

(19) 中华人民共和国国家知识产权局



## (12) 发明专利申请

(10) 申请公布号 CN 104935608 A

(43) 申请公布日 2015.09.23

(21) 申请号 201510395427.0

(22) 申请日 2015.07.07

(71) 申请人 成都睿峰科技有限公司

地址 610041 四川省成都市高新区天府大道  
北段 1480 号拉德方斯大厦东楼 10 层

(72) 发明人 马泳宇

(74) 专利代理机构 北京天奇智新知识产权代理  
有限公司 11340

代理人 杨春

(51) Int. Cl.

H04L 29/06(2006.01)

H04L 29/08(2006.01)

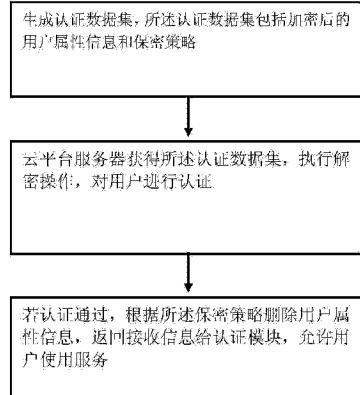
权利要求书1页 说明书5页 附图1页

(54) 发明名称

一种云计算网络中的身份认证方法

(57) 摘要

本发明提供了一种云计算网络中的身份认证方法，该方法包括：生成认证数据集，所述认证数据集包括加密后的用户属性信息和保密策略；云平台服务器获得所述认证数据集，执行解密操作，对用户进行认证；若认证通过，根据所述保密策略删除用户属性信息，返回接收信息给认证模块，允许用户使用服务。本发明提出了一种云计算网络中的身份认证方法，不需要可信第三方，用户和服务器之间彼此进行认证，不需要暴露隐私属性信息，防止信息的泄露或篡改。



1. 一种云计算网络中的身份认证方法,用于私有云对用户进行身份认证,其特征在于,包括 :

步骤一,生成认证数据集,所述认证数据集包括加密后的用户属性信息和保密策略;

步骤二,云平台服务器获得所述认证数据集,执行解密操作,对用户进行认证;

步骤三,若认证通过,根据所述保密策略删除用户属性信息,返回接收信息给认证模块,允许用户使用服务。

2. 根据权利要求 1 所述的方法,其特征在于,所述步骤一,生成认证数据集,所述认证数据集包括加密后的用户属性信息和保密策略,进一步包括 :

云平台的认证模块中的属性库根据云平台服务器请求的属性声明来收集用户对应的属性信息,然后利用认证模块的密钥数据库提供的属性加密私钥,调用虚拟机执行非对称加密过程,生成加密的用户属性信息,如果云平台服务器没有发送属性请求,则将用户允许的所有属性信息加密,发送到认证模块的认证执行单元,认证模块的策略执行单元选取相应保密策略,所述保密策略包括完整性自检、自删除策略,认证执行单元将加密的用户属性信息、保密策略、属性加密公钥、签名信息和虚拟机信息摘要五个部分一起用云平台服务器提供的公钥打包,生成认证数据集,并通过安全通道传输给云平台服务器。

3. 根据权利要求 2 所述的方法,其特征在于,所述步骤二,云平台服务器获得所述认证数据集,执行解密操作,对用户进行认证,进一步包括 :

云平台服务器获得认证数据集后,输入云平台服务器提供的私钥,虚拟机执行解密操作,成功解密后,认证数据集启动完整性自检,将计算出的值与之前已经保存在保密策略中的值对比,若符合则启用认证数据集。

4. 根据权利要求 3 所述的方法,其特征在于,所述步骤三,若认证通过,根据所述保密策略删除用户属性信息,返回接收信息给认证模块,允许用户使用服务,进一步包括 :

云平台服务器对用户的认证通过后,如果云平台服务器不查看用户属性信息,根据具体保密策略立即删除用户属性信息,并将签名信息交给云平台服务器保存,云平台服务器返回接收信息给认证模块,表示允许使用服务,当用户再次请求该相同的服务时,云平台服务器只返回所述签名,认证模块验证签名即可表示认证该云平台服务器;若云平台服务器需要查看用户的属性信息,输入云平台服务器提供的私钥到虚拟机,解密用户属性信息,在保密策略中将多余的信息删除,云平台服务器得到信息后进一步认证,认证通过后发送接收信息给认证模块,如果没有通过,则返回拒绝信息。

