



混合云联合身份认证与密钥协商协议设计^{*}

王崇霞¹, 高美真², 刘倩³, 周贤伟³

(1. 长治学院计算机系 长治 046010; 2. 焦作师范高等专科学校计算机与信息工程学院 焦作 454000;
3. 北京科技大学计算机与通信工程学院 北京 100083)

摘要: 针对混合云中用户群不同, 认证机制不一致的特点, 基于双线性对和密钥协商机制, 提出了一种混合云联合身份认证和密钥协商协议, 实现了混合云用户身份认证和授权策略等安全信息的分布式管理与动态获取。通过理论分析和实验证明, 该协议具有安全高效的特点, 可以有效预防篡改数据、伪造用户身份、重放和中间人攻击等, 且以较小的计算量和通信开销, 为混合云联合身份认证和密钥协商提供了一种较实用的解决方案。

关键词: 混合云; 身份认证; 双线性对; 安全性

doi: 10.3969/j.issn.1000-0801.2014.04.014

Design of United Identity Authentication and Key Agreement Protocol for Hybrid Cloud

Wang Chongxia¹, Gao Meizhen², Liu Qian³, Zhou Xianwei³

(1. Department of Computer Science, Changzhi University, Changzhi 046010, China;
2. School of Computer and Information Engineering, Jiaozuo Teachers College, Jiaozuo 454000, China;
3. School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)

Abstract: Aiming at the heterogeneous users and the inconsistent authentication mechanism for hybrid clouds, a design of united identity authentication and key agreement protocol for hybrid cloud was proposed based on bilinear pairings and key agreement mechanism, which could realize the distributed management and dynamic acquisition of security information of authentication and authorization policy. The theoretical analysis and experiment results show that the proposed protocol is safe and efficient, which can effectively prevent data tampering, identity forging, replay attacks and man-in-the-middle attacks. Else the proposed protocol provides a practical solution on identity authentication and key agreement in hybrid clouds with less computation and communication overheads.

Key words: hybrid cloud, identity authentication, bilinear pairing, security

1 引言

云计算是一种包括大量计算资源的新型的计算模式, 根据 NIST (National Institute of Standards and Technology) 的定义, 云计算基于互联网, 以现收现付的方式, 对服务

需求的网络提供基础设施、平台和应用程序等^[1,2]。随着云计算应用的深入, 云间资源整合和信息交互将是云计算的主要发展方向。

云计算主要有 3 种部署结构: 公共云 (public cloud)、私有云 (private cloud) 和混合云 (hybrid cloud)^[3,4]。公共云和

^{*} 国家自然科学基金资助项目 (No.61003250, No.61170014), 教育部科学技术研究重大基金资助项目 (No.311007)



私有云通常只有一个服务供应商,它允许用户通过接口使用主流 Web 浏览器访问云^[4],公共云扩展性好但性能滞后,而私有云可靠性好但扩展性有限^[3]。结合两者的优势,于是就产生了混合云,混合云包含多个私人云和/或公共云,如图 1 所示。混合云可能有多个服务供应商^[5],而每一个服务供应商都有自己的用户群和身份管理系统。用户群不同、认证机制不一致的特点,导致用户访问不同的云服务时可能需要多个不同的数字身份和口令^[5,6]。这既给用户访问混合云带来不便,也增加了操作的复杂性,降低了工作效率,于是业界提出了集中式统一身份管理模式。但是,由于用户身份信息的隐秘性,云服务供应商往往不愿意共享用户身份信息,致使集中式统一身份管理实现的难度增加^[7]。云计算结构各异、动态性强、分布广阔,混合云中的服务供应商之间可以通过建立某种动态松耦合的联合认证关系,实现用户身份认证和授权策略等安全信息的分布式管理与动态获取。

针对混合云的身份认证模式,业界提出了不同的方法或策略。2009 年 Li Hongwei 等人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^[8],通过签名和加密算法实现信息交互;其后, Yan Liang 等人提出了基于 HIBC 的混合云身份认证模型^[6],但没有详细的认证过程论证,而基于身份的分层密码体制密钥间的依赖性太强,一旦根密钥或域 PKG(private key generator)密钥泄露,将导致系统或域内的所有 PKG 和用户瘫痪。2012 年

