



基于代理的异构云认证方案^{*}

郭继文, 周贤伟

(北京科技大学计算机与通信工程学院 北京 100083)

摘 要: 针对异构云部署复杂、计算量大、频繁信息交互等问题, 提出了认证代理和服务代理两种异构云服务模式, 设计了异构云中具有较低握手次数的代理签名方案, 从而提高了认证执行效率。此外, 该方案能够有效防止恶意节点的重放攻击、伪造攻击和中间人攻击等。

关键词: 异构云; 认证协议; 代理

doi: 10.3969/j.issn.1000-0801.2013.03.015

Authentication Scheme Based on Agents for Heterogeneous Cloud

Guo Jiwen, Zhou Xianwei

(School of Computer and Communication Engineering, University of Science and Technology
Beijing (USTB), Beijing 100083, China)

Abstract: Considering the complexity of deploying network nodes, large amount of calculation and frequent mutual messages for heterogeneous cloud, two service patterns, i.e. authentication agent and service agent were proposed. Also, the proxy digital signature schemes with lower handshaking numbers were devised and the efficiency of authentication implementation was improved. In addition, the scheme can effectively guard against the replay attack, the impersonation attack and the man-in-the-middle attack of the malicious nodes, and so on.

Key words: heterogeneous cloud, authentication protocol, agent

1 引言

随着互联网技术的不断发展, 云计算技术已经逐渐成为未来网络的一个重要分支, 并为下一代网络的发展提供了以服务对象面向 IT 业的发展模式。与此同时, 虚拟化技术使得云平台的虚拟层、管理层和应用层都存在安全威胁^[1]。这严重影响了云计算技术的实用化。为了防止非法用户接入云计算平台获得服务资源, 认证机制可以从应用层、管理层、虚拟层 3 个方面, 保证云计算平台的正常运行。

根据云计算平台的不同应用模式, 认证策略主要包括 3 种类型: 密钥交互认证协议^[2,3]、信任行为监控机制^[4,5]和生物特征识别^[6]。上述这些方案都可应用于私有云或公共云, 从而防止云平台中恶意节点的伪造、假冒、恶意行为等攻击。随着云计算技术对国民经济影响的逐步加深, 支持数据共享的混合云^[7]成为可能。因此, 异构云的安全接入技术将成为影响云计算技术发展的重要因素之一。针对多个云平台共存的特性, 参考文献[8, 9]提出相应的异构认证方案。然而异构云部署复杂、计算量大、信息交互频繁等问题, 使得上述认证机制存在设计复杂、执行效

^{*} 国家“863”计划基金资助项目(No. 2012AA121604), 国家自然科学基金资助项目(No. 61170014)

针对上述问题,本文提出认证代理和服务代理两种异构云服务模式,设计了具有较低握手次数的代理签名方案,从而提高了认证执行效率。此外,该方案利用随机数能够有效防止恶意节点的重放攻击、伪造攻击和中间人攻击等。

无论是私有云还是公共云, 它们的组成元素都包括: 用户(user)、提供者(provider)和服务器(server)。为了提高认证效率, 每个云平台增加一个代理模块, 即云平台管理中心通过虚拟化技术共享提供者和服务器的密钥材料, 为身份识别提供基础条件。资源管理、调度等功能仍然由提供者统一管理。假设云平台管理中心是绝对安全且该模块由它负责执行。

- 如果该客户端是通过无线接入云平台,那么该用户可能在移动过程中需要获得异地云平台即时服务资源;
- 如果本地云端无法满足该用户的服务需求,那么它将通过本地云平台管理中心经过远程接入方式获得异地云平台的服务资源。

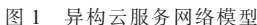
图 1(a)表示客户端在本地注册自己的客户信息并获取了密钥材料。当它移动到异地时,该节点想获得即时异地云服务。该用户的认证过程主要由异地云平台管理中心

