

基于云平台的电子证据存储中访问控制的动态委托方法

何 月^{1,2}, 陈 明¹

(1 中国石油大学, 北京 102200; 2 昌平区人民检察院, 北京 102200)

摘 要: 对动态云平台电子证据存储代表的必要性的研究, 证明所有资源网站的可信性是安全云平台电子证据存储计算的一个先决条件. 分析了现有的代表团类和电网计划, 并提出了云平台电子证据存储访问控制的模糊信任、委托模型(FTDM)和基于云平台电子证据存储实体之间信任关系的两个阶段的模糊推理过程, 进而决定类的代表团和信任级别授权访问的可能性. 并且引用数字取证分析云平台资源的 K-means 聚类算法的基础上的 CGRS 资源选择算法, 并在实务部门数字取证分析平台的可扩展环境中实施. 通过分析和实验结果验证了分析平台的资源选择算法的有效性和正确性.

关键词: 电子证据; 云平台; K-means 聚类算法; CGRS 资源选择算法; 动态访问控制

中图分类号: TP399

文献标识码: A

文章编号: 1000-7180(2013)05-0162-07

Dynamic Delegation Approach Based on Access Control in the Electronic Evidence Storage of the Cloud Platform

HE Yue^{1,2}, CHEN Ming¹

(1 China University of Petroleum, Beijing 102200 China;

2 The People's Procuratorate in Changping District, Beijing 102200, China)

Abstract: Study on the necessity of electronic evidence storage on dynamic cloud platform of electronic evidence storage. The trustworthiness of the web resources is a prerequisite for secure cloud platform of electronic evidence storage calculation. I analyze the existing classes of delegation and plan for power grid, put forward the new fuzzy trust and FTDM based on the cloud platform of electronic evidence storage access, advance the fuzzy reasoning process of two stage of trust relationship between electronic evidence storage entities based on the cloud platform, and then decide the possibility of classes of delegation and trust level of authorization access. I use CGRS resource selection algorithm which is based on the K-means clustering algorithm in digital forensics analysis of cloud platform resources, and the algorithm is used to scalable environment for digital forensics analysis platform in substantive departments. The analysis and the experimental results, verify the correctness and effectiveness of the analysis platform of resource selection algorithm.

Key words: electronic evidence; cloud platform; K-means clustering algorithm; CGRS resource selection algorithm; dynamic access control

1 引言

访问控制在今天对计算资源的访问是最根本、最普遍的安全机制. 访问控制策略一般符合直接授权的概念, 其中的对象可以直接授权请求的访问. 在一个动态的云平台电子证据存储计算环境中, 对象

和最终用户可能没有直接访问, 或任务、所需资源执行的授权. 直接授权是不可能实现的, 因为计算资源可能属于其他组织, 这意味着用户帐户和权限可能不存在. 因此, 用间接授权来解决这个问题就变得很重要. 代表团是一种间接的授权机制. 代表团一般认为具有静态和动态两种形式. 当要访问的方法或对

象是预先已知的时,可以使用提供资源实体的和预定义的静态代表团,所以,代表团可以被限制为预定义实体所需的行动。动态代表团是指执行某些操作,访问一些对象,或不知道任务开始时间的权利的代表团。

如果一个网站有其他云平台电子证据存储实体的代表,最终用户必须采用可以验证真伪的要求提交一个任务或子任务。通过委派凭据的实体也可以采用不同的方法。一种方法是创建使用的私钥的数字签名,这种方法适用于静态代表团。

为了实现动态授权,所涉及的实体必须建立彼此间信任的关系。格代表团最灵活的形式是模拟委托人代表委托授予完全的访问权限。完全委派的权利可能会受到影响。因此,这意味着通过委托授权,代表团受到限制不应该是全部或无限的。