Zhang Qikun 等人提出了云计算环境下的联盟认证协议^[9],提出包含 5 个密钥的树型结构联盟身份认证模型,密钥数量的增加为系统管理和密钥存储增加了负担。本文基于双线性对和认证密钥协商机制提出一种新的混合云联合身份认证与密钥协商方案,在不共享用户身份信息的情况下,实现混合云中资源共享和服务互访。

2 相关的数学难题假设

目前大多数基于身份的密码方案都是基于离散对数和双线性对来构造的,离散对数(discrete logarithm)和双线性对的构造及其相关数学难题如下。

定义 1 (离散对数问题)^[10]: 设 G 是 q 阶群,对于给定 $(P, Q) \in G$,找到整数 $a \in \mathbb{Z}_q^*$,满足 $Q = aP$ 。

定义 2 (双线性映射)^[10]: G_1, G_2 分别是阶位 q 的循环加法和循环乘法群,假设 G_1, G_2 中的离散对数问题是困难问题,则称 $e: G_1 \times G_1 \rightarrow G_2$ 为双线性映射且 e 满足以下属性。

- 双线性: 对任意 $Q, R, S \in G_1, a, b \in \mathbb{Z}_q^*$,有 $e(Q^a, R^b) = e(Q, R^{b^a}) = e(Q^a, R)^b = e(Q, R)^{ab}$ 。
- 非退化性: 存在 $P, Q \in G_1$,使 $e(P, Q) \neq 1$ 。
- 可计算性: 存在一个有效的算法对于任何 $Q, R \in G_1$,可以计算 $e(Q, R)$ 。

定义 3 (CDH 问题)^[10] (computational Diffie-Hellman problem, CDH problem): G_1 为素数 q 阶的循环群,对于随

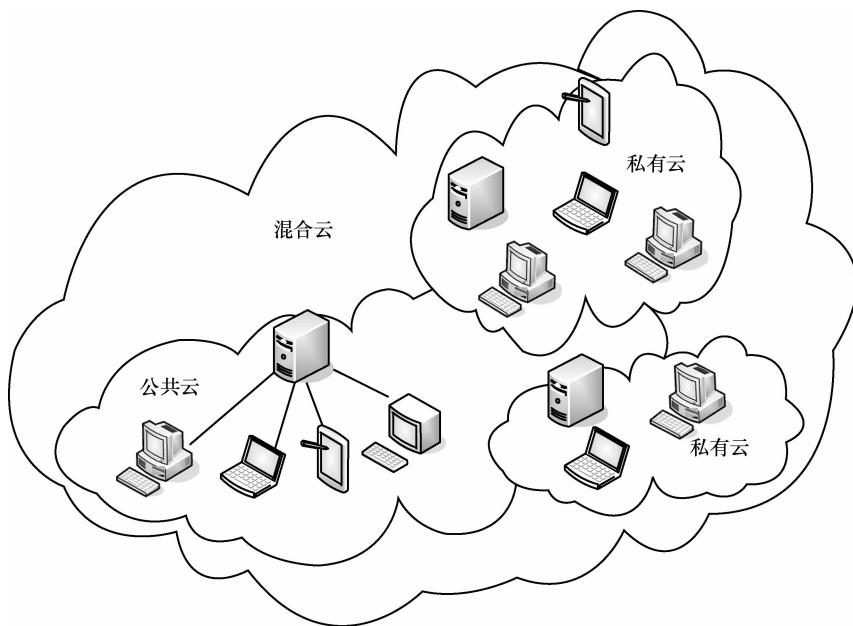


图 1 混合云结构

机给定的 $\langle P, aP, bP \rangle \in G_1$, 其中 $a, b \in \mathbb{Z}_q^*$, 计算 abP 的值。
CDH 的困难性也是基于离散对数问题的。