3 认证流程

3.1 认证代理的异地接入控制

(1) 客户端 U_j 发送一数据报 ($Requeset, ID_j, EA_i, r_j, h(ID_j || EA_i || r_j)$) 给异地云中心 EA_i ; 设异地云中心获得的公/私钥对为 (e_E, d_E) , 产生伪随机数 r_E , 并发送数据报 $P(e_E, ID_j || EA_i || LA_i || r_E)$ 给本地云中心 LA_i 。

(2) 当 LA_i 收到该消息后,解密并验证这个消息的合法性;若该消息是合法的, LA_i 产生一伪随机数 r_{Li} ,并发送数据报 $(Cert_{t_j}, r_j, r_{Li}, e_j, P(e_{Ei}, r_{Ei}), Sign_{t_j}(r_j, r_{Li}, r_{Ei}, e_j, ID_j, EA_i))$ 给 EA_{i0} .



(3) 当 EA_i 收到上述消息后, 验证该消息的合法性; 如果该消息是合法的, EA_i 发送数据报 $P(e_j, ID_j || EA_i || LA_j || r_j || r_E)$ 给 U_j 。

(4) 当 U_j 收到上述消息后, 验证并解密该消息; 如果该消息能正常解密, U_j 发送数据报 $(Cert_j, r_j, Sign_{r_j}(r_j, r_E, ID_j, EA_i))$ 给 EA_i 。

(5) 当 EA_i 收到该消息后, 验证该消息的合法性; 如果验证通过, EA_i 同意该用户接入异地云平台, 否则拒绝该用户的服务请求。

(6) 当 EA_i 需要对 U_j 进行重新认证时, 首先 EA_i 发送数据报 $(ID_j, EA_i, h(r_j || r_E))$ 给 U_j ; 当 U_j 收到该消息后, 验证这个数据报的散列值是否正确; 若散列值正确, 该客户端将发送消息报 $(Cert_j, r_j, Sign_{r_E}(r_j, r_E, ID_j, EA_i))$ 给 EA_i 。

(7) 当 EA_i 收到该消息后, 验证它的合法性; 如果该消息是合法有效的, 允许该用户继续接入异地云平台, 否则拒绝该用户的服务请求。

3.2 服务代理的本地接入控制

服务代理的本地安全接入是在本地执行认证过程, 但服务云端却被部署在异地。该方案采用本地云中心与异地云中心相互认证的策略, 可以降低云平台密钥材料交互的通信负荷和操作复杂度。那么服务代理的本地安全认证方案步骤如下。

(1) 客户端 U_j 产生一伪随机数 r_j , 并发送数据报 $(Cert_j, LA_i, P(e_{L_i}, r_j), Sign_{r_j}(r_j, LA_i, ID_j))$ 给本地云中心 LA_i ; 设本地云中心的公/私钥对为 (e_{L_i}, d_{L_i}) , 当它收到该消息后, 验证其合法性; 若该消息是合法的, LA_i 产生一伪随机数 r_{L_i} , 并发送数据报 $(Cert_i, LA_i, EA_i, P(e_{E_i}, r_j || r_{L_i}), Sign_{r_{L_i}}(r_{L_i}, r_j, LA_i, ID_j))$ 给异地云中心。

(2) 当 EA_i 收到上述消息后, 解密并验证该消息的合法性; 如果该消息是合法的, EA_i 产生一伪随机数 r_E , 并发送数据报 $(Cert_i, P(e_{L_i}, r_E), Sign_{r_E}(r_j, r_{L_i}, r_E, ID_j, EA_i, LA_i))$ 给 LA_i 。

(3) 当 LA_i 收到上述消息后, 验证该消息的合法性; 如果该消息是合法的, 则 LA_i 发送数据报 $(Cert_j, P(e_j, r_E || r_{L_i}), Sign_{r_E}(r_j, r_{L_i}, r_E, ID_j, LA_i, EA_i))$ 给 U_j 。