## 一种云计算网络中的身份认证方法

### 技术领域

[0001] 本发明涉及云计算,特别涉及一种云计算网络中的身份认证方法。

### 背景技术

[0002] 云计算中庞大的数据交易和各类信息服务的背后却隐藏着杂乱繁多的账户管理问题,使得数字身份无疑成为了关注焦点。近年来因为数字身份泄露造成的侵犯个人隐私案件时有发生。为了在云之间资源能安全共享,云彼此身份的合法性自然也成为重要的关注点。身份认证作为信息安全的守卫,是云安全措施不可或缺的环节。

[0003] 为了实现通用登录,很多机制也在开发和使用当中。其中一些是针对合作网站之间安全交换信息认证和授权而开发的框架或协议,而另一些则是横跨网站、应用程序和设备而搭建的,将身份以及关系信息融为一体的数据架构,但现有以上架构构造信任的高额成本和作为身份提供者的可信第三方可能存在单点失效问题。

### 发明内容

[0004] 为解决上述现有技术所存在的问题,本发明提出了一种云计算网络中的身份认证方法,包括:

[0005] 步骤一,生成认证数据集,所述认证数据集包括加密后的用户属性信息和保密策略;

[0006] 步骤二,云平台服务器获得所述认证数据集,执行解密操作,对用户进行认证;

[0007] 步骤三,若认证通过,根据所述保密策略删除用户属性信息,返回接收信息给认证模块,允许用户使用服务。

[0008] 优选地,所述步骤一,生成认证数据集,所述认证数据集包括加密后的用户属性信息和保密策略,进一步包括:

[0009] 云平台的认证模块中的属性库根据云平台服务器请求的属性声明来收集用户对应的属性信息,然后利用认证模块的密钥数据库提供的属性加密私钥,调用虚拟机执行非对称加密过程,生成加密的用户属性信息,如果云平台服务器没有发送属性请求,则将用户允许的所有属性信息加密,发送到认证模块的认证执行单元,认证模块的策略执行单元选取相应保密策略,所述保密策略包括完整性自检、自删除策略,认证执行单元将加密的用户属性信息、保密策略、属性加密公钥、签名信息和虚拟机信息摘要五个部分一起用云平台服务器提供的公钥打包,生成认证数据集,并通过安全通道传输给云平台服务器。

[0010] 优选地,所述步骤二,云平台服务器获得所述认证数据集,执行解密操作,对用户进行认证,进一步包括:

[0011] 云平台服务器获得认证数据集后,输入云平台服务器提供的私钥,虚拟机执行解密操作,成功解密后,认证数据集启动完整性自检,将计算出的值与之前已经保存在保密策略中的值对比,若符合则启用认证数据集。

[0012] 优选地,所述步骤三,若认证通过,根据所述保密策略删除用户属性信息,返回接

收信息给认证模块,允许用户使用服务,进一步包括:

[0013] 云平台服务器对用户的认证通过后,如果云平台服务器不查看用户属性信息,根据具体保密策略立即删除用户属性信息,并将签名信息交给云平台服务器保存,云平台服务器返回接收信息给认证模块,表示允许使用服务,当用户再次请求该相同的服务时,云平台服务器只返回所述签名,认证模块验证签名即可表示认证该云平台服务器;若云平台服务器需要查看用户的属性信息,输入云平台服务器提供的私钥到虚拟机,解密用户属性信息,在保密策略中将多余的信息删除,云平台服务器得到信息后进一步认证,认证通过后发送接收信息给认证模块,如果没有通过,则返回拒绝信息。

[0014] 本发明相比现有技术,具有以下优点:

[0015] 本发明提出了一种云计算网络中的身份认证方法,不需要可信第三方,用户和服务器之间彼此进行不公开的认证,不需要暴露隐私属性信息,防止信息的泄露或篡改。

## 附图说明

[0016] 图 1 是根据本发明实施例的云计算网络中的身份认证方法的流程图。

## 具体实施方式

[0017] 下文与图示本发明原理的附图一起提供对本发明一个或者多个实施例的详细描述。结合这样的实施例描述本发明,但是本发明不限于任何实施例。本发明的范围仅由权利要求书限定,并且本发明涵盖诸多替代、修改和等同物。在下文描述中阐述诸多具体细节以便提供对本发明的透彻理解。出于示例的目的而提供这些细节,并且无这些具体细节中的一些或者所有细节也可以根据权利要求书实现本发明。

