基于移动 agent 的云计算身份认证机制研究*

杨娜娜，王　杨，陈付龙，黄亚坤，邓　琨
（安徽师范大学 数学与计算机科学学院，安徽 芜湖 241000）

摘　要：针对当前云计算的安全需求，提出了一种适用于云计算环境下的身份认证方案。首先设计出适用于云计算身份认证场景的移动 agent（mobile agent）结构模型，然后给出了基于 mobile agent 的云计算安全认证策略。该方案引入了可信第三方机构对认证 agent 建立定量信任评估，每次进行认证前通过信任度的判断对认证过程进行控制；在认证完成后，又进一步引入了信任反馈评价机制。理论分析和原型系统的实现表明，提出的云计算认证方案具有一定的可行性和可用性。

关键词：移动 agent；云计算；认证机制；信任
中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1001-3695(2012)10-3812-03
doi:10.3969/j.issn.1001-3695.2012.10.054

Research on cloud computing security authentication mechanism based on mobile agent

YANG Na-na, WANG Yang, CHEN Fu-long, HUANG Ya-kun, DENG Kun
(*College of Mathematics & Computer, Anhui Normal University, Wuhu Anhui* 241000, *China*)

Abstract: Aiming at the current cloud computing security requirements, this paper proposed a novel cloud authentication scheme. Firstly, it designed a structural model of mobile agent and the certification process oriented to cloud computing environment. The authentication scheme introduced a trusted third party which was used to computing agent trust degree by trust evaluation mechanism. Trust value would be used to control every user agent for authentication of the certification. The agent who met the appropriate conditions would increase the trust value and the authenticator who had done incorrect or malicious behavior would reduce the trust value of the agent. Certification processor analysis and implemented prototype show that presented schema can increase the security service level of cloud computing.

Key words: mobile agent; cloud computing; authentication mechanism; trust

云计算是将大量网络计算资源、存储资源与软件资源统一调度以构成一个计算资源池向用户提供按需服务的 IT 服务模式。云计算的推广应用面临着诸多挑战，其中云计算安全问题中的云端用户的身份认证是需要解决的关键技术之一[1]。云计算环境具有资源集中、用户海量、有偿服务等特点，这些要求云计算中心：a）支持用户身份的鉴别、注销以及身份认证机制；b）实现身份联合和单点登录功能；c）提供生命周期各个阶段的安全性管理能力。网络环境下的身份认证技术主要有口令认证、挑战—响应身份认证、零知识身份认证、量子身份认证、混沌理论身份认证和生物特性身份认证技术等[1~4]，但以上技术存在的问题之一是缺少智能性，难以适应具有动态自适应需求的云计算认证场景。

由于智能 agent 具有自主性、推理性和移动性等优点，文献[4]设计并实现了一种基于 agent 的统一身份认证平台；文献[5]提出了融合 grid 和移动 agent 平台的安全认证服务框架；文献[6]提出了应用移动代理的双重 grid 认证机制。这些研究表明智能 agent 与云计算融合的可行性。在分析综合上述相关研究的基础上，结合目前云计算身份认证解决方案的不足，本文提出了一种基于移动 agent 的云计算认证解决方案。

1　基于移动 agent 的云计算认证模型

移动 agent 是一个能在异构网络中自主地从一台主机迁移到另一台主机，并可与其他 agent 或资源交互的程序。这里主要利用移动 agent 实现云端用户主机和云计算中心主机之间的安全认证过程。

1.1　移动 agent 结构模型

本文中的移动 agent 主要分为三类：认证 agent、条件状态控制状态 agent、协商 agent。认证 agent 具有环境交互、安全监控、任务求解、路由、信息汇聚等功能。条件状态集控制 agent 来保证 agent 行为和性能。本文认证方案中的移动 agent 结构如图 1 所示。移动 agent 主要具有创建、就绪、传输、运行、阻塞、退出六个基本状态。图 2 表示移动 agent 的状态转换图。创建状态表示移动 agent 处于创建过程，当创建者将移动 agent 放入发送队列后则进入就绪态。根据自己的路由策略等的发送过程称之为传输态。成功到达目的站点而没有获得执行权