(4) 当 U_j 收到该消息后, 验证该消息是否合法; 如果验证通过, LA_i 同意该用户接入云平台, 否则拒绝该用户的服务请求。

(5) 当 LA_i 需要对 U_j 进行重新认证时, 首先 LA_i 发送

数据报 $(ID_j, LA_i, h(LA_i || r_j || r_{L_i} || r_E))$ 给 U_j ; 当它收到该消息之后, 验证数据报的散列值是否正确; 如果散列值是正确的, 那么该客户端将发送消息报 $(Cert_j, r_j, Sign_{r_E || r_{L_i}}(r_j, r_{L_i}, r_E, ID_j, LA_i))$ 给 LA_i 。

(6) 当 LA_i 收到该消息之后, 验证其合法性; 若这个消息报是合法的, 那么允许它接入本地云平台, 否则拒绝该用户的服务请求。

4 安全分析与验证

认证代理的异地安全接入和服务代理的本地安全接入都通过数字签名、散列函数和公钥加密算法来实现。为了保证认证消息在传送过程中的机密性, 认证交互的消息受到严格的加密保障。每个认证消息都增加了伪随机序列, 它能够有效防止重放攻击、伪造攻击。由于云平台中大容量计算和存储工作都在云端执行, 云端只需要为云平台中心提供工作条件, 而云平台中心为云端提供计算或存储任务。如果客户端的任务量较大时, 云端可以进行脱机工作。因此, 简单的重复认证既有利于云平台的安全运行, 又保证了云平台的服务效率。本方案实现了异构云的双向认证, 即云平台中心与客户端之间的相互身份识别。本节将以认证代理的异地接入控制为例说明基于代理的认证方案是正确、安全的。

客户端 U_j 首先将自己的身份识别码 ID_j 和伪随机数 r_j 发送给异地云中心 EA_i , 尽管 EA_i 收到的伪随机数存在泄露的可能, 但散列函数保证了发送消息的不可修改性。这样保证了数据报信息的真实性, 即保证了 EA_i 收到的认证请求消息确实来自 U_j 。

EA_i 转发认证请求消息给本地云中心 LA_i 。该消息报通过 LA_i 的公钥进行加密, 且这个数据报包括伪随机数 r_E 。由于 r_E 是私密的, 该过程能防止恶意节点伪造和中间人攻击。当 LA_i 返还数据报时, EA_i 可以通过检测 r_E 来验证上述数据报是否被 LA_i 接收以及 EA_i 收到的消息是否来自对应的 LA_i , 同时加密机制能防止恶意节点窃听该数据报中的关键信息。

当 LA_i 收到消息之后, 首先需要进行解密, 如果解密不成功, 它将拒绝执行认证过程。随后, LA_i 发送带有数字签名的数据报给 EA_i 。此外, 客户端产生的伪随机数 r_j 被返回, 且客户端的注册公钥 e_j 也发送给 EA_i , 同时加密机制保证了私密 r_E 没有被泄露。

当 EA_i 收到该消息报之后, 验证该消息报的合法性, 包括: 该消息报是否被修改 (伪随机数 r_{L_i} 及签名机制可以



保证数据完整性);该消息报是否来自对应的 LA_i (伪随机 r_E 和 r_j 能够验证消息源的合法性)。与此同时, EA_i 也获得了 U_j 的公钥信息。那么该过程能够有效防止恶意节点的数据篡改、假冒身份和中间人攻击等。

