基于密钥共享的分层混合认证模型

赵茭茭 马文平 罗 维 刘小雪
(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要 随着信息时代的迅速发展,云计算数据访问安全已经成为了用户最关心的问题。身份认证技术是确保参与者在开放的网络环境中实现安全通信的一种重要手段,如何利用身份认证技术为云环境安全保驾护航,成为学者研究的热点。文中通过公钥基础设施(Public Key Infrastructure,PKI)颁发CA证书以在不同云服务间建立信任,将多个采用身份密码体制(Identity-Based Encryption,IBE)的云联合起来;采用分层身份加密体系,引入共享密钥技术,通过选取成环结构,提出一种PKI-IBE混合认证模型方案,并对方案的安全性进行分析,从理论上证明了云环境下PKI-IBE(Public Key Infrastructure-Identity-Based Encryption)同层成环模型提供服务的可行性。同时文中设计了一种基于该模型的签密技术,通过公私密钥对实现云内认证以及跨云认证。安全性理论证明与性能分析表明,该方案在计算量稍增加的前提下,保证了足够的安全性,更加满足云环境下的用户分属不同云域的认证以及用户安全访问的需求,有效解决了云环境中数据访问的安全问题。

关键词 云安全,PKI,IBE,层次模型,身份认证

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.02.018

Hierarchical Hybrid Authentication Model Based on Key Sharing

ZHAO Jiao-jiao MA Wen-ping LUO Wei LIU Xiao-xue
(State Key Laboratory of Integrated Services Networks,Xidian University,Xi'an 710071,China)

Abstract With the rapid development of the information age,cloud computing data access security has become the most concerned issue for users. Identity authentication technology is an important means to ensure that participants implement secure communications in an open network environment,and how to use identity authentication technology to escort the cloud environment has become a hot issue for many scholars. This paper proposed a public key infrastructure-identity-based encryption hybrid authentication model scheme by establishing a trust relationship between different cloud services by CA certificate that Public Key Infrastructure (PKI) issued,combining multiple clouds which use Identity Based Encryption (IBE) system,adopting hierarchical identity encryption system,introducing shared key technology,and choosing ring structure. And the security of the scheme was analyzed to prove the feasibility of providing services based on the identity-based hybrid authentication model in the cloud environment. At the same time,a signcryption technology based on this model was designed to achieve cloud authentication and cross cloud authentication by the public and private key pairs. Performance analysis shows that under the premise of a slight increase in the amount of calculation,the scheme ensures sufficient security,and better satisfies the requirements of users in the cloud environment belonging to different cloud domains and users' secure access,and solves the problem of data access security in a cloud environment effectively.

Keywords Cloud security,PKI,IBE,Hierarchical model,Identity authentication

1 引言

云计算是基于互联网的,以现收现付的方式,为有服务需求的网络提供基础设施和应用程序[1-2]。但随着云平台的迅猛发展,云计算系统面临着严重的安全挑战[3]。由于云端的数据可共享,只要用户提供匹配的身份验证消息,该用户就能访问其权限下的数据。攻击者当获取到合法用户的身份验证消息时便可冒充合法用户,访问云端数据,这样用户数据将完

到稿日期:2018-01-04 返修日期:2018-03-15 本文受国家自然科学基金(61373171),高等学校创新引智计划项目(B08038),国家重点研发计划重点专项(2017YFB0802400)资助。

赵茭茭(1993-),女,硕士生,主要研究方向为信息安全,E-mail:zjj582984208@163.com;**马文平**(1966-),男,教授,博士生导师,主要研究方向为密码学,E-mail:wp_ma@mail.xidian.edu.cn(通信作者);**罗 维**(1987-),男,博士生,主要研究方向为密码学和云计算安全;**刘小雪**(1991-),女,博士生,主要研究方向为密码学和云计算安全。

全暴露在攻击者面前，其他安全措施也都将失效，攻击者便可为所欲为，如修改用户数据、窃听用户活动、恶意消费等。而且，如果云计算平台被成功攻击，大量重要的资源都会掌握在破坏者手里，进而攻击者可以计划规模更加强大的攻击，最终导致的信息安全事故将很难想象。因而，仿冒攻击是云计算面对的首要安全威胁。云服务提供商若想安全地提供相应服务，就必须拥有完备的身份认证机制，为用户和云服务提供商的身份真实性提供保证[4]。合适的认证机制及管理对于确保识别身份信息以及提高云计算系统的安全性至关重要；同时，用户与云服务器之间的双向认证是云环境下用户访问云服务器数据或使用所需服务的重要前提[5]。