收稿日期：2012-03-19；**修回日期**：2012-04-26　**基金项目**：中国博士后基金资助项目（20100480701）；国家教育部人文社科青年基金资助项目（11YJC880119）；安徽师范大学大学生创新性实验资助项目（AHNUSC46）

作者简介：杨娜娜（1987-），女，山东无棣人，硕士研究生，CCF 会员，主要研究方向为云计算与数据挖掘（nanayang88629@sina.com）；王杨（1971-），男，安徽灵璧人，硕导，博士，主要研究方向为云计算、网络安全与数据挖掘；陈付龙（1978-），男，安徽霍邱人，硕导，博士，主要研究方向为嵌入式计算和普适计算、信息物理系统.

前是就绪态。就绪态时,服务设施能够对其进行身份确认和完整性检查,检查通过则转入执行态。执行态是移动 agent 完成预定义的操作。任务完成后,它可能会继续移动转入传输态,或转入结束态。在执行态,如果所需资源不足等情况就转入阻塞态。结束态是 agent 生命周期的结束。协商 agent 主要是云端用户的认证请求 agent,具有离线认证能力。

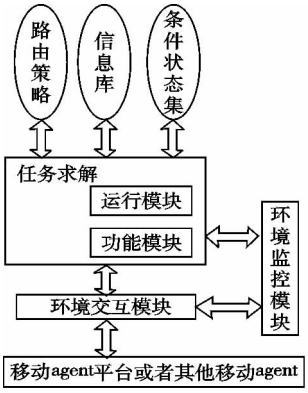

图1　移动agent模型

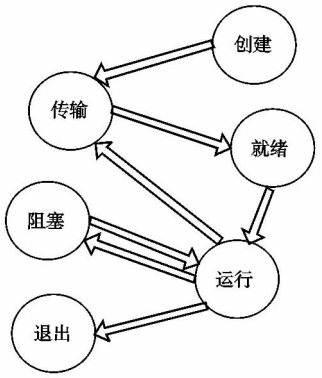

图2　移动agent的状态转换图

1.2　基于移动 agent 的云计算认证模型

基于移动 agent 的云计算认证模型需要考虑以下两个基本问题:

a)兼容性问题。在保持现有的各自治域的认证体系不变的前提下,当用户访问云计算环境中资源时需要进行的动态身份认证。

b)单点登录问题。单点登录需要实现不同自治域的相互证书识别问题,以实现统一的身份认证。本认证模型中采用 GT4 中的 grid security infrastructure 机制,以实现云认证基础设施的可扩展性和单点登录问题。