3 混合云联合身份认证及密钥协商

3.1 认证模型

典型的混合云联合认证模型如图 2 所示, 多个公共云或私有云组合在一起形成了混合云。

定义 4 (末端云): 云计算中由一个认证服务器管理的云计算区域称为末端云。一个末端云包含一个认证服务器、多个应用服务器和多个客户端, 混合云由多个末端云组成^[9]。

本文提出的混合云认证模型中, 所有末端云的 PKG 使用相同的系统参数。假设 G_1, G_2 分别是阶位 q 的循环加法和循环乘法群且 $e: G_1 \times G_1 \rightarrow G_2$ 是双线性映射, p, g 是 G_1 的生成元, 系统参数 $parameter = \{q, G_1, G_2, g, p, e, H_1, H_2\}$, 定义散列函数: $H_1: \{0, 1\}^* \rightarrow \{0, 1\}^* \in \mathbb{Z}_q^*$, $H_2: \{0, 1\}^* \rightarrow G_1$ 。每个末端云 PKG 主密钥和公钥不同, 这在目前基于身份的多域认证方案中是可行的, 通过身份认证模式标准化的推进, 这个假设是可以实现的^[11]。

3.2 符号与标记

Pk_A : A 的公钥。

Sk_A : A 的私钥。

$E_{ks}[y]$: 用对称密钥 ks 加密数据 y 。

$D_{ks}[y]$: 用对称密钥 ks 解密数据 y 。

$H(\cdot)$: 抗碰撞的散列函数。

K_{AB} : 云 A、B 间的协商密钥。

$\parallel$: 消息的串联。

$\|x\|$: x 的比特长度。

$\Rightarrow$: 等同于。

3.3 系统设置

(1) 系统建立: (以云 A 为例设置系统参数如下) 产生随机数 $Sk_A \in \mathbb{Z}_q^*$, $Pk_A = Sk_A g \in G_1$, 选择 Sk_A 为云 A 的主私密钥, Pk_A 为公钥, 认证服务器 AS_A 保存主密钥 Sk_A , 并公布系统参数 $parameter = \{q, G_1, G_2, g, p, Pk_A, H_1, H_2\}$ 。

同理, 其他云的参数设置类同 (以云 B 为例): Sk_B 为云 B 的主私密钥, Pk_B 为公钥, 系统参数 $parameter = \{q, G_1, G_2, g, p, Pk_B, H_1, H_2\}$ 。

(2) 用户注册: 当用户 UA 申请成为云 A 的成员时, UA 输入用户名 ID_{UA} 和口令 PW_{UA} , UA 的身份 $ID_{UA} \in \{0, 1\}^*$, 在用户数据库中保存用户 UA 的相关信息: ID_{UA} 和 $H_1(PW_{UA})$ 。

3.4 联合身份认证及密钥协商协议

假设用户 UA 申请访问云 B 的资源时, 执行如下。

(1) $UA \rightarrow AS_B: \{ID_{UA}, ID_{AS_B}, D_{UA}, E_{W_{UA}}[ticket_{UA}]\}$

UA 申请认证时, 输入用户名和口令, UA 计算 $r_1 = H_1(PW_{UA}) \bmod q \in \mathbb{Z}_q^*$ ($r_1 \neq 0, 1$), 产生随机数 $N_U \in \mathbb{Z}_q^*$, 计算 $D_{UA} = r_1 Pk_A$, $W_{UA} = r_1 g$, UA 产生认证票据 $ticket_{UA} = \{ID_{UA} \parallel ID_{AS_A}, N_U\}$, 并