国内外学者设计了一系列适用于云计算环境的身份认证方案。Li 等于 2009 年基于双线性运算和身份密码体制提出了基于分层身份机制的混合云身份认证方案[6]，通过签名和加密算法实现了信息互交，但该模型对根密钥的依赖性较强，一旦根密钥或者私钥生成中心(Private Key Generator，PKG)密钥泄漏，将导致系统或者域内所有 PKG 和用户瘫痪，因此安全性较低。随后，Yan 等提出了基于标识的分层密码体制 HIBC(Hierarchical Identity-Based Croptography)的身份认证模型方案[7]，分层 ID 树结构定义用户身份的 ID 值，保证了用户身份的唯一性，但没有对详细的认证过程进行论证。

文献[8-10]设计了基于数字证书的云端身份认证方案，但数字证书验证频繁，计算负载较重。文献[11-13]提出了基于身份密码体制的身份认证方案，能实现访问用户与云服务提供商之间的身份认证，但存在密钥托管问题。

文中基于公钥基础设施(PKI[14])和身份密码体制(IBE[15])的组合优势[16-18]，建立了一种 PKI-IBE 组合身份认证模型，与传统 PKI 或 IBE 认证框架相比，简化了系统结构，节约了成本；同时，将层次模型应用于云计算环境中，使得该模型具有安全、高效、灵活等特点，适用于大范围开放式环境；另外，引入环结构，增强了模型的安全性，使云内认证及跨云认证更加安全可行。

2 预备知识

2.1 密钥共享方案

Shamir[19]和 Blakley[20]于 1979 年提出了密钥共享方案，并分别提出几种不同的(k,n)门限的密钥共享方案。门限密钥共享方案的具体过程如下：

1)初始化：假设 q 是一个大素数，$s\in Z_q$ 是将要分享的密钥，可信中心 T_n 随机选择一个 $k-1$ 次随机多项式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}$ 使 $f(0)=a_0=s$；

2)密钥分发：T_n 选取 n 个非零且互不相同的随机数 x_1，x_2，…，x_n，计算 $y_i=f(x_i)(1\leqslant i\leqslant n)$，并将 y_i 作为子密钥发送给参与者 $P_i(1\leqslant i\leqslant n)$；

3)密钥恢复：不妨假设从 n 个参与者中任选的 k 个参与者为 P_1，P_2，…，P_k 则这 k 个参与者可以利用 Lagrange 插值公式恢复出密钥，具体算法为 $s=\sum_{i=1}^{k}y_i\prod_{j=1,j\neq i}^{k}\frac{x-x_j}{x_i-x_j}$。

(k,n)门限密钥共享方案有以下几个特点：1)即使恶意攻击者获得 $k-1$ 个子密钥，它也不能获得任何密钥的有用信息；2)即使 $n-k$ 个子密钥遭到破坏，密钥仍然可以恢复出来；3)将密钥分散管理，可有效避免权利过于集中而造成的权利滥用问题。本文符号如表 1 所列。

表 1 本文用到的符号

Table 1 Symbols in this paper

参数	含义
k	门限值
n	参与者的个数
$P_i(1\leqslant i\leqslant n)$	密钥共享参与者
$e(\cdot,\cdot)$	双线性映射
$H(\cdot)$	哈希函数
$\rightarrow$	从左边集合到右边集合的映射
$\|$	字符串连接

2.2 双线性映射

设 G_1 和 G_2 均为阶为 p 的乘法循环群，p 是素数。如果映射 $e:G_1\times G_1\rightarrow G_2$ 满足以下性质，则称 e 是一个双线性映射[12]。

