doi:10.3969/j.issn.1000-436x.2012.z2.004

基于 TPM 的云计算平台双向认证方案

刘振鹏[1,2]，吴凤龙[1]，尚开雨[2]，柴文磊[2]，王虓[1]
(1. 河北大学 数学与计算机学院，河北 保定 071002；2. 河北大学 网络中心，河北 保定 071002)

摘 要：为了解决云计算服务环境中用户和云服务器之间的双向认证问题，提出一种基于可信平台模块的云计算平台双向认证方案。将可信计算技术和传统的智能卡口令认证方法相结合应用于云计算服务平台，实现云计算中双方身份的认证，协商生成会话密钥，同时对云服务器的平台可信状况进行了验证。实验分析表明，该方案可以抵抗常见的各种攻击，安全性较高。计算时间复杂度在云计算服务中能够满足要求。
关键词：云计算；身份认证；可信平台模块；双向认证
中图分类号：TP399 **文献标识码**：A **文章编号**：1000-436X(2012)Z2-0020-05

Mutual authentication scheme based on the TPM cloud computing platform

LIU Zhen-peng[1,2], WU Feng-long[1], SHANG Kai-yu[2], CHAI Wen-lei[2], WANG Xiao[1]
(1. College of Mathematics and Computer Science, Hebei University, Baoding 071002, China;
2. Network Center, Hebei University, Baoding 071002, China)

Abstract: A mutual authentication scheme based on the TPM cloud computing platform was proposed to solve the problem of mutual authentication between user and cloud computing server. Trusted computing technology and traditional smart card password method were used in cloud computing service platform. The scheme completed the authentication of both sides in cloud computing, generated the session key according consulting, at the same time, verified the credibility of cloud service platform. Experiment analysis shows that our scheme can resist various kinds of possible attacks, so it is therefore more secure than other schemes. And the computing time meet the requirements of cloud computing environment.
Key words: cloud computing; identity authentication; TPM; mutual authentication

1 引言

云计算作为一种新的概念和技术得到了人们的广泛关注[1]，云计算存在的最大问题是云安全[2]。在云计算模式中，用户的数据和计算被放在云服务提供商的数据中心存储和运行，且多个用户共享数据中心的各种资源。为了保证云系统的安全，必须建立用户和云服务器双方身份的强认证机制[3]。由于可信计算技术在网络安全认证中的特殊优势，在云计算服务平台中引入可信计算技术，建立基于可信技术的云服务平台框架，可以有效解决云计算服务环境中用户和云服务器之间的双向认证问题。本文提出了一种新的智能卡用户和云计算服务平台的双向认证方案，完成双方身份相互认证、协商会话密钥，同时验证云计算服务器平台的可信性。

收稿日期：2012-10-24
基金项目：国家自然科学基金资助项目（60873203）；河北省自然科学基金资助项目（F2010000319）；河北大学自然科学校内基金资助项目
Foundation Items: The National Natural Science Foundation of China (60873203); The Natural Science Foundation of Hebei Province (F2010000319); The Natural Science Foundation of Hebei University

2　基于可信计算技术的云计算服务平台框架

可信计算技术的核心是在终端平台上嵌入可信平台模块（TPM, trusted platform module）。TPM 为各类计算平台提供信任根，为各种可信机制和安全功能提供硬件保障，并为度量和验证平台的可信属性即完整性提供基础[4]。

身份认证是实现云服务平台安全体系的重要机制，是整个安全体系的基础，为云服务平台用户身份的真实性提供安全保证[5]。相对于传统的安全机制，采用 TPM 进行认证具有更强安全性、私密性。TPM 将关键密钥密封在不可侵入的硬件中，且具有唯一性，位于 TPM 密钥管理根部的是存储根密钥，对于一个可信平台模块拥有者只有一个。服务器可以利用硬件架构中的可信平台模块创建公私密钥对实例（PK，SK）。这样的密钥是根存储密钥的衍生密钥，且特定于平台硬件及服务器自身[6]。从系统加电启动到执行环境建立的全过程中，TPM 度量平台硬件和软件组件，对应的散列值等完整性度量信息保存在 TPM 的一组 PCR 寄存器中，同时创建事件并记录在度量存储日志（SML, stored measurement log）中。PCR 值和 SML 值一起用于向远程验证方证明平台的状态。基于 TPM 的云服务平台框架如图 1 所示。

