文章编号:1007-5321(2014)05-0085-06 **DOI**:10.13190/j.jbupt.2014.05.018

IaaS 云虚拟机 eID 可信验证系统

吴 旭[1,2], 许 晋[1,2], 李春文[3], 刘川意[1,2]

(1. 北京邮电大学 计算机学院, 北京 100876; 2. 北京邮电大学 可信分布式计算与服务教育部重点实验室, 北京 100876;
3. 中国农业银行总行 软件开发中心, 北京 100073)

摘要: 为了解决云计算模式下数据与计算迁移造成的用户与云之间的互可信问题,从硬件平台、用户身份和用户行为多个维度,研究并设计了 IaaS 云虚拟机(eID)可信验证系统. 硬件平台采用可信第三方架构,采用全国唯一的公民网络电子身份 eID 标识用户身份,建立诚信记录,评估用户行为. 通过用户身份可信性验证、虚拟机可信性验证等 4 个阶段,有效解决了用户与云之间的互可信问题. 实验结果表明,该系统可抵御常见攻击方式,安全性高,且其计算时间复杂度在可接受范围内.

关 键 词: 可信计算; 云计算; 基础设施云; 网络电子身份证; 远程验证

中图分类号: TP309.1 **文献标志码**: A

Research on eID-Based Virtual Machine Trusted Attestation System in IaaS Cloud

WU Xu[1,2], XU Jin[1,2], LI Chun-wen[3], LIU Chuan-yi[1,2]

(1. School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, Beijing 100876, China;
3. Software Development Center, Head Office of the Agricultural Bank of China, Beijing 100073, China)

Abstract: In cloud computing, the data and computation migration gives rise to trust problems between the user and the cloud. Including the hardware platform, the multiple dimensions method was studied, as well as the user identity and behavior. The electronic identity (eID)-based virtual machine trusted attestation system in infrastructure-as-a-service (IaaS) cloud was designed. The hardware platform was used for trust third party architecture. The citizen's network eID was used as users' unique authoritative identity. The credit records were also applied to evaluate the user's behaviors. Four steps were adopted to solve the trust problem between two sides, including trusted attestation of the user identification and trusted attestation of the virtual machine. Experiment analysis shows that this system can defend common attacks, it is more safety, and the time complexity is within acceptable limitations.

Key words: trust computing; cloud computing; infrastructure as a service; electronic identity; remote attestation

云计算在受到广泛关注的同时其所面临可信安全等方面的挑战也是前所未有的[1]. IaaS 作为云计算中的服务模式,要求用户将全部数据与计算托管到 IaaS 中,根据需求"弹性"的扩展服务能力,但同时带来了两大可信问题:云服务(虚拟机)可信性[2]和用户身份可信性. 针对这些问题,笔者从硬件平

收稿日期: 2013-10-17
基金项目: 国家高技术研究发展计划项目(2012AA01A404)
作者简介: 吴 旭(1963—), 女, 研究员, 博士生导师;许 晋(1990—), 男, 硕士生, E-mail: xujin59545@bupt.edu.cn.

台、用户身份和用户行为多个维度,采用基于国家公安部人口库的 eID(electronic identity),建立用户行为诚信记录,研究实现了 IaaS 云虚拟机 eID 可信验证系统,为 eID 在全国范围内应用推广奠定基础.

1 相关研究

对于云中虚拟机可信性的问题,现有方法是针对硬件平台使用可信计算技术和可信远程验证技术[3],使用 TTP(trust third party)对云服务提供商进行可信验证. Imran Khan 等[4]设计并部署了 Trusted Eucalyptus Cloud,引入可信第三方可信完整性验证者(TIV),确保用户的虚拟机只能在满足完整性验证的物理节点上启动. XinSiyuan 等[5]提出一种基于属性的远程验证方式,TPM(trusted platform module)保存云节点的可信性信息,验证代理直接与 TPM 通信以获取云节点可信性信息.