1)双线性：对于任意的 $a,b\in\mathbb{Z}_p$ 和 $R,S\in G_1$，有 $e(R^a,S^b)=e(R,S)^{ab}$；

2)非退化性：存在 $R,S\in G_1$，使 $e(R,S)\neq 1_{G_2}$，1_{G_2} 代表 G_2 群的单位元；

3)可计算性：对于任意的 $R,S\in G_1$，存在有效的算法使之能够计算 $e(R,S)$ 的值。

3 云环境下的分层混合认证模型

3.1 云环境下的 PKI-IBE 组合模型

图 1 所示为云环境下基于 PKI-IBE 的分层成环认证模型。该体系通过 PKI 技术在各个云服务器之间建立起可靠的信任关系，各个云服务器采用了基于身份的密码体制，利用分层模型，采取成环结构构建出扩展性强、服务动态组合、易用性更高、安全性更高的认证服务系统。在该模型中，CA 负责颁发证书给根 PKG(PKG_{rA} 和 PKG_{rB})以建立 A，B 两个私有云之间的信任关系，根 PKG 通过分层模型将共享密钥分配给环 PKG(如 PKG_{cA1} 等)。

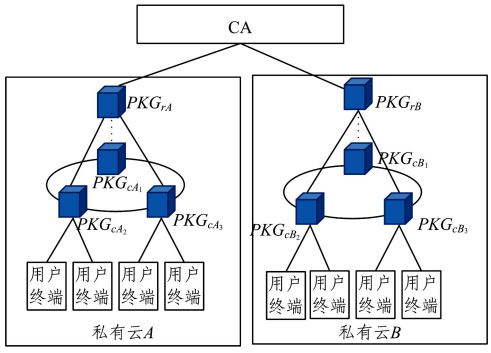

图 1 基于 PKI-IBE 的分层成环认证模型

Fig. 1 Hierarchical looped authentication model based on PKI-IBE

3.2 层次模型方案

图 2 所示为基于身份的层次模型，该模型由 3 层组成。

第一层(level-1)为根 PKG(PKG_r)；第二层(level-2)为子 PKG(PKG_c)，每个子 PGB 对应云计算服务的其中一个数字中心，如云服务提供商；底层(level-3)是用户层。在云环境基于身份的层次模型中，每个节点都有唯一的名称，该名称是节点加入云服务时注册的可分辨名称(DN)。例如，在图 2 中，根节点 r 的 DN 为 DN_r，节点 v 的 DN 为 DN_v，节点 u 的 DN 为 DN_u。定义节点的身份是从根节点到当前节点本身的 DN 字符串，即实体 r 的身份 $ID_r=DN_r$，实体 v 的身份 $ID_v=DN_r \| DN_v$，实体 u 的身份 $ID_u=DN_r \| DN_v \| DN_u$。

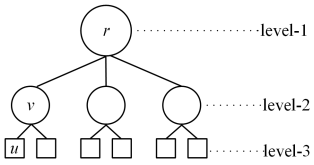

图 2　基于身份的层次模型

Fig. 2　Identity-based hierarchy model

3.3　密钥生成

3.3.1　PKG_r 的设置

1)选择 G_1，G_2 分别为两个阶为素数 p 的循环群，双线性映射 $e:G_1\times G_1\rightarrow G_2$；

2)设 g 为生成元；

3)选择两个单向的哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$ 和 $H_2:\{0,1\}^*\rightarrow\{0,1\}^n$；

4)假设 q 为一个大素数，选择一个随机数 $s\in Z_q$，设置 $pk=g^s$，s 为 PKG_r 的主密钥，(s,pk)构成系统主密钥对，系统公开参数为$\langle G_1,G_2,e,g,pk,H_1,H_2\rangle$。

3.3.2　PKG_c 的设置

1)初始化：s 是 PKG_r 的主密钥，即为(k,n)方案中的共享密钥，假设 level-2 是由 n 个 PKG_c 构成的环，则 s 可由子秘密持有者 $P_1,P_2,\cdots,P_n$ 共享。

2)密钥分发：

Step1　PKG_r 随机选取一个 $k-1$ 次随机多项式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}(a_0\neq 0)$，使得 $f(0)=a_0=s$；

Step2　PKG_r 再选取另一个 $k-1$ 次随机多项式 $g(x)=b_0+b_1x+b_2x^2+\cdots+b_{k-1}x^{k-1}(a_0\neq b_0)$；

Step3　PKG_r 计算 $m_i=f(i)$，$r_i=g(i)$，并向 PKG_c 中的 $P_i(1\leqslant i\leqslant n)$发送密钥$(m_i,r_i)$，$m_i$ 为子密钥，r_i 为验证子密钥，公开 $pk_i=g^{m_i}(1\leqslant i\leqslant n)$；

