享区数据进行区域的划分,根据共享情况把共享区分成多个区域,每个区域设置不同的共享密钥。在共享数据部分由共享区的分区数 β 和共享次数 m 以及当前时间 t 生成共享密钥 k_β^m。β 可以限制共享的者浏览共享区的范围,m 可以确定共享者的身份(共享次数 m 与共享者身份对应),这样本文协议中用参数组 (β, m, t) 就可以确保共享者仅获取指定共享内容,同时数据所有者可以随时取消其浏览此共享内容的权限。

每个共享密钥虽然对应每个共享分区,但是只凭共享密钥是不能够获得此共享区数据的。共享密钥只是共享权限验证参数的一部分。在用户想获得共享权限时,云服务端会把用户虚拟账户的参数 T 和共享密钥一起验证。共享者在云服务端结合式(6)作共享权限验证,从式(6)可以看出验证中不仅仅使用共享密钥作为参数。用户于每次访问共享数据时,云服务端会把共享者的虚拟身份公钥 T 作为参数的一部分,所以即使共享者的共享密钥被窃取,用户也不用担心数据的泄露,攻击者仅获得共享密钥而没有对应的虚拟账号是不能够完成共享权限验证的。这种共享密钥绑定虚拟账号的方法增强了数据共享的安全性。

4.2 安全性对比

本文的研究重点是对接入控制端的权限限制。针对文献[4]的部分同态加密算法下,用户可以恶意进行第三方认证以及攻击云服务的问题,这里增加了对用户的身份判定。我们把客户端存储在接入控制端的个人信息分成可见和保密两

部分,第三方可以通过用户的手机信息确认用户的合法性,同时却不能够获取用户转发给移动云服务的私人信息。第三方协议与 Opaak 协议[3]相比较,虽然都把接入控制端作为半可信状态,但本文除了使第三方不参与用户登录使用云服务过程,在用户注册以及共享资源环节,也不让用户信息暴露给接入控制端。

在用户的个人证书验证方面,考虑到用户丢失证书的安全风险。在 Opaak 身份证书协议的基础上增加了身份证书绑定用户手机的功能。这里对身份密钥的顺序拆分既降低了用户身份证书被盗用的概率,又避免了因为使用复杂的加密方法增加客户端计算量的问题(具体如式(7)所示)。

5　结语

本文提出了一种移动云环境下的安全隐私保护机制,可以在保护用户隐私的前提下,保证用户合法地使用移动云存储与共享服务。协议中用半可信的第三方给用户提供身份证明,用户凭借身份证书在移动云服务端进行虚拟账户的注册。在三方协议中,用户只透露私人信息中的手机信息给接入控制端,第三方通过手机信息验证用户的合法身份。为了防止第三方获取用户隐私和移动云服务的商业机密,之后将不再参与用户与云服务间的密钥验证过程。用户身份证书注册和云服务账户的验证过程中本文均采用零知识验证算法,在保证用户密钥安全的同时节省计算开销和密钥传递时间。在密钥处理上,本文的身份密钥和共享密钥都是使用绑定用户身份信息的方法,防止攻击者盗用用户信息,同时也防止用户把权限外借给别人使用。同时验证了第三方的半可信状态以及身份密钥与共享密钥的安全性。

参考文献:

[1] LING C, SU W, MENG K, *et al.* cloud computing security: Architecture, mechanism and modeling[J]. Chinese Journal of Computers, 2013, 36(9): 1765 - 1784.(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).

[2] OpenID[EB/OL].[2013-10-20]. http://openid.net.

[3] MAGANIS G, SHI E, CHEN H, *et al*. Opaak: using mobile phones to limit anonymous identities online[C]// Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services. New York: ACM, 2012: 295 - 308.

[4] WANG Z, SHA K, LYU W. Slight homomorphic signature for access controlling in cloud computing[J]. Wireless Personal Communications, 2013, 73(1): 1 - 11.

[5] CAMENISCH J, LYSYANSKAYA A. A signature scheme with efficient protocols[M]. Berlin: Springer, 2003: 268 - 289.

[6] CAMENISCH J, STADLER M. Efficient group signature schemes for large groups[C]// Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 1997: 410 - 424.

[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, JENSEN M, *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 the 2013 International Workshop on Security in Cloud Computing. New York: 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.

(上接第 1892 页)

[7] WANG Y, DU W. Security analysis and improvement of certificateless signature scheme without bilinear pairing[J]. Journal of Computer Applications, 2013, 33(8):2250 - 2252.(王怡,杜伟章.无双线性对的无证书签名方案的分析和改进[J].计算机应用,2013,33(8):2250 - 2252.)

[8] CHAUM D. Blind signatures for untraceable payments [C]// Proceedings of Crypto83. Heidelberg: Springer-Verlag, 1983: 199 - 203.

[9] YAO Y, ZHU H, CHEN K. Generalized ElGamal type blind signature based on affine transform[J]. Acta Electronica Sinica, 2000,28(7):128 - 129.(姚亦峰, 朱华飞, 陈抗生. 基于二元仿射变换的广义 ElGamal 型盲签名方案[J]. 电子学报, 2000, 28(7): 128 - 129.)

[10] SU W, ZHANG Y, ZHANG X, *et al.* Certificateless blind signature scheme[J]. Journal of University of Electronic Science and Technology of China, 2009,38(4):533 - 536.(苏万力,张跃宇,张晓红,等.无证书盲签名方案[J].电子科技大学学报,2009,38(4):533 - 536.)

[11] YANG X, LIANG Z, GUO Y, *et al.* An efficient certificateless blind signature scheme[J]. Journal of Nanjing University of Posts and Telecommunications: Natural Science Edition, 2009,29(3): 37 - 42.(杨晓元,梁中银,郭耀,等. 一个高效的无证书盲签名方案[J].南京邮电大学学报:自然科学版,2009,29(3):37 - 42.)

[12] POINTCHEVAL D, STEM J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3):361 - 396.