目前,已有针对用户身份验证方式如用户名密码、随机数验证码等,是针对已注册的用户,缺乏权威普适性. ManikLal Das 等[6]提出了一种 ID-based 动态远程验证方法,使用存储密钥的智能卡作为唯一授权用于验证登录用户,但没有解决 ID 被盗的风险,且无法抵御远程主机的伪造攻击. Wang Yan 等[7]提出了一种更安全有效的 ID-based 动态远程验证方法,需要用户提交 ID,并根据此 ID 做 Hash 运算后与密钥一起存储在智能卡中. Lee 等[8]指出这种做法虽然解决了 ID 被盗的风险,但是却依然不能抵御远程主机的伪造攻击,且无法处理 ID 信息变更所带来的问题,并没有给出针对问题的解决方案. 将用户身份与硬件相结合,Yu Jinwei[9]提出一种基于 USB-Key 技术的网络安全认证方式,使用了 MD5 算法及随机数方案. Chuang Mingchin 等[10]使用智能卡、密码和生物识别技术,基于可信计算技术提出一种匿名多服务器身份验证密钥协商方法,使用随机数和散列函数构造轻量级认证方案,但均缺乏从用户身份到硬件的普适映射方式,真实环境下无法做到抗仿冒攻击.

用户身份是可信的,但行为并不一定可信[11],尤其是在云计算中,如果黑客在开始时伪造合法身份使用云平台,等时机成熟后突然发起攻击,这是难以防御的. 即便是可信合法用户,其行为评估原则与基本思路、单个访问与长期访问的信任评估策略、基于用户行为历史的动态访问策略、基于用户角色的访问控制策略(RBAC,role based acess control)等均是下一步云计算中需要解决的热点问题[12-15].

总之,分别从硬件平台、用户身份或者用户行为等单一维度进行 IaaS 云虚拟机可信验证,均不能解决双方的互可信问题,迫切需要基于全国唯一的公民网络身份标识,将硬件、身份与行为多维度结合的研究成果.

2 虚拟机可信验证系统模型设计

笔者在硬件平台中使用可信计算技术有效验证云虚拟机可信性的基础上,引入全国唯一公民网络电子身份标识 eID 对用户身份可信性进行有效验证,并通过建立“诚信记录”,从用户行为维度增强系统的可信度.

相关符号定义如表 1 所示.

表 1 相关符号定义

符号	定义
VM_req	虚拟机请求
VM_id	虚拟机标号
eID_SerialNum	eID 序列号
eID_Verify	eID 验证信息
eID_Behavior	eID 绑定用户行为记录
Connect_req	虚拟机连接请求
IR	虚拟机完整性报告
‖	连接操作
LSR[ ]	左移操作

虚拟机 eID 可信验证系统模型如图 1 所示.

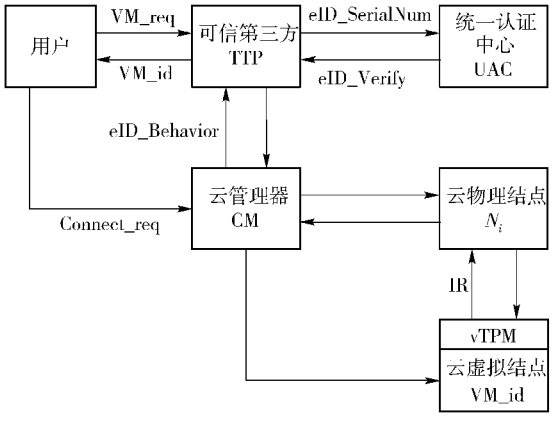

图 1 IaaS 云虚拟机 eID 可信验证系统模型设计

硬件平台维度采用可信第三方 TTP 架构,TTP 即用户和云共同信任的第三方,为用户代理验证云服务是否可信,同时为云代理验证用户是否可信. IaaS 云架构包括云管理器(CM,cloud manager)和一系列的云物理结点 N_i. 其中,CM 是 IaaS 云的接入与管理结点,其主要功能是合理分配 N_i 给不同需求

的用户. 每个 N_i 上运行的云虚拟机必须满足可信计算结构,即在虚拟机中嵌入可信平台模块(vTPM, virtual TPM). 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,为度量和验证平台的可信属性即完整性提供基础.