随后, EA_i 与 U_j 通过信息交互来完成相互认证。首先 EA_i 发送加密信息给 U_j , 加密算法保证了消息的机密性。而伪随机数 r_j 和 r_E 能有效防止恶意节点假冒 EA_i 和 U_j 的身份, 即中间人攻击。如果 U_j 能解密成功, U_j 实现对 EA_i 的身份识别。 U_j 发送带有数字签名的数据报给 EA_i 。同理, EA_i 通过伪随机数 r_E 来验证数据报来源的合法性以及签名机制保证了数据完整性。如果通过验证, EA_i 将允许 U_j 接入云平台获得服务资源, 因此该过程能有效防止恶意节点的数据伪造、身份假冒和中间人攻击等。 EA_i 与 U_j 重新认证的安全性分析类似于它们第一次相互身份识别的分析过程。因此基于认证代理的异地接入控制机制是正确、安全的。同理, 基于服务代理的本地接入控制机制也是正确、安全的。基于代理的异构云认证方案的安全性效率对比见表 1。

表 1 安全性与效率对比

方案	是否能 够防止 重放 攻击	是否能 够防止 伪造身 份攻击	是否能 够防止 欺骗 攻击	是否能 够防止 中间人 攻击	握手 次数 (次)
参考文献[7]方案	是	否	否	是	6
参考文献[8]方案	是	否	是	是	6
参考文献[9]方案	是	是	是	否	8
本文方案	是	是	是	是	5

表 1 给出了本方案与其他 3 个认证方案在安全性和执行效率的对比。从安全性上看, 本方案能够防止重放、伪造身份、欺骗以及中间人攻击, 而参考文献[7~9]中的认证方案并不能完全防止上述的安全威胁。从认证效率方面, 本方案能够通过较少的认证次数实现客户端的身份识别, 优于其他 3 个方案。

5 结束语

针对异构云部署复杂、计算量大、信息交互频繁等问题, 本文提出基于代理的异构云认证方案, 实现了异构云中的具有较低握手次数的代理签名方案, 从而提高了认证执行效率。此外, 该方案利用伪随机数能够有效防止恶意节点的重放攻击、伪造身份攻击和中间人攻击等。如果某个客户端需要多个云平台共同支持, 那么多云平台中心的

接入控制机制是下一步的研究重点。

参考文献

- 1 Khan A N, Kiah M L M, Khan S U, *et al.* Towards secure mobile cloud computing: a survey. *Future Generation Computer Systems*, 2012, 25(8): 1~22
- 2 Singh M, Singh S. Design and implementation of multi-tier authentication scheme in cloud. *International Journal of Computer Science Issues*, 2012, 9(5): 181~187
- 3 Yassin A A, Jin H, Ibrahim A, *et al.* Efficient password-based two factors authentication in cloud computing. *International Journal of Security and Its Applications*, 2012, 6(2): 143~148
- 4 田立勤, 林闯. 基于双滑动窗口的用户行为信任评估机制. *清华大学学报(自然科学版)*, 2010, 50(5): 763~767
- 5 刘宴兵, 刘飞飞. 基于云计算的智能手机社交认证系统. *通信学报*, 2012, 33(Z1): 28~34
- 6 Senk C, Dotzler F. Biometric authentication as a service for enterprise identity management deployment. *Proceedings of International Conference on Availability, Reliability and Security*, Regensburg, Germany, 2011: 43~50
- 7 Zhang Q, Li Y, Song D, *et al.* Alliance-authentication protocol in clouds computing environment. *China Communications*, 2012, 9(7): 42~54
- 8 Zhang Q, Zheng J, Tan Y, *et al.* Cross-domain authentication alliance protocol based on isomorphic groups. *Journal of Computers*, 2011, 6(4): 650~656
- 9 Kim J, Hong S. A consolidated authentication model in cloud computing environments. *International Journal of Multimedia and Ubiquitous Engineering*, 2012, 7(3): 151~160

[作者简介]



郭继文, 男, 北京科技大学计算机与通信工程学院博士研究生, 主要研究方向为云计算安全与信息安全技术。



周贤伟, 男, 博士, 北京科技大学计算机与通信工程学院教授、副院长, 主要研究方向为云计算、智慧网络、空间网络、无线网络及信息安全技术。

(收稿日期: 2013-01-12)