基于如上考虑,本文建立云计算认证系统模型如图 3 所示。整个认证系统模型按照功能可以自下而上划分为三个层次:云认证基础设施、虚拟组织认证系统层、认证服务应用层。

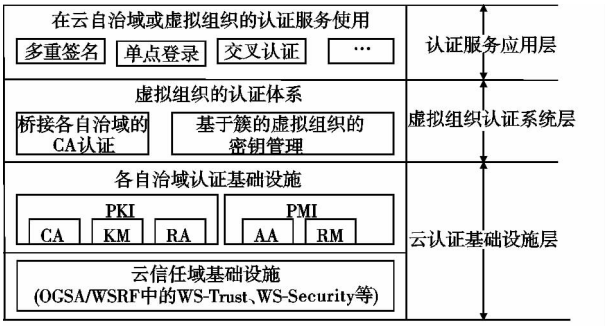

图3　云计算环境下的身份认证分层模型

认证基础设施包括云信任域基础设施和各自治域认证基础设施。云信任域基础设施包括现有的云计算安全服务中的有关认证规范,如 GSI 中的证书链和 WS-Security 中的 WS-Trust 等。这些认证服务是针对云计算环境而规定的,对上层认证体系的建立具有指导性的作用。各自治域认证基础设施层为各自治域根据云计算环境的特点和自身环境的认证需求所制定的本域认证系统,如采用网状、层状和列表状的 PKI 模型等。但是它们一般都包括公钥基础设施(PKI)和授权管理基础设施(PMI)两个部分。云认证基础设施主要是为上层虚拟组织的认证系统建立和认证应用提供基础平台。虚拟组织认证系统层主要是建立虚拟组织间的认证机制。由于云计算主要的运行环境是虚拟组织,因而该层是云计算认证系统的重点。针对自治域的认证模型可以有上面所提供的两种方案,即桥接 CA 和基于簇的虚拟组织的密钥管理。认证服务应用层使用多种认证技术系统来提供不同的认证服务,如多重签名、委托代理、单点登录和交叉认证等[7]。

1.3　基于移动 agent 云计算认证方案

根据图 3,下面提出一种应用移动 agent 技术的云计算安全认证方案。云计算认证过程放到第三方认证平台中,同时采用 RSA、DES 加密技术和 TLS 安全传输通道等技术[7],保证移动 agent 的移动过程中的安全性。图 4 是基于移动代理的云计算安全认证基本认证场景。假设存在一个安全的第三方认证机构 C,它负责存储、查询参与节点的信任度;颁发给 agent 数字证书等功能。User 是请求云计算服务的代理,server 是提供服务的代理。User、server、C 中有各自的协商 agent、管理 agent 和查询 agent 等。协商 agent 用来携带相关信息进行认证,管理 agent 用来对平台进行管理,查询 agent 用来查询信任度、身份信息等。各个 agent 之间进行通信时利用 RSA 或 DES 加密产生的会话密钥,agent 之间的通信数据利用会话密钥进行加密。当 agent 需要进行转移时,利用 RSA 等加密算法和 TLS 协议进行传递。

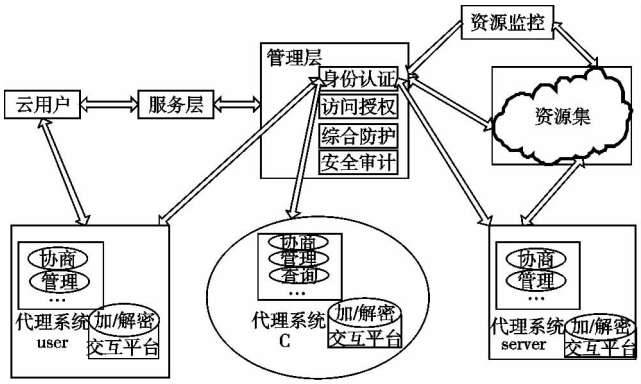

图4　基于移动agent的云计算认证场景

认证时通过 user 的协商 agent 与 C 的协商 agent 协商,查询信任度。满足条件,再将索求信息由 C 的协商 agent 传递给 server,经过 server 的协商同意后,再由 user 的协商 agent 将所需要的服务传达给 C,在确定无误后,user 和 server 之间便可通信。Server 产生子 agent 经 C 颁发数字证书(证书符合国际 X.509 v3标准)传给 A,而后 user 上的子 agent 和 server 上的 agent便可进行信息的交换。降低移动 agent 在移动过程中被网络黑客劫取、窃听的风险,从而保证移动 agent 的安全性。

2　基于移动 agent 的云计算认证协议

2.1　协议描述

为了更好地描述基于移动 agent 的云计算认证协议,首先给出相关符号和定义。

表 1　相关符号及意义

符号	意义	符号	意义
U	用户	TS	时间戳
S	服务端	Δt	预期的传输时间延时
C	第三方	$x0$	注册节点与登录节点的共享密钥,在部署这些节点前已设置
ID	用户账号	$h(\ )$	单项 hash 函数
pw	用户密码	CL	信任度
K	验证码		

定义 1　Agent 是一个实体对象,采用五元组形式描述:

agent = (agentID, act, destination, information, resource)