让我们通过一个例子来说明电网的代表团。域D1的网站 S_i 的服务器要访问代表最终用户的域D2的另一个站点 S_j 的文件。为了使 S_j 信任 S_i , S_i 发送了一个具有凭证的消息,或向 S_j 发送一个令牌来说明已经被最终用户授权 S_i 。动态的云平台电子证据存储环境面临着两个问题。首先是最终用户提交任务后,可能会断开连接的目标网站 S_j 。第二个问题是事先不知道访问要求(它是动态的已知)。因此,另一种方法是通过动态代表团授予访问权限。

对于这一点,站点 S_j 必须信任 S_i ,这意味着一个最小的站点之间的信任关系是强制性的。图1显示了两个网站 S_i 和 S_j 是最终用户在快速情况下是如何动态地建立信任关系,以及信任如何作为代表团证书或从最终用户到站点 S_i 的令牌。

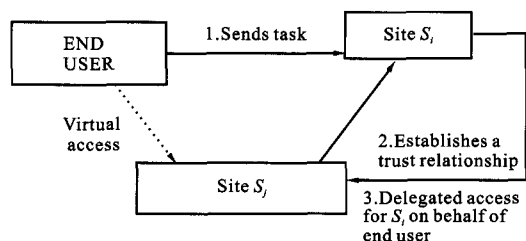


图1 通过信任的动态代表团

Hilary H. Hosmer 等人认为模糊逻辑方法可以用来确保计算机系统的安全。由于安全系统的许多元素是不确切的,为了得到一个更为现实和值得信赖的结果,我们需要通过模糊逻辑处理非传统的世界。

我们可以保证在模糊信任模型的基础上,分布式电网应用在多个云平台电子证据存储资源网站^[5]建立相互信任的关系。模糊信任的集成方法可以加

强安全机制。模糊推理能够量化不精确的数据或测量资源网站的安全性指标的不确定度。不同的推理规则可以使用相同的模糊逻辑推理引擎制定不同的云平台电子证据存储应用程序。

对云平台电子证据存储中的访问要求而言,对于支持像全局负载均衡、经纪或条件计算网站(在一个工作流设置内)上的网站或机器可以运行选择是很有必要的。委托授权也可以用来控制由后台进程执行的动作。本文中,我们分析了现有的代表团类和电网计划,并提出了云平台电子证据存储访问控制的新的模糊信任和委托模型(FTDM)。

云平台电子证据存储中动态代表团的挑战:

使用中的两云平台电子证据存储代表团模型为GSI和UNICORE模型。其弊端是强调需要有明确的使授权访问云平台电子证据存储的信任委托。一种可能的选择是有一个可信的第三方,如Kerberos服务器。第三方授权只能由用户角色的平台来做,这在电网上至今都没有很好地界定。这些事实导致的结论是,委派凭据必须通过一些动态的机制才能产生。现在的大多数电网系统正朝着网络服务发展,这意味着动态代表团机制需要与网络服务基础设施共存。这些原因因为基于模糊逻辑模型的发展提供了动力。

2 模糊信任与代表模型(FTDM)

信托一般可分为身份信任和行为信任^[1]。身份信任是云平台电子证据存储实体的真实性,并决定该实体权利的处理。使用加密和数字签名的加密方法进行身份认证。与身份实体相比,行为信任更注重可信赖程度。云平台电子证据存储计算系统的授权政策形成了实体^[2]的行为信任模式的基础。为了定义云平台电子证据存储系统中两个实体之间的授权策略,第一步是在它们^[3]之间建立一种信任关系。

我们考虑决定信任的因素。这些参数的值得到的从委托者站点的以前的操作日志,并从由委托站点提供的数据。不准确和模糊性的投入尤其是国防能力和行为模式的主要原因是使用了模糊的方法。由于信任是一个非数字的数量,我们需要通过一些手段进行量化它。模糊治疗帮助我们进行值得信赖的量化。代表团也可以是完整的(完全访问权)、零(无负面权利的权限)或部分(部分转让的访问权限),这意味着决策在一个不精确的设置中需要做的。

模糊逻辑方法是最合适分析这种模糊数据的方法。

法. 在模糊的方法中,不精确的输入模糊化(将清楚的数据转换到模糊集合),然后它通过一个模糊推理过程来验证规则. 我们建议的 FTDM 有两个阶段. 我们使用第一阶段来量化信任值,用第二阶段来进行模糊化过程的模糊推理,进而决定类的代表团和信任级别授权访问的可能性.