[0018] 本发明的一方面提供了一种云计算网络中的身份认证方法。图 1 是根据本发明实施例的云计算网络中的身份认证方法流程图。本发明通过匿私有云身份认证方案,可以被嵌入如智能卡等微型硬件中,终端用户获得合法使用权后通过各种移动设备来请求服务。终端用户不用担心自己身份隐私问题,同时降低网络负载,克服网络延迟。

[0019] 云身份认证空间参与的角色包含:私有云平台服务器、云终端用户和云平台认证模块。而云平台认证模块包含了以下六个部分。

[0020] 虚拟身份库:虚拟身份库中包括签名密钥。签名密钥里存储对用户的虚拟账户 VID 进行签名保护的数字签名 Sg, Sg 被发送到认证执行单元中去组建认证数据集。认证过程结束后,云平台服务器将得到并选择保存 Sg。当下一次被请求服务时,即使云平台服务器有认证属性的需求,终端用户只需用 Sg 作为条件进行元数据认证,云平台服务器把解密元数据得到的值跟之前存储的 Sg 对比就能完成认证了。这样即提高了认证效率也减少了暴露隐私信息的次数。

[0021] 属性库:属性库用于将用户的个人隐私属性信息收集起来并用密钥数据库提供的属性加密私钥 AKpr 加密,生成密文 EAT 保存其中,如:Email 地址、电话号码。认证初始化过程中属性库将 EAT 发送给认证执行单元打包生成认证数据集。在认证过程中,如若云平台服务器需要查看用户的属性信息 ATT,则首先使用属性加密公钥 AKpu 解密获取属性信息。值得注意的是,用户可以选择提供给属性库全部或部分个人隐私信息,而不是由属性库自动搜索用户所拥有的所有属性,这样给了用户更多权力来掌控自己的隐私。而且,由于云

环境的动态特性,用户信息也可能变化,所以用户想请求新的服务时,需要添加新的属性信息,这时可以通过属性库更新或是修改自己的属性信息。

[0022] 认证执行单元:认证执行单元的职责是生成非公开认证的元数据描述令牌和认证数据集。认证阶段首先认证执行单元首先会得到云平台服务器发送的服务器令牌,然后调用虚拟机中的查询算法描述元数据令牌的有效性来认证云平台服务器是否合法。然后认证执行单元还会利用得到的服务器 ID 及其他安全参数等为用户生成自己的元数据描述令牌 UTKf,让云平台服务器完成对用户的身份匿名认证。认证执行单元还负责生成属性认证所需的认证数据集。

[0023] 认证数据集由五部分构成:加密的属性信息 EAT、签名的虚拟账户 Sg、保密策略、属性加密公钥 AKpu 和基于虚拟机的信息摘要(包含认证过程所必需的执行代码和算法)。保密策略中包括了认证数据集在到达云平台服务器后,启用前后的一系列保密策略,通过虚拟机实施这些策略,完成认证。整个认证数据集打包后用云平台服务器的公钥加密,又添加了一道安全防线。

[0024] 策略执行单元:包括了各种保密策略和机制,如:完整性自检、自删除、生命周期、审计和日志等,还可以根据用户应用需求添加的策略来加强认证安全。其中完整性自检策略规定了定期检查自我数据的完整性,确保数据没有被恶意篡改或破坏。当数据集到达云平台服务器时,也会启用完整性自检,成功通过后才能启用认证模块。自删除机制则包括两种形式:

[0025] 当发现威胁或是恶意破坏的迹象,立即通过虚拟机启动自删除所有数据,以防隐私信息被窃或是篡改。或是认证过程中,对于云平台服务器没有请求的属性信息,视为多余隐私信息,把这部分信息消除掉,以防隐私安全问题。而生命周期管理,制定了 VID 的生成、配置、管理和撤消回收等。日志和审计制度则记录认证模块运行的情况,及时获得危险警告或故障通知等,以便描述或是事故处理。

[0026] 虚拟机:系统中(包括认证模块和云平台服务器端)的虚拟机是一个执行代码的容器,含操作系统和一些基础的系统代码,同时装载了加解密、查询等算法和程序,用于加强实施保密策略,和执行其他组件的任务。发送给云平台服务器的认证数据集和元数据数据库都会分配虚拟机信息摘要,包含了执行属性认证和匿名认证过程所需的算法和代码,来完成整个认证过程。

[0027] 密钥数据库:存储着供加解密属性信息的密钥,和认证中元数据加密过程生成的密钥。

[0028] 双向云身份认证包含两大机制:匿名认证和属性认证。首先介绍这两个机制的认证细节,然后分析具体场景下整个认证流程。

[0029] 属性认证:

[0030] 1) 认证数据集生成阶段

[0031] 属性库根据云平台服务器请求的属性声明来收集用户对应的属性信息。然后利用密钥数据库提供的属性加密私钥 AKpr,调用虚拟机执行非对称加密过程,生成 EAT。如果云平台服务器没有发送明确的属性请求,则将用户允许的所有属性信息加密,发送到认证执行单元。策略执行单元选取相应保密策略,如:完整性自检、自删除策略等。认证执行单元将 EAT、保密策略、AKpu、Sg 和虚拟机信息摘要五个部分一起用云平台服务器提供的公钥

SKPu 打包,生成认证数据集,并通过安全通道传输给云平台服务器。

[0032] 2) 认证数据集启用阶段

[0033] 云平台服务器获得认证数据集后,输入云平台服务器提供的私钥 SKPr 和解密过程,虚拟机执行解密操作。成功解密后,认证数据集启动完整性自检,将计算出的值与之前已经保存在保密策略中的值对比,符合则启用认证数据集。如果完整性自检失败,则启用自我保护策略的完全删除策略,终断认证。

[0034] 3) 认证数据集认证阶段

[0035] 云平台服务器对用户的认证通过后,如果云平台服务器无需查看用户属性信息,根据具体保密策略立即删除 EAT,并将 Sg 作为签名交给云平台服务器保存,云平台服务器返回接收信息给认证模块,表示允许使用服务。当用户再次请求该相同的服务时,云平台服务器只需要返回签名 Sg,认证模块验证签名即可表示认证该云平台服务器。若云平台服务器需要继续查看用户的属性信息,输入私钥 SKpr 到虚拟机,解密 EAT。保密策略中会根据情况将多余的信息删除。云平台服务器得到信息后进一步认证。认证通过后发送接收信息给认证模块,如果没有通过则返回拒绝信息。

[0036] 匿名认证 :

[0037] 本方案,在两个阶段运用了前面介绍的两种不同的元数据加密概念,首先实现云平台服务器向用户进行匿名认证,然后完成认证模块向云平台服务器认证用户的合法身份。

[0038] 第一阶段 : 云平台服务器向用户进行认证

[0039] 云平台服务器首先生成一对密钥 SPK, SMK ; 然后加密公钥和自己的 ID 生成密文 SCT ; 接着把密钥对 SPK、SMK 和元数据描述函数 f 作为输入项,生成元数据描述令牌。

[0040] 当认证模块得到令牌和 SPK、SCT 后,虚拟机调用查询算法输出元数据描述结果布尔值。如果为真,则表示云平台服务器为所请求的服务器,进行下一步通信,否则,用户立即停止通信,以防钓鱼网站或其他虚假服务器带来的安全威胁。

[0041] 第二阶段 : 认证模块向云平台服务器证明用户身份

[0042] 同理,该阶段加密时输入的参数增加了云平台服务器声明的属性条件 I。不同之处在于,当认证模块在云平台服务器端被启用后,云平台服务器将得到密文 UCT 和 UCK,作为两个输入参数,调用解密过程进行解密计算。如果得到用户自己的 ID 值,则表明认证模块的拥有者是合法的;如果得到空字符,则拒绝提供服务。当用户向某云平台服务器再次请求服务时,可以选择在第二步的加密过程中使用 Sg 替代服务器的 ID。这样,云平台服务器解密 UTKf 后,把结果值与之前保存的 Sg 进行对比,如果一致则可以判定请求者是合法的。

[0043] 此外,若终端用户是请求扩充资源的另一个私有云 PC,则请求云服务的身份认证全过程具体步骤如下:

[0044] Step1 : PC 向云平台服务器请求服务。

[0045] Step2 : 云平台服务器通过元数据加密过程,把密钥对 SPK、SMK 和元数据描述函数 f 作为输入项,生成元数据描述令牌,用于认证。云平台服务器将服务器令牌、公钥 SKpu,生成认证数据集一起发送给 PC。

[0046] Step3 : PC 接受到认证数据集后,传送给认证模块,认证执行单元首先进行元数据描述,判定云平台服务器是否为 PC 所请求的真实提供者。如果元数据判定结果为真,进入