用户身份维度. 使用 USB 接口的智能芯片设备 eID-key 以及统一认证中心 UAC. eID-key 内存储一对非对称密钥及相关电子信息(eID_SerialNum). 密钥对在智能芯片内部产生,读取时由 PIN 码保护,防止非法复制,保证芯片载体与持有人一一对应. UAC 作为 eID 电子身份信息的颁发验签机构,必须是权威的国家职能部门或者其分布式认证服务结点,笔者所使用的认证结点基于公安部人口库. 当 eID 在网络上远程使用时,使用密钥进行芯片内部的数字签名等运算,通过 UAC 完成实时验证. eID 前端匿名后端实名的方式使得黑客难以伪造合法用户身份,保护用户的合法权益,解决了 ID 被盗或者伪造的风险.

用户行为维度. eID 作为公民在网络上的唯一身份标识,在虚拟机可信验证的整个流程中使用 eID 作为认证标识与步骤标识,具体是使用 eID 内部智能加密芯片生成的 RandomNum. 初始生成随机数 $\mathrm{RandomNum_{req}}$ 是由用户的 eID 序列号与虚拟机请求时的时间戳共同生成的,如式(1)所示.

$$\mathrm{RandomNum_{req}} = \mathrm{eID\_SHA1}(\mathrm{eID\_SerialNum} \parallel \mathrm{Timestamp_{req}}) \quad (1)$$

eID_SHA1 可以用来验证数据的完整性,其继承了 SHA1 操作的如下特点:不可以从消息摘要中复原信息;两个不同的消息不会产生同样的消息摘要. 同时该操作在 eID 内部智能加密芯片进行,保证生成的 $\mathrm{RandomNum_{req}}$ 具有唯一性和不可抵赖性.

在验证流程之后的几个阶段中,每次通信过程均使用新的 RandomNum,如式(2)所示.

$$\mathrm{RandomNum_{new}} = \mathrm{LSR}[\mathrm{RandomNum_{old}}, 10] \quad (2)$$

在原有随机数的基础上,做左移十位操作. 其优势如下:为网络通信提供了额外的安全保障;同样的 RandomNum 保证了整个通信过程在同一个流程内;每次左移代表了一次信息发送,用于标明验证流程的进度;保存了时间戳等信息,一旦中间环节用户越权操作,可追溯原始信息.

同时,CM 将用户行为记录 eID_Behavior 反馈给 TTP,保存在可信控制列表(TCL,trust control list)中可以直接追溯不良用户的非法行为. 通过建立基于云平台使用的"诚信记录",直接拒绝不良信誉的用户使用 IaaS 云. 更进一步地充分挖掘和利用云平台海量的用户使用记录信息,减轻云端检测恶意应用的压力,提高识别准确度.