3)验证阶段：环中所有 $P_i(1\leqslant i\leqslant n)$共同选取随机数 a_1，$a_2\in Z_q^*$，当收到 m_i 和 r_i 时，公布 $a_1m_i+a_2r_i$ 的值，计算$(i,a_1m_i+a_2r_i)$这 n 个点的拉格朗日多项式$l(x)$，若 $l(x)$是 $k-1$ 次的，则所有子密钥都是有效的，否则环密钥中存在错误的子密钥。

3.3.3　用户私钥

1)假设 PKG_c 中的 $PKG_{ci}(pk_i=g^{m_i},1\leqslant i\leqslant n)$是由 α 个用户组成的用户集 $U=\{u_1,u_2,\cdots,u_\alpha\}$，令 $u_A=u_j(1\leqslant j\leqslant\alpha)$；

2)u_A 随机选取 $x_A\in Z_q$，计算 $pk_A=g^{x_A}$ 以及 $P_A=H_2(ID_A)(ID_A=DN_r \| DN_i \| DN_A)$，同时将$\{pk_A,P_A,DN_A\}$发送给 PKG_{ci}；

3)PKG_{ci} 收到 u_A 消息，根据 DN_A，DN_i，DN_r 获取 ID_A，验证 $P_A\stackrel{?}{=}H_2(ID_A)$，若成立，则计算 $Q_A=H_1(P_A)$，并将$(pk_A)^{m_i}$ $(Q_A)^{m_i}$ 发送给 u_A，同时在用户注册列表中保存$\{DN_A,P_A,pk_A\}$；

4)u_A 计算部分私钥$(pk_A)^{m_i}(Q_A)^{m_i}/(pk_i)^{x_A}=(Q_A)^{m_i}$，并验证 $e((Q_A)^{m_i},g))\stackrel{?}{=}e(H_1(P_A),pk_i)$，若成立，则用户最终的私钥 $sk_A=(x_A,(Q_A)^{m_i})$，公开公钥 pk_A。

4　身份认证模型的应用

假设两个可信任云域分别为云域 A 和云域 B，PKG_{ci} $(1\leqslant i\leqslant n)$是云域 A 内 PKG_{cA} 中任意一个密钥生成中心，$pk_i=g^{m_i}$，u_A 是 PKG_{ci} 中任意一个用户，私钥 $sk_A=(x_A,(Q_A)^{m_i})$，公钥 $pk_A=g^{x_A}$。PKG_{cj} $(1\leqslant j\leqslant n)$是云域 B 内 PKG_{cB} 中任意一个密钥生成中心，$pk_j=g^{m_j}$，u_B 是 PKG_{cj} 中的任意一个用户，私钥 $sk_B=(x_B,(Q_B)^{m_j})$，公钥 $pk_B=g^{x_B}$。通过层次模型的建立可以实现 u_A 与 PKG_{ci} 之间的相互认证，即云内认证；u_A 与 u_B 之间的相互认证，即跨域认证。

4.1　云内认证

1)用户 u_A 随机选取 $y\in Z_q$，利用私钥 $sk_A=(x_A,(Q_A)^{m_i})$，计算 $Y=g^{y+x_A}$ 和 $Y'=(pk_i)^{y+x_A}$；输入匿名身份 P_A，计算 $h_A=H_2(Y \| Y' \| pk_A \| P_A)$，生成签名 $\sigma_A=h_A^{x_A}Q_A^{m_i}$，发送认证消息$\{Y',pk_A,\sigma_A,P_A\}$给 PKG_{ci}。

2)PKG_{ci} 收到认证消息后，计算 $Y=(Y')^{1/m_i}=(g^{m_i})^{(y+x_A)/m_i}=g^{y+x_A}$ 和 $h_A=H_2(Y \| Y' \| pk_A \| P_A)$，验证 $e(\sigma_A,g)\stackrel{?}{=}e(h_A,pk_A)e(H_1(P_A),pk_i)$，若成立，确认用户 u_A 的身份；PKG_{ci} 随机选取 $z\in Z_q$，计算 $Z=g^{z+m_i}$，$Z'=(pk_A)^{z+m_i}$ 和 $h_i=(Z \| Z' \| pk_i)$，生成 PKG_{ci} 的签名 $\sigma_i=h_i^{m_i}$，并发送认证消息$\{Z',pk_i,\sigma_i\}$给 u_A。