2.1 FTDM 的第 1 阶段:模糊信任级别的计算

一个特定网站 S_j 放在其他网站 S_i 上的信任取决于 S_i 先前的行为. 我们考虑了三个输入,即任务成功率(α)、防御能力(β)、行为模式(γ)、信任级的计算(η). 这些输入从以前行为网站的历史抵达. 任务的成功率是先前执行的任务和 S_j 提交给它的总数由现场 S_i 的任务的数量的比率,它是一个数值. 如果没有安全漏洞的报道,我们认为该网站的防御能力还是不错的. 一个网站的防御能力可以基于现有的安全机制发生作用.

典型的网站防御措施是通过隧道、智能数据包的过滤器、状态防火墙、流量监控和入侵检测系统的安装来加密的. 如果在 S_i 上没有安全漏洞,我们可以认为它已经被正确固定. 由于信任是衡量网站的防御能力和安全保证的,所以我们更重视这两个输入^[8].

如果我们收集的过去有关网站的意图和关于安全性的数据,行为模式,即第三个输入可以获得. 当进行量化时,行为模式可以作为代表团授予的未来行动的委派站点的指标. 最后的两个输入在本质上是不精确、模糊的. 由于三分之二的输入是不精确的,同时输出信任级别是一个非数字的值,我们采用模糊逻辑的方法建立委派模型.

虽然他们可能已增加了级别,我们认为这里的三个输入隶属于低、中、高函数. 输入的 3 个隶属函数的符号是:任务成功率的 $\alpha_l, \alpha_m, \alpha_h$, 防御能力的 $\beta_l, \beta_m, \beta_h$ 和行为模式的 $\gamma_l, \gamma_m, \gamma_h$. (在 0~100 分内,模糊输入电平的支持如下:较低是在范围 0~40 之间,中等是在范围 38~70 之间,较高是在 68~100 的范围内).

令 $\eta_{vl}, \eta_l, \eta_m, \eta_h, \eta_{vh}$ 代表输出信任水平的五个等级:非常低,低,中等,高和非常高(0~100 规模,支持的水平非常低为 0~20,低是 18~40,中等是 38~60,高是 58~80,非常高显示 78~100). 我们认为信任计算的精确度越高,数量输出电平越多. 表 1 示出了模糊变量、它们的含量和范围、模糊隶属函数和它们的范围的详细信息.

表 1 模糊分类、成员函数及它们的范围

Fuzzy Variables	Range[a,b]	Levels	Fuzzy Membership Functions	Membership Range or Support of Fuzzy Levels
Task success ratio(α)	[0,100]	1	α_l	$[\alpha_l^{\min}, \alpha_l^{\max}]$
		m	α_m	$[\alpha_m^{\min}, \alpha_m^{\max}]$
		h	α_h	$[\alpha_h^{\min}, \alpha_h^{\max}]$
Defense Capability (β)	[0,100]	1	β_l	$[\beta_l^{\min}, \beta_l^{\max}]$
		m	β_m	$[\beta_m^{\min}, \beta_m^{\max}]$
		h	β_h	$[\beta_h^{\min}, \beta_h^{\max}]$
Behavioral Patterns (γ)	[0,100]	1	γ_l	$[\gamma_l^{\min}, \gamma_l^{\max}]$
		m	γ_m	$[\gamma_m^{\min}, \gamma_m^{\max}]$
		h	γ_h	$[\gamma_h^{\min}, \gamma_h^{\max}]$
Trust Level (η)	[0,100]	vl	η_{vl}	$[\eta_{vl}^{\min}, \eta_{vl}^{\max}]$
		l	η_l	$[\eta_l^{\min}, \eta_l^{\max}]$
		m	η_m	$[\eta_m^{\min}, \eta_m^{\max}]$
		h	η_h	$[\eta_h^{\min}, \eta_h^{\max}]$
		vh	η_{vh}	$[\eta_{vh}^{\min}, \eta_{vh}^{\max}]$

图 2 示出了第一阶段模糊推理过程的基本原理. 形式 T1 的转换: $(\alpha, \beta, \gamma) \rightarrow \eta$. 它显示了三个输入和输出的信任级别. 该计算信任值可能会下降到五个级别中的任何一个.