3　虚拟机可信验证系统流程实现

笔者所使用的 IaaS 云实验环境基于 Eucalyptus 构建. 虚拟机可信验证流程分为 4 个阶段:虚拟机请求阶段、用户身份可信性验证阶段、虚拟机可信验

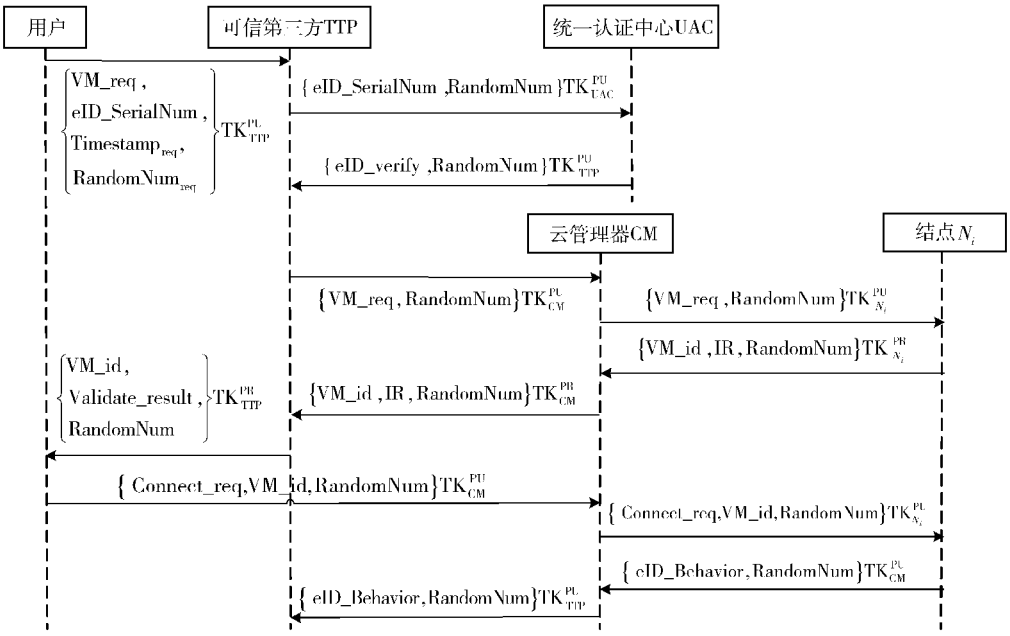

图 2　IaaS 云虚拟机 eID 可信验证流程

证阶段、虚拟机连接阶段,如图2所示. 其中,用户、TTP、CM互为保存对方公钥,TTP与UAC、CM与N_i互为保存对方公钥. 相关符号定义如表2所示.

表2 相关符号定义

符号	定义
$TKPU_{UAC}$	UAC公钥
$TKPR_{UAC}$	UAC私钥
$TKPU_{TTP}$	TTP公钥
$TKPR_{TTP}$	TTP私钥
$TKPU_{CM}$	CM公钥
$TKPR_{CM}$	CM私钥
$TKPU_{Ni}$	N_i的公钥
$TKPR_{Ni}$	N_i的私钥
Validate_result	完整性验证结果

3.1 虚拟机请求阶段

此阶段主要针对用户发出的虚拟机请求.

1)远程用户发出虚拟机请求VM_req,TTP接受请求的同时读取用户的eID_SerialNum,与$Timestamp_{req}$、$RandomNum_{req}$等用TK_{TTP}^{PU}一起进行加密发送至TTP.

2)TTP在接收到虚拟机请求消息后,使用TK_{TTP}^{PR}解密,保存VM_req、eID_SerialNum与$Timestamp_{req}$等信息. 此时,TTP会对$RandomNum_{req}$进行校验,根据生成$RandomNum_{req}$的计算公式在TTP本地生成$RandomNum_{TTP}$,并验证两个随机数是否相同. 如果不同,则说明用户与TTP间的远程链路可能存在安全问题,拒绝虚拟机请求. 然后在TCL中检索eID_SerialNum是否存在违规行为记录,如存在,根据约定访问控制量化此次虚拟机请求.

3.2 用户身份可信性验证阶段

用户身份可信性验证阶段由TTP代理验证用户身份可信性,涉及TTP与UAC之间的两次通信.

1)首先,TTP将用户的eID_SerialNum、RandomNum使用TK_{UAC}^{PU}加密发送给UAC.

2)UAC在接收消息并解密,检索并验证eID_SerialNum是否真实有效,生成验证结果eID_verify. 之后使用TK_{TTP}^{PU}加密eID_verify及RandomNum返回TTP.

3)TTP在接收到消息后使用TK_{TTP}^{PR}解密,获得eID_verify,以此判断用户身份可信性.

3.3 虚拟机可信性验证阶段

虚拟机可信性验证阶段主要涉及由TTP代理验证虚拟机的可信性,涉及TTP与CM,CM与N_i之间的4次通信过程.

1)在第2阶段完成后,TTP使用TK_{CM}^{PU}将加密保存的VM_req与RandomNum转发给CM.

2)CM接收并解密获得VM_req,选择合适的物理机N_i(如使用负载均衡技术)转发VM_req,连同RandomNum使用TK_{Ni}^{PU}对信息进行加密.