其中:agentID = {userNegtizteAgent, CManageAgent, agentID3, agentID4, …};act = {create, migrate, transfer, authenticate, manage, …};destination = {destination1, destination2, destination3, …};information = {information1, information2, information3, …}, resource = {resource1, resource2, …}。

提出的认证协议主要由以下六个步骤组成:

a)User 向 server 请求提供服务时,user 代理系统就会自动地根据用户的请求创建协商 agent(negotiate agent)NA_U〈UNA, {create, migrate, transfer}, C, {ID, pw, K, CL}, null〉,NA_U 移动到第三方认证机构 C,与其管理 agent(manage agent) MA_C〈CMA, manage, C, null, null〉和查询 agent (inquiry agent) IA_C〈CIA, inquiry, C, null, null〉进行交互。MA_C 授权 IA_C 到客户数据管理中查询{ID *,pw *,K *,}和其信任度 CL,MA_C 根据查询信息进行初步判断是否满足信任需求,而后反馈给 NA_U〈UNA, {create, migrate, transfer}, U, {ID, pw, K, CL}, resource1〉。若满足,则可以继续进行;如果不满足条件或访问超时则认证失败。信任度的计算方法采用文献[7]的方法。

b)若满足服务,则 MA_C 创建 NA_C〈CAN, {create, migrate, transfer}, server, {ID, pw, K, CL}, null〉,与其管理agent MA_S〈SMA, manage, server, null, null〉进行交互。MA_S 创建协商 agent NA_S〈SNA, {create, migrate, transfer}, C, {ID, pw CL}, {ID *, pw *, CL}〉。参照步骤 a),MA_S 根据 user 的信任度及相关信息,进行判断作出是否提供服务的决定。

c)Use 代理系统的管理 agent MA_U 根据 NA_U 反馈回来的信息,作出具体的服务请求,并放到 NA_U〈UNA, {create, migrate, transfer}, C, {ID, pw, K, CL, information1}, resource1〉。

d)User 与 server 协商结束之后,MA_C 建立安全通道,NA_U提交具体服务描述请求,NA_S〈SNA, {create, migrate, transfer}, S, {ID, pw, CL, information1}, {ID *, pw *, CL}〉,MA_S 跟据具体服务请求,调用相关云服务访问授权策略,准备为 user 提供服务。

e)NA_S〈SNA, {create, migrate, transfer}, C, {ID, pw, CL, information1}, {ID *, pw *, CL, resource1}〉给 NA_U 提供具体的授权信息。获得授权信息后,NA_U 返回,通过 MA_U 将最终的授权信息返回给 user 上的用户,用户以后就可以直接带着这个授权信息获得 server 为其提供的对应服务。

f)Server 根据 user 的需求对在 server 平台上的 MA r_b,产生子 agent sub_b 并传送到第三方认证机构 C,经过 C 传输到平台 user。User 上的子 agent sub_b,可通过网络与 server 上的 agent r_b 进行信息交互。

如果认证的某方发生不正确或恶意的行为,则降低其信任度,或将其加入黑名单中,禁止其以后的访问。设信任度的范围为 0 ~ M,允许认证的最低信任度为 N,0 < N < M。如果认证成功率(认证成功率 = 认证成功次数/总认证次数)达到一定值,便将信任度增加 a,如果发生了不正确的行为,则将信任度减去 b,如果发生恶意行为则将信任度值降低到 N 下;如果信任度低于 N 则不能再对所要求的平台提出服务请求。

2.2 协议性能分析

本文提出的认证机制将认证的过程放到 C 这样一个完全可信的安全平台上,确保了认证中心的独立性与安全性;在认证机制中加入了信任度这一概念,每次认证的双方都会事先判断另外一方的信任状况,信任度太低的就拒绝服务,这样降低了认证的盲目性;认证机制采用了 RSA 加密算法,该算法利用大数分解的困难,保证加密信息的安全性;应用移动 agent 迁移到资源地,进行本地交互,降低了网络负载提高了认证的效率。因此,此机制相比于传统的双方相互认证机制不仅能够符合人们对云安全的需求,也具有认证的灵活性。