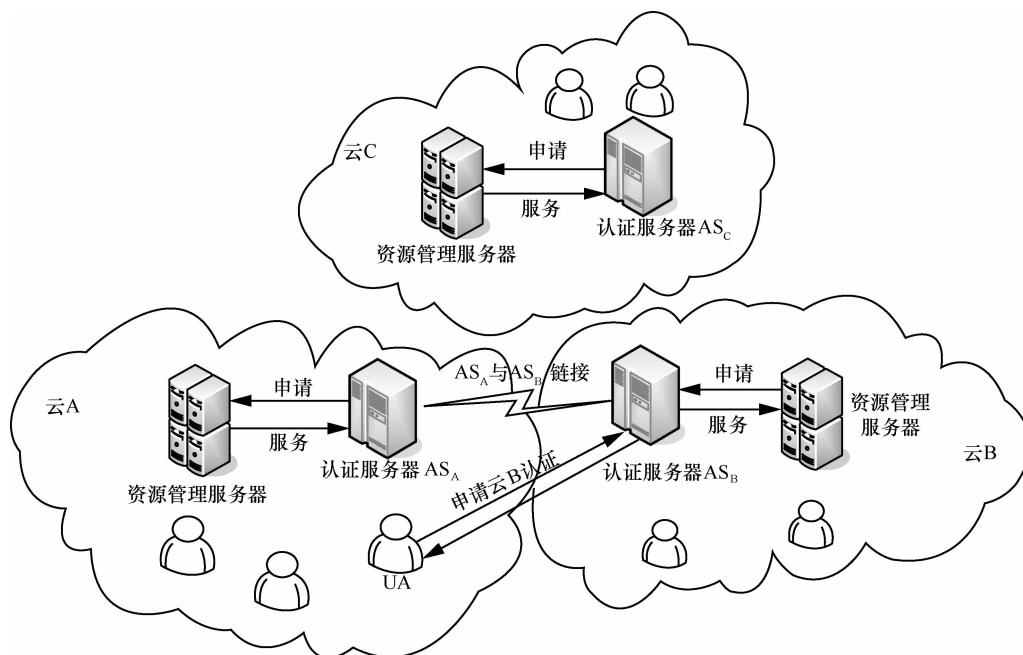


图 2 混合云联合身份认证模型



用 W_{UA} 加密 $ticket_{UA}$ 。发送 $\{ID_{UA}, ID_{AS_B}, D_{UA}, E_{W_{UA}}[ticket_{UA}]\}$ 到 AS_B , 其中 $ID_{UA}, ID_{AS_B}, ID_{AS_A}$ 为用户 $UA, AS_A (PKG_A)$ 和 $AS_B (PKG_B)$ 的身份。

(2) $AS_B \rightarrow AS_A: E_{K_{AB}}[D_{UA}, ID_{AS_B}, ID_{AS_A}, E_{W_{UA}}[ticket_{UA}], N_{RS}]$

AS_B 收到消息后, 检查 UA 是否为本云用户, 如果是, 则按照云内认证服务方式为其提供服务; 否则, 产生随机数 $N_{RS} \in \mathbb{Z}_q^*$, 与 UA 发来的消息 (并不解密 $E_{W_{UA}}[ticket_{UA}]$), 用 AS_A 和 AS_B 间的协商密钥 K_{AB} 加密: $E_{K_{AB}}[D_{UA}, ID_{AS_B}, ID_{AS_A}, E_{W_{UA}}[ticket_{UA}], N_{RS}]$, 一起发送到认证服务器 AS_A 。

(3) $AS_A \rightarrow AS_B: E_{K_{AB}}[D_{UA}, ID_{AS_B}, E_{UA}, \alpha, "1", E_{W_{UA}}[ticket_{UA}'], N_{RS}]$

AS_A 收到消息后, 用协商密钥 K_{AB} 对消息解密, 计算 $W_{UA} = Sk_A^{-1} D_{UA}$, 解密 $D_{W_{UA}}[ticket_{UA}]$, 查找用户信息库中 U_A 的相关信息, 确定 UA 的合法性, 计算 $r_1 = H_1(PW_{UA}) \bmod q, \alpha = H_2(ID_{AS_B})^{r_1}, R_{UA} = g^{-r_1}$ 。产生随机数 $N_{AS} \in \mathbb{Z}_q^*$, 产生新的票据 $ticket_{UA}' = \{ID_{UA} || ID_{AS_A}, N_{UA}, N_{AS}\}$, 并用 W_{UA} 加密。将消息 $E_{K_{AB}}[ID_{AS_B}, ID_{AS_A}, R_{UA}, \alpha, "1", E_{W_{UA}}[ticket_{UA}'], N_{RS}]$ 发送到 AS_B , 其中, "1" 为确认比特, 当确认比特为 "1" 时, 说明 UA 为 AS_A 的合法用户; 为 "0" 时说明 UA 不是 AS_A 的合法用户。