3)u_A 收到认证消息之后，计算 $Z=(Z')^{1/x_A}=(g^{x_A})^{(z+m_i)/x_A}=g^{z+m_i}$ 和 $h_i=H_2(Z \| Z' \| pk_i)$，验证 $e(\sigma_i,g)\stackrel{?}{=}e(h_i,pk_i)$，若成立，确认用户 PKG_{ci} 的身份。

4.2　跨云认证

1)用户 u_A 随机选取 $y\in Z_q$，利用私钥 $sk_A=(x_A,(Q_A)^{m_i})$，计算 $Y=g^{y+x_A}$ 和 $Y'=(pk_B)^{y+x_A}$；输入匿名身份 P_A，计算 $h_A=H_2(Y \| Y' \| pk_A \| P_A)$，生成 h_A 的签名 $\sigma_A=h_A^{x_A}Q_A^{m_i}$，发送认证消息$\{Y',pk_A,\sigma_A,P_A\}$给 u_B；

2)u_B 在收到认证消息之后，计算 $Y=(Y')^{1/x_B}=(g^{x_B})^{(y+x_A)/x_B}=g^{y+x_A}$ 和 $h_A=H_2(Y \| Y' \| pk_A \| P_A)$，验证 $e(\sigma_A,g)\stackrel{?}{=}e(h_A,pk_A)e(H_1(P_A),pk_i)$，若成立，确认用户 u_A 的身份；u_B 随机选取 $z\in Z_q$，利用私钥 $sk_B=(x_B,(Q_B)^{m_j})$，计算$Z=g^{z+x_B}$ 和 $Z'=(pk_A)^{z+x_B}$，输入匿名身份 P_B，计算 $h_B=H_2(Z \| Z' \| pk_B \| P_B)$，生成 h_B 的签名 $\sigma_B=h_B^{x_B}Q_B^{m_j}$，发送认证消息$\{Z',pk_B,\sigma_B,P_B\}$给 u_A，并计算与 u_A 间的会话密钥 $SK=Y^{z+x_B}$。

3)u_A 收到认证消息之后，计算 $Z=(Z')^{1/x_A}=$

$(g^{x_A})^{(z+x_B)/x_A}$ 和 $h_B=H_2(Z\parallel Z'\parallel pk_B\parallel P_B)$，验证 $e(\sigma_B,g)?=e(h_B,pk_B)e(H_1(P_B),pk_B)$，若成立，确认用户 u_B 的身份，并计算会话密钥 $SK=Z^{y+x_A}$。

5 方案分析

5.1 抗伪造攻击和抗重放攻击

云内认证及跨云认证身份的安全性与签名息息相关，文献[23]已经充分证明了此签名无法伪造，因此攻击者并不能对认证消息及响应消息进行有效伪造；同时，认证消息及响应消息中含有随机数，所以本方案也能合理地抵挡攻击者的重放攻击。

5.2 会话密钥的前后向安全

u_A 计算会话密钥 $SK=Y^{z+x_B}=(g^{y+x_A})^{z+x_B}=g^{(y+x_A)(z+x_B)}$，用户 u_B 计算会话密钥 $SK=Z^{y+x_A}=g^{(y+x_A)(z+x_B)}$，两者的会话密钥均为 $g^{(y+x_A)(z+x_B)}$。由于 y 与 z 均为随机数，每轮会话均不相同，因此会话密钥具有随机性。即使攻击者能够获取到当前密钥，也无法根据当前密钥计算出之前或者之后的会话密钥，因此会话密钥具有前后向安全性。

5.3 身份认证模型安全分析

因为云计算域的用户众多，所以保证用户身份的合法性至关重要，因此本方案将用户身份认证模型的安全与已有身份认证模型进行比较，结果如表 2 所列。本方案通过两方面来保证系统的安全性：

1)若攻击者想要攻击 PKG_c 中的子密钥来恢复主密钥，子密钥必须达到门限值，即攻击者必须攻击门限值 k 个以上的子密钥，任何不足门限值 k 个的子密钥均无法恢复主密钥，这是因为 k 个以下的方程式无法解开未知数为 k 的方程组，攻击者即使能够伪造出门限值 k 个子密钥，也必须完全保证这 k 个子密钥全部正确。