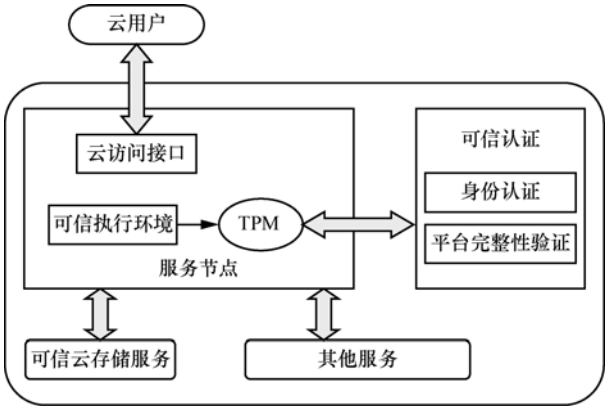


图 1　基于可信计算技术的云计算服务平台

3　可信双向认证方案

本文的方案场景模型如图 2 所示。用户、云服务器（TPM）、CA（certificate authority）在整个互联网络中可以相互访问。首先用户 U 在云服务器 S 所在的平台完成注册，得到智能卡后通过客户端登录，向云服务器提出访问请求。云服务器和用户完成双向可信认证。CA 负责云服务器（TPM）身份和产生公钥的管理，实现对云服务器身份和公钥的绑定。拥有智能卡的用户可以向 CA 提出查询请求，验证所收到公钥和云服务器身份的一致性[7]。

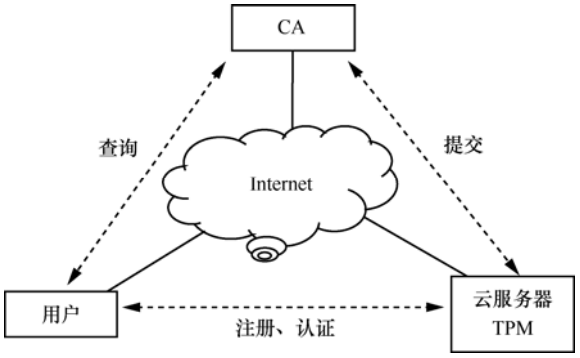


图 2　方案场景模型

用户利用持有的智能卡请求对云服务器的访问，方案实施过程中包括注册、登录验证和口令更改 3 个阶段。假定用户的终端平台是可信的并且在注册阶段用户和云服务提供者的行为都是诚实善意的[8]。文中用到的符号定义如表 1 所示。

表 1　　相关符号定义

符号	含义
S	云计算服务器
U	用户
ID	用户身份
PW	用户口令
$h(\cdot)$	安全单向哈希函数
PK	TPM 产生的公私密钥对中的公钥
SK	TPM 产生的公私密钥对中的私钥
‖	串联操作
⊕	按位异或操作
T	系统时间戳
$\mathrm{Sig}\{\}_{SK}$	私钥签名运算
Log{}	安全度量日志提取
K_{US}	最终会话密钥

3.1　注册

用户首先成为系统的合法用户，注册过程包括用户向云服务器发送注册请求和云服务器签发注册信息给用户，具体步骤如下：① 当用户 U 向云服务器请求注册时，U 选择一个身份 ID、口令 PW 和一个随机数 n，计算 $h(PW\oplus n)$，发送 ID 和 $h(PW\oplus n)$给云服务器 S；② 云服务器 S 收到注册请求消息后，计算 $\mathrm{PID}=h(\mathrm{ID}\,\|\,x)$，$R=\mathrm{PID}\oplus h(PW\oplus n)$。$x$