(4) $AS_B \rightarrow UA: \{ID_{UA}, ID_{AS_B}, T_{B1}, T_{B2}, E_{W_{UA}}[ticket_{UA}'], N_{SB}'\}$

AS_B 收到消息后用协商密钥 K_{AB} 解密, 验证随机数 N_{SB} , 如果与发送时一致, 确认消息为 AS_A 的回复消息, 查看验证比特, 如果为 "0", 本次消息传输终止; 否则, 确认 UA 为 AS_A 的合法用户。 AS_B 产生随机数 $t_2, N_{SB}' \in \mathbb{Z}_q^* (t_2 \neq 0, 1)$, 计算 $T_{B1} = g^{t_2}, T_{B2} = R_{UA}^{t_2}$, 将消息 $\{ID_{UA}, ID_{AS_B}, T_{B1}, T_{B2}, E_{W_{UA}}[ticket_{UA}'], N_{SB}'\}$ 发给 UA 。

(5) $UA \rightarrow AS_B: \{ID_{UA}, ID_{AS_B}, T_{A1}, T_{A2}, N_{SB}', N_U'\}$

收到消息后, 验证随机数 N_{SB}' , 用 W_{UA} 解密 $D_{W_{UA}}[ID_{UA} || ID_{AS_B}, N_{UA}, N_{AS}]$, 验证 N_U , 确认此消息为回应消息。产生随机数 $t_1, N_U' \in \mathbb{Z}_q^* (t_1 \neq 0, 1), T_{A1} = g^{t_1}, T_{A2} = (T_{B1})^{-t_1}$ 将 $\{ID_{UA}, ID_{AS_B}, T_{A1}, T_{A2}, N_U'\}$ 发送到 AS_B 。

UA 计算如下:

$$\begin{aligned} key1 &= e(p^h \alpha, T_{B1}) e(H_2(ID_{AS_B}), T_{B2}) \\ &= e(p^h H_2(ID_{AS_B})^h, g^{t_2}) e(H_2(ID_{AS_B}), (g^{-h})^{t_2}) \\ &= e(p^h, g^{t_2}) e(H_2(ID_{AS_B})^h, g^{t_2}) e(H_2(ID_{AS_B}), g)^{-h t_2} \\ &= e(p, g)^{h t_2} \\ key2 &= T_{A1} \times T_{B1} = g^{t_1} \times g^{t_2} = g^{h t_1 + t_2} \end{aligned}$$

(6) AS_B

AS_B 计算如下:

$$\begin{aligned} key1 &= e(p^{t_2} \alpha, T_{A1}) e(H_2(ID_{AS_B}), T_{A2}) \\ &= e(p^{t_2} H_2(ID_{AS_B})^{t_2}, g^{t_1}) e(H_2(ID_{AS_B}), (g^{-h})^{t_1}) \\ &= e(p^{t_2}, g^{t_1}) e(H_2(ID_{AS_B})^{t_2}, g^{t_1}) e(H_2(ID_{AS_B}), g)^{-h t_1} \\ &= e(p, g)^{h t_1} \\ key2 &= T_{A1} \times T_{B1} = g^{t_1} \times g^{t_2} = g^{h t_1 + t_2} \end{aligned}$$

UA 与 AS_B 间的会话密钥为 $K_{UAAS_B} = H_1(D_{UA} || ID_{AS_B} || key1 || key2)$ 。 UA 与 AS_B 可以通过会话密钥实现安全通信。

4 安全和性能

4.1 安全性

引理 1^[12] 假设 G 是一个有限群, $|G|=q$ (q 是一个大素数), 对于任意元素 $g \leftarrow G$ 且令 $g' := k \cdot g$ 。同理, 对元素 $g' \leftarrow G$, 存在元素 $\hat{g} \in G$, 使 $\hat{g} = k \cdot g$ 成功的概率为:

$$pr(\hat{g} = k \cdot g) = 1/q$$

定义 5^[12] 对多项式 $p(\cdot)$, 存在整数 N , 对于所有 $n > N$, 存在 $f(n) < 1/p(n)$, 则认为函数 $f(\cdot)$ 是可以忽略的。