3 基于移动 agent 的云计算认证系统的实现

移动 agent 的设计与开发通常采用 IBM 公司的 Aglet 平台,开发工具选取 Java[9]。本文采用的 mobile agent 开发平台是 IBM Aglet WorkBench,集成开发工具为 Eclipse,服务器操作系统为 Linux,中心 Web 服务器采用 Tomcat,数据库采用 Oracle。云计算中心的 master Aglet 把任务委派给各云端用户的 slave agent,slave agent 移动到云服务代理平台实现获取服务后返回结果。

首先是云计算中心的 agent 根据 user agent 需求生成访问参数传递给 AgletRequestDispatch 类,根据请求的服务类别产生 RequestRecord 实例,提交给 RequestManager 类,RequestManager 维护一个服务请求列表 RequestList,RequestManager 根据服务请求列表生产移动的服务访问 agent,把它们派遣到目认证中心主机,根据信任值等判断认证是否成功。若成功就把 RequestRecord 中的状态设置成 success,最后通过服务处理 handleMessage(),根据不同类的服务输出不同的内容,并接收返回的消息。由云计算中心的 agent 接收 user 认证请求,并完成认证判断过程,其关键代码段如下:

```
AgletProxy authentication;
Connectionconn = CommonMethods. DBConnection( );
Statement authid = conn. createStatement( );
String sql = "select * form ip_address";
ResultSet rsl = authid. executeQuery( sql);
while( rsl. next( ) ) {
  fd = "atp://" + rsl. getString( "computer" );
  msg. setArg( "fdest",fdest);
  URL authentication Url = new URL( fd);
  /* 调用 AgletContext 方法,获得与各个主机地址相对应的主机的上下文,派出协商认证 aglet,并获得相应的句柄 */
  authentication = client. getAgletContext( authenticationUrl);
  authentication sendMessage( msg);
  }
```

4 结束语

本文根据当前云计算的安全需求,提出了一种基于移动 agent 的云计算安全认证方案。借助移动 agent 的灵活性和第三方认证机构,以及 agent 信任度库,提高了云计算认证的敏捷性和可靠性。该认证策略利用已有的 aglet 开发平台实现了认证过程的协商与撤消,增强了云计算服务系统的智能性和自适应能力。但是提出的方案在应对云端用户的合谋、free rider 行为等方面缺少一定的防范措施。对于这一问题,本文主要考虑引入隐私保护和激励机制加以解决。

(下转第 3837 页)

(上接第 3814 页)

参考文献:

[1] 冯登国,张敏. 云计算安全研究[J]. 软件学报, 2011,22(1):71-83.

[2] 成谢锋,马勇,刘陈,等. 心音身份识别技术的研究[J]. 中国科学:信息科学,2012,42(2):237-251.

[3] 罗长远,霍士伟. 普适环境中基于身份的跨域认证方案[J]. 通信学报,2011,32(9):111-115.

[4] 孙超,陈钢. 基于 agent 技术的统一身份认证系统[J]. 计算机应用研究,2005,22(3):138-140.

[5] AVERSA R,Di MARTINO B, RAK M,*et al*. Cloud agency:a mobile agent based cloud system[C]//Proc of International Conference on Complex, Intelligent and Software Intensive Systems. 2010:132-137.

[6] WANG Hai-yan,WANG Ru-chuan. Two-step mobile agent based authentication architecture: towards effective grid authencation [J]. Trans of Nanjing University of Aeronautics and Astronautics, 2008,25(1):61-66.

[7] WANG Yang,WANG Ru-chuan,HAN Zhi-jie. Dynamical trust construction schema with fuzzy decision in P2P network[J]. Chinese Journal of Electronics,2009,18(3):417-421.

[8] YANG Li. Application research of digital gas fields production management information system based on mobile agent[J]. Application Research of Computers,2006,23(7):172-175.