为云服务器 S 挑选的秘密数，为安全考虑应大于 100bit；选择大素数 P 以及 $g \in GF(P)$；云服务器 S 利用硬件架构中的可信平台模块(TPM)创建公私密钥对(PK, SK)；云服务器 S 将$\{R、P、g、h(\cdot)、PK\}$通过安全信道签发给用户 U 的智能卡；③ 用户 U 将 ID 和 n 输入到智能卡，则智能卡中存有：$\{ID、R、P、g、h(\cdot)、PK、n\}$，此时用户 U 不需要再记忆 n。

3.2 登录验证

用户 U 将智能卡插入终端的读卡器。输入 ID 和 PW。智能卡首先检查 ID 的格式是否有效，如果 ID 无效，则智能卡拒绝 U 的认证请求。若通过执行以下操作。

1) 用户 U 产生一个临时的随机数 r 和一个秘密数 a，计算 $PID=R \oplus h(PW \oplus n)$，$K_U=g^a \bmod P$，$C_1=PID \oplus h(r \oplus n)$，$C_2=h(h(r \oplus n) \oplus T_1)$，其中，$T_1$ 为用户本地时间戳；计算 $H_U=h(ID, C_1, C_2, K_U, T_1)$；发送消息 $M_1=\{ID, C_1, C_2, K_U, T_1, H_U\}$给云服务器 S。

2) 云服务器 S 收到消息 M_1 后，验证时间戳 T_1，检查 $T_1' - T_1 \leqslant \triangle T$ 是否成立，其中，T_1' 为云服务器当前时间戳，$\triangle T$ 为合法的通信延迟。若成立，则计算 $H_U'=h(ID, C_1, C_2, K_U, T_1)$，判断 H_U' 与原值 H_U 是否一致，以验证 U 所发送消息的完整性；若通过，计算 $PID=h(ID \| x)$，$C_1'=PID \oplus C_1$ 以及 $C_2'=h(C_1' \oplus T_1)$；云服务器 S 判断 C_2' 值与接收到的 C_2 值是否相等。若相等，则云服务器 S 确定用户 U 为该系统的合法用户。云服务器 S 挑选秘密数 b，计算 $K_S=g^b \bmod P$。然后利用收到的 K_U 计算双方会话密钥 $K_{US}=(K_U)^b=(g^a)^b \bmod P$；然后 S 利用 TPM 芯片计算云服务器平台完整性校验值 PCR_S，即 $PCR_S=SHA(PCR_0 \| PCR_1 \| \cdots \| PCR_N)$。用私钥 SK 进行签名得到 $C_3=Sig\{C_1', PCR_S\}_{SK}$。加载平台安全度量日志 $L=Log(SML)$，计算 $H_S=h(C_3, K_S, L, T_2)$，其中，T_2 为 S 产生的时间戳。发送消息 $M_2=\{C_3, K_S, L, T_2, H_S\}$给用户 U。

3) 用户 U 收到消息 M_2 后，首先验证时间戳 T_2 的正确性。检查 $T_2' - T_2 \leqslant \triangle T$ 是否成立，T_2' 为用户当前时间戳。若成立，则验证消息是否被篡改即计算 $H_S'=h(C_3, K_S, L, T_2)$与 H_S 是否一致。若通过，利用公钥 PK 解密 C_3 得到 C_1' 值和 PCR_S 值。判断 $h(r \oplus n)$是否与 C_1' 相等，若相等，验证通过，用户 U 确定云服务器 S 身份。随后，用户 U 利用收到的云服务器的 K_S，得到双方会话的密钥：$K_{US}=(K_S)^a \bmod P=(g^b)^a \bmod P$。