定理 1 对所有的概率多项式时间攻击者, 设计的联合身份认证与密钥协商协议是安全的。

证明 假设任意攻击者 A_{anony} 预计算密钥 W_{UA} , 必须获得私钥 Sk_A 或参数 r_1 。攻击者 A_{anony} 假设参数 r , 使 $r \cdot D_{UA} = r_1 \cdot g \Rightarrow r \cdot r_1 \cdot Pk_A = r_1 \cdot g \Rightarrow r \cdot r_1 \cdot Sk_A \cdot g \Rightarrow r \cdot r_1 \cdot Sk_A = r_1 \bmod q$, 因为 q 是一个素数, 对于所有的 $q \in \mathbb{Z}_q$ 的非 0 元素, 都有一个乘法逆模运算, 因为 r_1 是非 0 元素, 所以 $r \cdot r_1 \cdot Sk_A = r_1 \bmod q \Rightarrow r \cdot Sk_A = 1 \bmod q \Rightarrow r = Sk_A^{-1} \bmod q$, 依据上述推理, 计算如下。

$$\begin{aligned} pr(r \cdot D_{UA} = r \cdot g) &= pr(r \cdot r_1 \cdot Pk_A = r_1 \cdot g) = pr(r \cdot r_1 \cdot Sk_A \cdot g = r_1 \cdot g) = pr \\ (r \cdot r_1 \cdot Sk_A &= r_1 \bmod q) = pr(r \cdot Sk_A = 1 \bmod q) = pr(r = Sk_A^{-1} \bmod q) = \\ 1/q - 2 & \text{ (引理 1 和 } Sk_A^{-1} \neq 0, 1) \end{aligned}$$

对于所有的 $Sk_A^{-1} \in \mathbb{Z}_q^*$, 一个均匀分布的随机数 r 模拟 Sk_A^{-1} 的概率是可以忽略的。

假设 $\|p - 2\| = n, p - 2 = \Theta(2^n)$, 则 $pr(r \cdot D_{UA} = r \cdot g) = 1/p - 2 \leq negl(n)$, $negl(n)$ 表示一个可忽略函数。同理, 攻击者 A_{anony} 成功模拟参数 r_1, t_1, t_2 的概率也是可以忽略的, 所以本文提出的认证与密钥协商协议被成功攻击的概率是可忽略的。证毕。

4.1.1 全认证

在协议实施过程中, 参与协议的三方进行了全认证^[13]。

(1) UA 与 AS_A 的认证: AS_A 用系统私钥 Sk_A 计算 W_{UA} ,

解密 $E_{w_{UA}}[ticket_{UA}]$, UA 认证了 AS_A ; 对 UA 发来的 $ticket_{UA}$ 的解密和回复的 $ticket_{UA}'$ 的加密, 及随机数 N_U 的返还, AS_A 认证 UA。

(2) AS_A 与 AS_B 的认证: AS_A 与 AS_B 之间通过协商密钥 K_{AB} 的加解密和随机数 N_{BS} , 实现了相互认证。

(3) UA 与 AS_B 的认证: 通过 AS_A 回复的确认比特, AS_B 认证了 UA; UA 通过 AS_B 将 $E_{w_{UA}}[ticket_{UA}]$ 传输给 AS_A , 又将 $E_{w_{UA}}[ticket_{UA}']$ 回复给 UA 且 UA 需要验证 N_U , UA 认证了 AS_B 。