2)即使 PKG_c 中有一个被攻击，对于用户私钥而言，影响的是 PKG_c 下一层的用户，但对云域内不属于此 PKG_c 的用户私钥没有任何影响，保证了云域内众多用户的安全性。

因此，由以上两个方面可知，本文方案比文献[21-22]中的方案更具安全性。

表 2 用户身份认证模型的安全性能比较

Table 2 Comparison of security features of user identity authentication model

方案	获得主密钥攻击次数/次	PKG_{ci} 出错是否会影响用户私钥	系统安全性
文献[21]	1	影响所有用户	不安全
文献[22]	1	无环，仅影响子 PKG 之下的用户	不安全
本文方案	至少 k	仅影响 PKG_{ci} 之下的用户	安全

5.4 性能分析

如表 3 所列，假设只考虑计算量相对较大的指数 Exp 与双线性计算 P_a，本文方案在用户私钥生成阶段比文献[23-24]的方案多两次指数运算，但这两个方案存在明显的安全缺陷，必须通过建立安全信道来保证用户私钥安全，而且不能进行云内认证以及跨云认证。文献[25]与本文方案的计算开销相对都比较大，但本方案并不需要建立安全信道，同时可以支持云内认证以及跨云认证，因此本方案的计算开销与安全性能均优于文献[23-25]中的方案。

表 3 用户计算开销与安全性能比较

Table 3 Comparison of users' computing overhead and security performance

	文献[23]	文献[24]	文献[25]	本文方案
用户私钥生成	$2P_a$	$2P_a$	$2Exp+2P_a$	$2Exp+2P_a$
跨域认证	$2Exp+4P_a$	$2Exp+4P_a$	$5Exp+2P_a$	$4Exp+2P_a$
抗重放攻击	√	√	√	√
双向认证	√	√	√	√
安全信道	√	√	×	×
云内认证	×	×	×	√
跨域认证	×	×	×	√

结束语 本文通过提出一种 PKI-IBE 混合身份认证模型，来解决在云环境中的数据访问安全问题；同时将分层身份加密体系引入该模型，来避免 PKG 拥有主密钥所产生的安全隐患，在分层中利用共享密钥成环结构，使得云环境身份认证的安全性能大幅提高。其适合用户众多且大范围开放的云环境域。另外，本文还设计了一种基于该方案的云内认证及跨云认证方案。分析结果表明，在计算量稍微复杂的前提下，该方案具有较高的安全性。下一步将基于密钥共享的分层混合认证模型，构造更加安全且高效的云端认证方案。

参 考 文 献

[1] 周洪波. 云计算技术、应用、标准和商业模式[M]. 北京：电子工业出版社，2010.

[2] MELL P, GRANCE T. The NIST Definition of Cloud Computing: Technical Report 800-1450 [R]. National Institute of Standards and Technology(NIST), 2011.

[3] XIE L Z. Cloud computing and cloud computing security overview[J]. Information Security and Communication Confidentiality, 2012, 23(12): 24-25. (in Chinese)
谢灵智. 云计算及云计算安全概述[J]. 信息安全与通信保密，2012，23(12)：24-25.

[4] LUO J. Encryption mechanism for access control in cloud computing environment[J]. Information Security and Communication Confidentiality, 2012(11): 44-46. (in Chinese)
罗俊. 采用加密机制在云环境中进行访问控制[J]. 信息安全与通信保密，2012(11)：44-46.

[5] ZHU Z Q. Research on Some Theoretical and Key Technologies of Hybrid Cloud Service Security[D]. Wuhan: Wuhan University, 2011(in Chinese)
朱智强. 混合云服务安全若干理论与关键技术研究[D]. 武汉：武汉大学，2011.

[6] LI H, DAI Y, TIAN L, et al. Identity-Based Authentication for Cloud Computing[C]// IEEE International Conference on Cloud Computing. Springer, Berlin, Heidelberg, 2009.

[7] YAN L, RONG C, ZHAO G. Strengthen Cloud Computing

Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography[C]// IEEE International Conference on Cloud Computing. Springer, Berlin, Heidelberg, 2009.

[8] BINU S, MISBAHUDDIN M, RAJ P. A mobile based remote user mutual authentication scheme without verifier table for cloud based services[C]// Proceedings of the Third International Symposium on Women in Compution and Informatics. New York, 2015: 502-509.