4) 用户 U 验证云计算服务平台的完整性，以确保服务器系统配置信息是否符合安全策略，即判断服务器的状态是否可信。利用 L 中的存储值重新计算 $PCR_S' = SHA(PCR_0 \| PCR_1 \| \cdots \| PCR_N)$，验证 PCR_S' 与 PCR_S 是否一致。若一致，云服务器平台完整性获得验证。

云服务器 S 验证了用户 U 的合法身份，同时用户 U 验证了云服务器 S 的合法身份，且确认了云服务器 S 的平台完整性，服务器接受用户的合法接入请求并向其提供服务，交互数据由密钥 K_{US} 加密保护。

3.3 口令更新

将智能卡插入用户终端，输入 ID 和 PW，执行登录阶段和认证阶段完成双向认证后，请求更改口令。输入新口令 PW_{new}，U 的智能卡计算 $R_{new}=R \oplus h(PW \oplus n) \oplus h(PW_{new} \oplus n)$，将生成 $R_{new}=h(ID \| x) \oplus h(PW_{new} \oplus n)$，然后用 R_{new} 替换掉原来的 R 存储在智能卡中。

4 方案分析

4.1 安全性分析

本文方案提供了云计算中用户和云服务提供商之间的双向认证。借助 TPM 所固有的属性实现对云服务器身份和平台的双重认证，能保证方案整体的有效性和强安全性。对抵抗常见攻击和满足其他安全目标情况分析如下。

1) 抗重放攻击：在登录认证阶段，用户 U 向服务器发送的消息包含时间戳 T_1，时间戳的采用可以有效地防范消息重放攻击。

2) 抗拒绝服务攻击：用户需要提供正确的 ID，并通过智能卡的合法性验证后，才可以向云服务器提出访问请求；用户 ID 和智能卡是绑定在一起的，攻击者不能同时得到用户的智能卡和对应的 ID 则不能通过智能卡的验证，也就不能向服务器发起拒绝服务攻击。

3) 抗口令猜测攻击：包括在线口令猜测攻击和离线口令猜测攻击。针对在线口令猜测攻击可以通过限制用户单位时间内的登录次数来阻止；当他人获取用户 U 所丢失的智能卡时，可以获得智能卡中所存储的信息，包括$\{ID、R、P、g、h(\cdot)、PK、n\}$，不能从中获取关于用户口令的信息。另外，$R=h(ID \| x) \oplus h(PW \oplus n)$，因为 $h(ID \| x)$对其他人来讲是机密的，因此无法通过 R 和 n 实行离线口令猜测攻击。

4) 抗伪装攻击：假设攻击者截获了消息 M_1 的全部消息，得到了 C_1 和 C_2 值，通过重放伪装合法用户，但由于攻击者不知道用户 U 的秘密数 a，不

能在后续步骤中与云服务器协商密钥，伪装攻击失败，同样攻击者若伪装服务器企图欺骗请求登录的用户 U，它必须有一个有效的消息 C_3，而 C_3 是私钥 SK 签名的消息，由于非对称密钥的特性，这是不可行的。因为它无法获取系统平台 TPM 产生的私钥值，签名不可伪造。此外攻击者无法得到云服务器的秘密数 b，也不能完成与用户的会话密钥协商，伪装攻击失败。

5) 抗云平台内部人员攻击：既然 U 用 $h(PW\oplus n)$代替 PW 提交给云服务器 S 进行注册，S 的内部人员不能直接得到 PW，此外，n 没有泄露给 S，S 的内部人员也不能通过对 $h(PW\oplus n)$进行离线猜测攻击得到 PW，因此方案能够抵抗内部人员攻击。

6) 提供完备前向安全性：攻击者窃听用户 U 和云服务器 S 之间登录过程和验证过程的情况下，能够获得的消息包括{ID，C_1，C_2，C_3，K_U，K_S，L，T_1，T_2}。其中，从 C_1，C_2，C_3，L 中无法得到有用的信息。因为 $K_U=g^a \bmod P$，$K_S=g^b \bmod P$，$K_{US}=(g^a)^b \bmod P$。攻击者无法从 K_U 和 K_S 得到 U 和 S 的共享密钥 K_{US}。另外，如果攻击者获取到用户 U 口令 PW，因为上述信息与 PW 无关，攻击者也不能获得 U 和 S 以前的共享密钥。