4.1.2 抵抗攻击

提出的混合云联合身份认证与密钥协商协议中采用了随机数、抗碰撞散列运算和对称加解密算法等, 可以有效防止篡改数据、伪造用户身份、重放和中间人攻击等。

(1) 篡改数据和伪造用户身份

UA 产生随机数 N_U 并被加密后与消息一起传输给 AS_B , AS_B 产生随机数 N_{SB} 同样被加密后与消息一起传输给 AS_A , AS_A 分别解密 AS_B 和 UA 传来的密文, 并用 w_{UA} 、 K_{AB} 分别加密相应的消息, 返还给 AS_B 和 UA, AS_B 和 UA 不仅要解密消息还需要验证相应随机数。可以看出 UA、 AS_A 和 AS_B 间的消息是以密文方式传输, 攻击者如果想篡改数据或在不知用户口令(私钥)的情况下伪造用户身份, 需要破解多个密钥并获得相应的随机数, 在本文提出的算法中这是难以实现的。

(2) 重放和中间人攻击

消息在传输过程中均采用随机数或加密传输。所以可以有效预防重放和中间人攻击。

综合本节安全性分析的各个方面, 与参考文献[7,9]进行比较, 结果见表 1。

表 1 安全性比较

方案	全认证	预防重放攻击	预防伪造攻击	预防中间人攻击	预防欺骗攻击
参考文献[7]	是	是	是	是	否
参考文献[9]	否	是	是	是	*
本文提出方案	是	是	是	是	是

注: * 表示没有涉及此项内容

4.2 性能

根据计算复杂性理论, 远程身份认证方案的效率主要取决于交互轮数和计算量。而交互轮数是远程认证过程中影响认证方案性能的最主要因素^[14]; 计算量主要包括散列运算、加解密运算、对运算, 其中, 对运算耗时最大, 约占总耗时的 50%。本文提出的方案在实现过程中, 用户 UA 进行 1 次

散列运算、1 次对称加密运算和 1 次双线性对运算; AS_A 进行 1 次散列运算和 2 次对称加密、解密运算; AS_B 进行 1 次散列运算、1 次对称加密、解密运算和 1 次双线性对运算。协议在 UA、 AS_A 和 AS_B 间的通信有 5 次。综合性能分析的各个方面, 与参考文献[7,9]进行比较, 结果见表 2。通过分析表 2 列举的 3 个混合云身份认证方案, 说明本文提出的方案是综合效率最好的。

表 2 性能比较

方案	散列运算	加解密运算	对运算	交互轮数
参考文献[7]	3	4	5	5
参考文献[9]	6	4	5	6
本文提出方案	3	4	2	5

5 结束语

混合云分布广泛、动态性强、部署复杂。基于混合云中末端云间的信任关系和密钥协商机制, 提出混合云联合身份认证和密钥协商协议, 实现了用户身份认证和授权策略等安全信息的分布式管理与动态获取, 避免集中式统一身份管理的认证与存储开销, 提高了认证效率。协议中采用了随机数、抗碰撞散列运算和加解密算法等, 可以有效预防重放、篡改数据、伪造用户身份和中间人攻击等。理论分析表明, 笔者设计的协议在保证混合云安全的基础上, 以较小的计算量和通信开销, 为混合云联合身份认证和密钥协商提供了一种较为实用的认证解决方案。通过在 5 台计算机联合的虚拟实验平台验证证明, 本文提出方案具有良好的可操作性。下一步将对混合云中的多服务器协作进行研究。

参考文献

- 1 周洪波著. 云计算实践指南丛书 云计算: 技术、应用、标准和商业模式. 北京: 电子工业出版社出版, 2010
- 2 Mell P, Grance T. The NIST Definition of Cloud Computing (Draft). National Institute of Standards and Technology (NIST), January 2011
- 3 沈建苗. 2013——混合云之年. http://www.cnw.com.cn/cloudgo2012/htm2013/20130104_262085.shtml, 2012
- 4 Ramgovind S, Eloff M M, Smith E. The management of security in cloud computing. Proceedings of IEEE Conference on Information Security for South Africa, South Africa, 2010
- 5 Hoover J N, Martin R. Demystifying the cloud. InformationWeek Research & Reports, December 2009

(下转第 108 页)