3)物理机N_i读取VM_req,根据用户的虚拟机类型和硬件需求开启标号为VM_id的虚拟机. 虚拟机启动时,使用TPM模块对系统进行完整性度量. 系统启动后自动生成完整性报告IR,其中包括:TPM保存的PCR值,对所有PCR值使用AIK私钥做quote操作的签名值,BIOS和运行时IML文件中事件类型、名称、摘要值的记录. 随后使用TK_{Ni}^{PR}对VM_id、IR、RandomNum做签名并转发至CM.

4)CM收到消息后,使用TK_{Ni}^{PU}解密,验证是由N_i发送过来的消息. 将得到的信息使用TK_{CM}^{PR}对信息进行签名,发送给TTP.

5)TTP接收到CM转发信息,对IR进行验证,生成虚拟机可信性验证结果Validate_result. 连同VM_id、RandomNum用TK_{TTP}^{PR}做签名发送至用户.

3.4 虚拟机连接阶段

虚拟机连接阶段是连接虚拟机相关操作,直接在用户与CM之间进行.

1)用户收到TTP发送的消息后,使用TK_{TTP}^{PU}解密,如果虚拟机验证结果是不通过,则用户放弃连接到该虚拟机;如果验证通过,则向CM发送连接请求. 使用TK_{CM}^{PU}对Connect_req、VM_id、RandomNum加密,发送给CM.

2)CM接收到连接请求后,使用TK_{Ni}^{PU}加密并转发给N_i,指定连接到标号为VM_id的虚拟机.

3)物理机N_i收到CM发送的连接请求解密后,允许用户连接到标号为VM_id的虚拟机. 记录用户使用虚拟机时行为生成eID_Behavior并与RandomNum一起用TK_{CM}^{PU}加密发送给CM.

4)CM负责将信息反馈给TTP,即用TK_{TTP}^{PU}将eID_Behavior、RandomNum加密发送至TTP. 由TTP保存至TCL中,以便根据用户行为记录量化用户的下一次虚拟机请求.

至此,完成一次完整的虚拟机可信验证流程.

4 分析与验证

4.1 安全性

对抗常见的攻击形式分析如下:

1）抗消息重放攻击

用户在虚拟机请求时使用的 $Timestamp_{req}$，通过 SHA1 将其映射到 RandomNum 中，随后保存在 TTP 中备查，在可信验证的整个过程中使用该 RandomNum. 黑客如果使用相同的虚拟机请求{$Timestamp_{req}$，eID_SerialNum，$RandomNum_{req}$}，由于已经存在该虚拟机请求会遭到 TTP 的直接拒绝，从而有效地抵抗消息重放攻击.

2）抗中间人攻击

TTP 接收到用户的虚拟机申请后，会首先对 $RandomNum_{req}$进行校验. 由于 SHA1 的函数特性，中间人无法使用其他{$Timestamp_{req}$，eID_SerialNum}组合生成相同的 RandomNum. 假使中间人截获用户发送的{$Timestamp_{req}$，eID_SerialNum}并解密，替换其中的 $Timestamp_{req}$. 但由于其无法通过 eID 智能芯片产生正确的消息摘要，也就无法通过 TTP 的校验，此时 TTP 会判断虚假虚拟机请求并拒绝此次请求，有效抵抗了中间人攻击.

3）抗拒绝服务攻击

用户的 eID_SerialNum 由智能卡内部芯片产生，同时需要到 UAC 进行验证，只有在验证通过的前提下才能继续进行后续操作. 攻击者需要大量合法有效的 eID 卡才能发起 DoS 攻击，但由于 eID 与人是一一对应的，不存在一人拥有多张 eID 卡情况. 这有效抵抗了拒绝服务攻击.

4）抗口令猜测攻击

虚拟机请求阶段需要提供用户的 eID_SerialNum，而 eID 具有 PIN 码保护，5 次输入错误即锁定用户的使用权限，有效地抵抗了口令猜测攻击.