4.2　计算性能分析

方案的计算时间复杂度满足云计算环境的认证需求，计算时间符号定义如表 2 所示。分析可知文中方案总的计算时间复杂性为 $T=13T_h+12T_{xor}+4T_{exp}+T_{sig}+T_{pk}+2T_{PCR}+T_{log}$。其中，注册阶段 $2T_h+2T_{xor}$，登录认证阶段 $9T_h+7T_{xor}+4T_{exp}+T_{sig}+T_{pk}+2T_{PCR}+T_{log}$，口令更新阶段 $2T_h+3T_{xor}$。在对云服务器平台可信性进行验证时，增加的计算时间为 $2T_{PCR}+T_{log}$，其中，PCR 值的生成和验证只需若干次散列运算，且不需要全部的 PCR 的值，可由用户随机抽取一定数量的值完成验证。增加的时间复杂度提供了云服务器平台的可信验证和对方案安全性得到了增强，而时间复杂度在可允许的范围内。

表 2　计算时间符号定义

符号	含义
T_h	执行一次散列运算的时间
T_{xor}	执行一次异或运算的时间
T_{exp}	执行一次指数运算的时间
T_{sig}	执行一次签名加密运算的时间
T_{pk}	执行一次公钥解密运算时间
T_{PCR}	计算平台 PCR 值的时间
T_{log}	平台安全度量日志加载的时间

针对本文所提出的方案用 Microsoft Visual C++ 6.0 结合 SQL Server 2 000 工具在 Windows 操作系统上进行了实验验证。具体的计算机硬件和软件参数为：处理器：Intel(R) Core(TM) 2 E7 500，主频为 2.93GHz，内存为 1.98GB，硬盘空间为 300GB；操作系统为 32 位 Microsoft Windows XP 系统。Microsoft Visual C++ 6.0 应用于前端，SQL Server 2 000 用于后台的数据处理，其中，执行各类操作的数据长度不超过 256bit。表 3 表示了在上述实验环境下，双向认证方案中登录验证阶段各个操作的处理时间。

将本文所提出的方案与近年来提出的几种较为典型的智能卡口令身份认证方案[7,9~11]进行了实验对比，总的操作处理时间对比结果如表 4 和表 5 所示。

表 3　各操作处理时间/ns

操作方式	1	2	3	4	5	6	7	8	平均值
异或操作	1 233	1 189	955	890	8 561	7 516	9 455	8 466	4 783.125
指数操作	455	852	873	4 582	4 686	14 859	45 646	13 774	10 715.875
散列操作	824 553	1 454 260	127 645	57 842	65 542	65 466	—	—	432 551.333
加密操作	1 256 731	5 614 958	874 214	3 558 642	—	—	—	—	2 826 136.25
解密操作	4 245 666	9 427 670	3 595 233	158 579	—	—	—	—	4 356 787

表 4　各个方案操作数量

操作	JUANG 方案[9]	FAN 方案[10]	SANTHOSH 方案[11]	YANG 方案[7]	本文方案
异或操作	1	3	12	12	9
指数操作	4	1	—	15	7
散列操作	5	4	6	4	4
加密操作	3	3	2	1	1
解密操作	3	4	2	1	1

表 5　　总的处理时间

操作	总处理时间/ns
JUANG 方案[9]	23 759 143.04
FAN 方案[10]	27 660 827.332
SANTHOSH 方案[11]	17 018 551.998
YANG 方案[7]	9 131 264.207
本文方案	9 031 187.832

通过分析，本文所提出的方案与其他智能卡口令认证方案相比，能够达到更多的安全目标并且在抵抗常见的安全攻击方面有明显的优势。同时可以看出本文所提出的方案在计算时间复杂度方面也优于其他方案。