- 17 Small T, Haas Z J. The shared wireless infostation model-a new Ad Hoc networking paradigm (or where there is a whale, there is a way). Proceedings of the 4th ACM Int'l Symp on Mobile Ad Hoc Networking and Computing (MOBIHOC 2003), Annapolis, 2003: 233~244
- 18 Wang Y, Wu H Y. DFT-MSN: the delay fault tolerant mobile sensor network for pervasive information gathering. Proceedings of the IEEE 25th Int'l Conference on Computer Communications (INFOCOM 2006), Barcelona, 2006: 1~12
- 19 Wang Y, Wu H Y, Dang H. Analytic study of delay/fault-tolerant mobile sensor networks (DFT-MSN's). Proceedings of the 10th IEEE Int'l Symp on World of Wireless, Mobile and Multimedia Networks(WoWMom 2009), San Francisco, USA, 2009: 1~9
- 20 Wu H Y, Wang Y, Dang H, *et al.* Analytic, simulation and empirical evaluation of delay/fault-tolerant mobile sensor networks. IEEE Transactions on Wireless Communications, 2007, 6(9): 3287~3296
- 21 Pasztor B, Musolesi M, Mascolo C. Opportunistic mobile sensor data collection with SCAR. Proceedings of the 4th IEEE Int'l Conference on Mobile Ad Hoc and Sensor Systems (MASS 2007), Pisa, Italy, 2007: 1~12
- 22 Song L B, Kotz D F. Evaluating opportunistic routing protocols with large realistic contact traces. Proceedings of the 2nd ACM Workshop on Challenged Networks (CHANTS 2007), Montreal, 2007: 35~42
- 23 Fiore M, Casett C, Chiasserini C F. Efficient retrieval of user

contents in MANETs. Proceedings of 26th Annual IEEE Conference on Computer Communications, IEEE INFOCOM 2007, Anchorage, Alaska, USA, 2007: 10~18

- 24 Opportunistic network environment simulator. <http://www.netlab.tkk.fi/tutkimus/dtn/theone/>

[作者简介]



吴大猛,男,宁波大学硕士生,主要研究方向为延迟容忍网络查询处理。

钱江波,男,博士,宁波大学教授,主要研究方向为数据库、数据流、逻辑电路设计。

陈叶芳,女,宁波大学讲师,主要研究方向为数据流处理。

董一鸿,男,博士,宁波大学教授,主要研究方向为移动数据库、数据挖掘和人工智能。

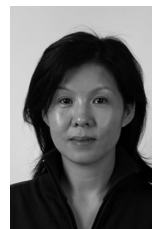
(收稿日期:2013-10-31)

(上接第 99 页)

- 6 Yan L, Rong C, Zhao G. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. Proceedings of the First International Conference on Cloud Computing, Beijing, China, 2009:167~177
- 7 Reede J. On a-select and federated identity management systems. Netherlands: University of Twente, 2007
- 8 Li H, Dai Y, Tian L, *et al.* Identity-based authentication for cloud computing. Lecture Notes in Computer Science, 2009 (5931):167~177
- 9 Zhang Q K, Li Y Z, Song D J, *et al.* Alliance-authentication protocol in clouds computing environment. China Communications, 2012, 9(7): 43~54
- 10 张华,温巧燕,金正平. 可证明安全算法与协议. 北京: 科学出版社, 2012
- 11 彭华熹. 一种基于身份的多信任域认证模型. 计算机学报, 2006, 29(8):1271~1282
- 12 Kata J, Lindell Y. Introduction to modern cryptography. New York: CRC Press, 2007
- 13 罗长远,霍士伟,邢洪智. 普适环境中基于身份的跨域认证方案. 通信学报, 2011, 32(9): 111~117
- 14 汪定,马春光,张启明等. 一种强口令认证方案的攻击和改进.

计算机科学, 2012, 39(6): 72~76

[作者简介]



王崇霞,女,长治学院副教授,主要研究方向为密码学、网络安全、云计算安全。

高美真,女,焦作师范高等专科学校计算机与信息工程学院副教授,主要研究方向为计算机网络与图像处理。

刘倩,女,北京科技大学计算机与通信工程学院博士生,主要研究方向为智能网络及网络安全。

周贤伟,男,博士,北京科技大学计算机与通信工程学院教授、博士生导师,主要研究方向为云计算、智慧网络、空间网络等。

(收稿日期:2013-12-18)