5）抗云平台外部人员攻击

假如黑客盗取合法用户的 eID 并已首次通过身份验证，申请到虚拟机企图进行恶意操作. 一旦黑客产生恶意行为，基于云的用户行为监测即会监测出该用户行为超出预期. 此时会将 eID_Behavior 与 eID 绑定返回 TTP 并保存至 TCL 中. 持有该 eID 的非法用户在下一次虚拟机请求时，TTP 会在 TCL 中查到相应的非法记录，即使通过身份验证 TTP 也会选择量化该用户的操作请求，或者直接拒绝该用户的虚拟机请求，有效地抵抗云外部人员攻击.

6）抗云平台内部人员攻击

RandomNum 的左移次数可作为步骤标识，每次通信过程中均会检查该标识. 用户在虚拟机申请时由 TTP 处理 RandomNum 进行左移操作生成 $RandomNum_{new}$并转发给 CM. 假设拥有云平台管理权限的入侵者获得了加密的{VM_req，RandomNum}TK_{CM}^{PU}. 由于入侵者并不知道 TK_{CM}^{PR}，也就不能解密该消息. 最坏情况下，入侵者破译了 TK_{CM}^{PR}，得到 RandomNum 并希望用该随机数伪装合法用户. 此时存在两种情况，一种是入侵者不知道左移操作，CM 收到了旧的 RandomNum，说明存在中间人攻击现象，CM 拒绝此次连接请求；一种是入侵者将 RandomNum 左移生成 $RandomNum_{new}$并发送给 CM，CM 收到 2 次相同随机数，说明云平台存在越权操作现象，同样拒绝此次连接请求.

4.2　计算性能

通过测试完整的虚拟机请求分析引入可信验证系统所带来的计算时间消耗. 如图 3 所示，从下到上依次为普通虚拟机（VM）、只嵌入 vTPM 的虚拟机（TVM）、只使用 eID 的虚拟机（eVM）、引入可信验证系统中的虚拟机（eTVM）的虚拟机启动时间消耗.

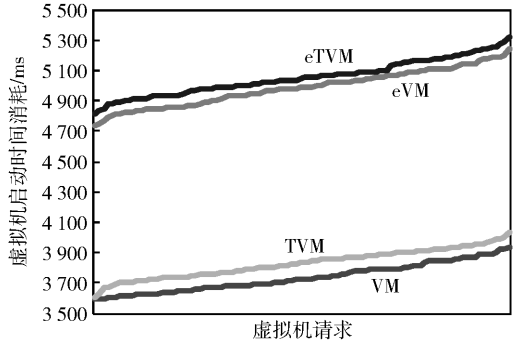

图 3　虚拟机启动时间消耗对比

在相同网络环境下，实验对 4 种类型虚拟机分别做 100 次虚拟机启动请求，对比相应的启动时间消耗. 从图 3 中可以看出嵌入 vTPM 对虚拟机的启动影响不大，差别在 500 ms 左右. 而引入 eID 带来了 1 000 ms 的额外时间消耗，这是由于需要检索 UAC 的庞大数据库，需要进一步改进和完善. 但对于用户来说 1 000 ms 仍是可以接受的.

另外，使用 BYTEmark 对比 eTVM 与 VM 的计算性能差别，测试引入可信验证系统所带来的计算性能代价，如图 4 所示.

BYTEmark 运行 10 种计算密集型算法，根据每秒迭代次数考察计算性能，一次测试会依次运行 10 种算法，每个算法运行 5 次，综合分析给出 3 个综合评分指标. 实验结果取 1 000 次的平均值，从图 4 中可以看出，eTVM 与 VM 的比值均小于 1，这是因为

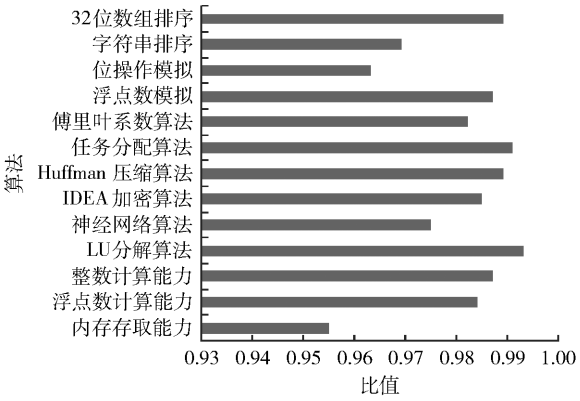

图4 BYTEmark 测试结果比值(eTVM/VM)

eTVM 中的 IMA 要记录运行程序哈希值并记录至 TPM 中,可信验证系统确实为虚拟机的计算性能带来一定代价,导致 eTVM 的得分都要比 VM 低,但是其代价消耗基本可忽略.