[9] ZHOU C C, TIAN X L, ZHANG N, et al. Research on Authentication Technology in Cloud Computing[J]. Computer Science, 2016, 43(6A): 339-341. (in Chinese)
周长春，田晓丽，张宁，等. 云计算中身份认证技术研究[J]. 计算机科学，2016，43(6A)：339-341.

[10] HU Y. Research on the Authentication of Cloud Computing Environment[D]. Beijing: Beijing University of Technology, 2014. (in Chinese)
扈莹. 云计算环境的身份认证的研究[D]. 北京：北京工业大学，2014.

[11] CHEN P L, YANG J H, LIN C I. ID-Based user authentication scheme for cloud computing[J]. Journal of Electronic Science and Technology, 2013, 11(2): 221-224.

[12] LI X H, YANG B. Efficient identity-based signature authentication scheme in cloud service[J]. Int'l Journal of Advancements in Computing Technology, 2013, 5(5): 867-876.

[13] CAO C L, ZHANG R, ZHANG M Y, et al. IBC-Based entity authentication protocols for federated cloud systems[J]. On Internet & Information Systems, 2013, 7(5): 1291-1312.

[14] LEI Y, YANG S P. PKI-based signature mechanism[J]. Communication Technology, 2013(1): 43-46. (in Chinese)
雷咏，杨世平. 基于 PKI 的签名机制[J]. 通信技术，2013(1)：43-46.

[15] CUI J K. CPK Based Authentication and Key Management Technology[D]. Harbin: Harbin Institute of Technology, 2010. (in Chinese)
崔杰克. 基于 CPK 的认证及密钥管理技术研究[D]. 哈尔滨：哈尔滨工业大学，2010.

[16] TIAN J. Comparative Analysis and Application of PKI and IBC in Hybrid Cloud Service Authentication Technology[J]. Computer Security, 2014(6): 33-35. (in Chinese)
田静. 混合云服务身份认证技术 PKI 和 IBC 对比分析及应用[J]. 计算机安全，2014(6)：33-35.

[17] LIU T Q. Research and Design of Authentication Service System Based on Identity and Password System in Cloud Environment[D]. Zhengzhou: Henan University of Technology, 2016. (in Chinese)
刘团奇. 云环境下基于身份密码体制的认证服务体系的研究与设计[D]. 郑州. 河南工业大学. 2016.

[18] YANG B. IBC and PKI combination of applied research. Information Engineering University[D]. Luoyang: Information Engineering University, 2009. (in Chinese)
杨斌. IBC 和 PKI 组合应用研究[D]. 洛阳：解放军信息工程大学，2009.

[19] SHAMIR A. How to share a Secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[20] BLAKLEY G R. Safeguarding cryptographic keys[C]// Proceedings of the AFIPS. 1979: 313-317.

[21] JIANG H. Research on key management based on authentication password system in cloud environment[D]. Chengdu: Southwest Jiaotong University, 2016. (in Chinese)
江昊. 云环境中基于身份认证密码体制的密钥管理问题研究[D]. 成都：西南交通大学，2014.

[22] MA L L. Research on Identity Authentication Based on Combination of PKI and IBE in Hybrid Cloud Computing[D]. Yunnan: Yunnan University, 2016. (in Chinese)
马丽莉. 混合云计算下基于 PKI 和 IBE 组合的身份认证机制研究[D]. 云南：云南大学，2016.

[23] MISHRA R. Anonymous remote user authentication and key agreement for cloud computing [C]// Proceedings of the 3rd Int'l Conference on Soft Computing for Problem Solving. Springer-Verlag, 2014: 899-913.

[24] DONG Z M, ZHANG L, LI J T. Security enhanced anonymous remote user authentication and key agreement for cloud computing[C]// Proceedings of the 17th Int'l Conference on Computational Science and Engineering. IEEE Computer Society Press, 2014: 1746-1751.

[25] WNAG Z H, HAN Z, LIU J Q, et al. Authentication Scheme Based on PTPM and Certificateless Public Key in Cloud Environment[J]. Journal of Software, 2016, 27(6): 1523-1537. (in Chinese)
王中华，韩臻，刘吉强，等. 云环境下基于 PTPM 和无证书公钥的身份认证方案[J]. 软件学报，2016，27(6)：1523-1537.