下一步 ;为假,则返回一个拒绝信息,中断通信。

[0047] Step4 :虚拟身份库把服务器 ID 记录到字典目录中。如果该服务是 PC 第一次请求,虚拟身份库会提供一个虚拟账户 VID,并数字签名 ;如果该云平台服务器曾被请求过,虚拟身份库会根据服务器 ID 在目录中查找到对应的 VID 然后签名生成 Sg。接着将服务器 ID 发送到认证执行单元。

[0048] Step5 :认证执行单元收到服务器 ID 后,利用虚拟机中的元数据加密过程来处理,生成密文 UCT 和元数据描述令牌 UTKf,存储在元数据数据库中并发送给云平台服务器,向其认证 PC 的身份。

[0049] Step6 :云平台服务器接受元数据数据库后,验证结果值是否为自己的 ID 值。如果值相等,则说明 PC 是合法的,此时如果云平台服务器不需要额外的属性信息验证,就可以直接返回同意信息,允许 PC 获取资源 ;若想获取其他属性信息,则返回给认证模块请求属性验证信息。如果值不相等,云平台服务器返回拒绝信息,并停止与请求者 PC 的交互。

[0050] Step7 :当认证模块收到属性验证请求信息后,启动基于认证数据集的认证,生成认证数据集发送给云平台服务器。

[0051] Step8 :云平台服务器得到认证数据集后首先用自己的私钥解密。等待成功通过虚拟机执行的完整性自检后启用。如果没能启用则说明认证数据集被破坏,云平台服务器重新发出请求。

[0052] Step9 :顺利启用后,云平台服务器将得到 PC 的 Sg 和属性加密公钥 AKpu。云平台服务器使用公钥解密 EAT,验证属性信息。

[0053] Step10 :云平台服务器成功验证属性信息后返回接收信息给认证模块。验证失败返回拒绝信息。

[0054] Step11 :认证模块将接收信息传送给 PC。

[0055] Step12 :PC 开始使用服务。

[0056] 综上所述,本发明提出了一种云计算网络中的身份认证方法,不需要可信第三方,用户和服务器之间彼此进行认证,不需要暴露隐私属性信息,防止信息的泄露或篡改。

[0057] 显然,本领域的技术人员应该理解,上述的本发明的各模块或各步骤可以用通用的计算系统来实现,它们可以集中在单个的计算系统上,或者分布在多个计算系统所组成的网络上,可选地,它们可以用计算系统可执行的程序代码来实现,从而,可以将它们存储在存储系统中由计算系统来执行。这样,本发明不限制于任何特定的硬件和软件结合。

[0058] 应当理解的是,本发明的上述具体实施方式仅仅用于示例性说明或解释本发明的原理,而不构成对本发明的限制。因此,在不偏离本发明的精神和范围的情况下所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。此外,本发明所附权利要求旨在涵盖落入所附权利要求范围和边界、或者这种范围和边界的等同形式内的全部变化和修改例。

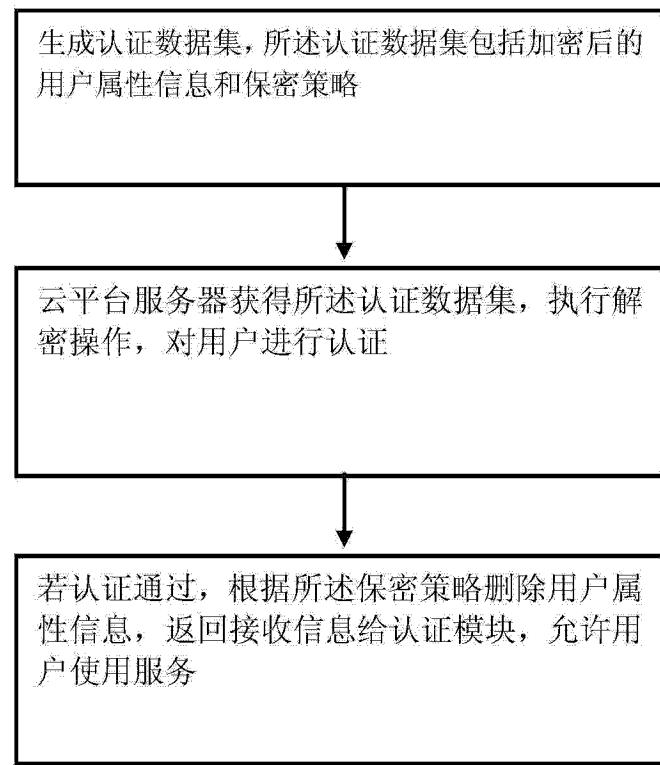


图 1