5 结束语

为解决用户在使用 IaaS 云服务时存在的互可信问题,从硬件平台、用户身份与用户行为多个维度,将云计算与可信计算技术相结合,引入全国权威的网络唯一身份标识 eID,设计了可信虚拟机验证流程,实现了 IaaS 云虚拟机 eID 可信验证系统. 系统使用 TTP 的设计,由其代理验证用户身份可信性,进一步保证了云平台可信性. 该系统符合可信计算的标准,相较已有系统提高了安全性与稳定性,可抵抗常见的攻击形式,且计算时间复杂度在可接受范围内. 更为重要的是该系统实现了基于 eID 的用户身份可信性验证,为构造可信的云计算环境奠定基础. 下一步工作将在基于用户行为的访问控制方面深入研究.

参考文献:

[1] Pearson S. Privacy, security and trust in cloud computing [M]. [S.l.]: Springer London, 2013: 3-42.

[2] Huang J, Nicol D M. Trust mechanisms for cloud computing[J]. Journal of Cloud Computing, 2013, 2(1): 1-14.

[3] Trusted Computing Platform Alliance (TCPA). TCPA main specification version 1.1b[R]. Trusted Computing Group, 2002: 2-9.

[4] Imran K, Rehman H, Zahid A. Design and deployment of a trusted eucalyptus cloud[C]//2011 IEEE International Conference on Cloud Computing(CLOUD). Washington DC: IEEE, 2011: 380-387.

[5] Xin Siyuan, Zhao Yong, Li Yu. Property-based remote attestation oriented to cloud computing[C]//2011 Seventh International Conference on Computational Intelligence and Security. Sanya: [s.n.], 2011: 1028-1032.

[6] Manik L D, Ashutosh S, Ved P G. A dynamic ID-based remote user authentication scheme[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 629-631.

[7] Wang Y, Liu J, Xiao F, et al. A more efficient and secure dynamic ID-based remote user authentication scheme [J]. Computer Communications, 2009, 32(4): 583-585.

[8] Lee H, Choi D, Lee Y, et al. Security weaknesses of dynamic ID-based remote user authentication protocol[J]. Proceedings of the World Academy of Science Engineering and Technology, 2009, 59: 190-193.

[9] Yu Jinwei. The program design for the network security authentication based on the USB key technology[C]// 2011 International Conference on Electronic and Mechanical Engineering and Information Technology. [S.l.]: IEEE, 2011: 2215-2218.

[10] Chuang M C, Chen M C. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics[J]. Expert Systems with Applications, 2014, 41(4): 1411-1418.

[11] 林闯, 田立勤, 王元卓. 可信网络中用户行为可信的研究[J]. 计算机研究与发展, 2008, 45(12): 2033-2043.
Lin Chuang, Tian Liqin, Wang Yuanzhuo. Research on user behavior trust in trustworthy network[J]. Journal of Computer Research and Development, 2008, 45(12): 2033-2043.

[12] Tian L, Lin C, Ni Y. Evaluation of user behavior trust in cloud computing[C]//Computer Application and System Modeling (ICCASM), International Conference on. [S.l.]: IEEE, 2010: 567-572.

[13] Dewangan M B K, Shende M P. Survey on user behavior trust evaluation in cloud computing[J]. International Journal of Science, Engineering and Technology Research, 2012, 1(5): 113-117.

[14] Lin Honggang. Research on trust-degree based dynamic access control model[C]//E-Product E-Service and E-Entertainment (ICEEE), 2010 International Conference on. [S.l.]: IEEE, 2010: 1-4.

[15] Lin G, Bie Y, Lei M. Trust based access control policy in multi-domain of cloud computing[J]. Journal of Computers, 2013, 8(5): 5-10.