5　结束语

将云计算与可信计算技术相结合，设计了基于可信计算技术的云计算服务平台，提出了一种新的智能卡口令认证方案，提供云服务器和用户相互身份认证的同时，验证了云服务器平台的可信性。该方案因为 TPM 的固有特性，与已有方案相比，安全性较高且计算时间复杂度较少，可以为用户提供更安全的服务。

参考文献：

[1] 陈康, 郑纬民. 云计算：系统实例与研究现状[J]. 软件学报, 2009, 20 (5):1337-1348.
CHEN K, ZHENG W M. Cloud computing: system instances and current research[J]. Journal of Software, 2009,20(5):1337-1348.

[2] 罗军舟, 金嘉晖, 宋爱波等. 云计算：体系架构与关键技术[J]. 通信学报, 2011,32(7): 3-21.
LUO J Z, JIN J H, SONG A B, *et al*. Cloud computing: architecture and key technologies[J]. Journal on Communications, 2011, 32(7): 3-21.

[3] 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.
FENG D G, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2011, 22(1):71-83.

[4] 冯登国, 秦宇, 汪丹等. 可信计算技术研究[J]. 计算机研究与发展, 2011, 48(8):1332-1349.
FENG D G, QIN Y, WANG D, *et al*. Research on trusted computing technology[J]. Journal of Computer Research and Development, 2011, 48(8):1332-1349.

[5] Towards trusted cloud computing[EB/OL]. http://www.usenix.org/ events/ hotcloud09/tech/full_papers/santos.pdf, 2009.

[6] 徐贤, 龙宇, 毛贤平. 基于 TPM 的强身份认证协议研究[J]. 计算机工程, 2012, 38(4):23-27.
XU X, LONG Y, MAO X P. Research on TPM based strong ID authentication protocol[J]. Computer Engineering, 2012, 38(4):23-27.

[7] 杨力, 马建峰. 可信的智能卡口令双向认证方案[J]. 电子科技大学学报, 2011, 40 (1):128-133.
YANG L, MA J F. Trusted mutual authentication scheme with smart cards and passwords[J]. Journal of University of Electronic Science and Technology of China, 2011, 40(1):128-133.

[8] CHEN T H, HSIANG H C, SHIH W K. Security enhancement on an improvement on two remote user authentication schemes using smart cards[J]. Future Generation Computer Systems, 2011,27(4):377-380.

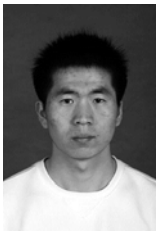
[9] JUANG W S. Efficient password authenticated key agreement using smart card[J]. Computer and Security, 2004,23(2):167-173.

[10] FAN C I, LIN Y H, HSU R H. Remote password authentication scheme with smart cards and biometrics[A]. Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM′06)[C]. San Francisco, CA, USA, 2006.1-5.

[11] SANTHOSH B S, GOKULRAJ K. An enhanced dynamic mutual authentication scheme for smart card based networks[J]. Computer Network and Information Security, 2012, 4(4):30-38.

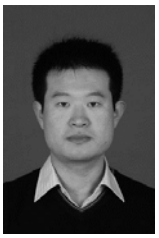
作者简介：

刘振鹏（1966-），男，河北安国人，博士，河北大学教授，主要研究方向为云计算、对等网络和信息安全等。



吴凤龙（1985-），男，河北唐县人，河北大学硕士生，主要研究方向为云计算与信息安全。

尚开雨（1974-），男，河北保定人，河北大学网络中心实验师，主要研究方向为对等网络、Web 服务。



柴文磊（1982-），男，河北高碑店人，河北大学网络中心实验师，主要研究方向为网络环境、Web 服务。

王旎（1986-），男，河北巨鹿人，河北大学硕士生，主要研究方向为云计算与信息安全。