表 2 示出了第一阶段的模糊推理规则. 我们用复合算子 AND 来使输入和 IMPLY 相关联进而得到相应的输出. 在第一阶段的模糊进程中,用 3 个输入,且每个输入都有三个层次.

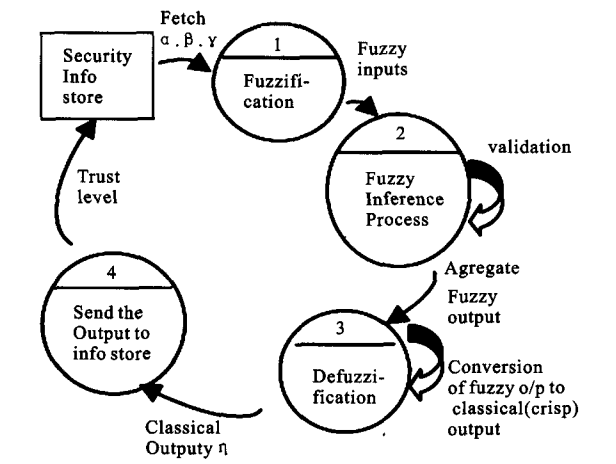


图 2 模糊进程的第一阶段

表 2 信任计算的模糊参考规则

Inputs	Output (Trust)
$(\alpha_1, \beta_1, \gamma_1)$	η_{v1}
$(\alpha_1, \beta_1, \gamma_h)$	η_l
$(\alpha_h, \beta_1, \gamma_m)$	η_l
$(\alpha_m, \beta_m, \gamma_m)$	η_m
$(\alpha_m, \beta_m, \gamma_l)$	η_m
$(\alpha_h, \beta_m, \gamma_l)$	η_m
$(\alpha_1, \beta_h, \gamma_m)$	η_h
$(\alpha_h, \beta_h, \gamma_l)$	η_h
$(\alpha_h, \beta_h, \gamma_h)$	η_{vh}

对于五个范围的输出信任级别,我们使用 5 种不同的可能性,这意味着我们有 27×5 种完全的可能性.除了 135 个输入输出映射,我们去掉了多余和不可行的规则,这将产生 27 个可能的映射.我们得到了 9 个最有可能的规则^[4-5].

图 3 示出了在一定范围内的输入组合是如何产生输出信任级别的.对于示例值,我们已经考虑了在所有的输入范围内和国内模糊推理规则的情况下废除和产生落在非常高水平的输出信任级别.这是一个展示如何废除规则 and 如何生成输出的实例.这些值与规则 9 对应.输入值被映射到一个通过集模糊集合^[11]的输出空间中.

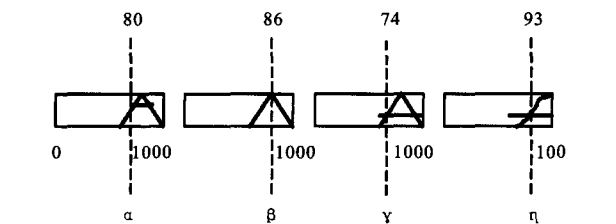


图 3 信任级别的产生

2.2 FTDM 的第二个阶段:模糊代表级别的计算

当最终用户请求实体执行一些操作时,用户授予该实体的代表团.一般情况下,无限代表团是理所当然的.现在的大多数电网系统都授予不受限制的代表团,因为设计、实施和验证受限制的代表团是很难的.无限的代表团可能导致安全性忽视.而放弃一些权利仅仅可以防止任务的完成.因此,有一个限制和可实现的电网代表团^[6]是很有必要的.可实现的代表可以被定义为用户或原理的能力,这种能力通过授予一组有限的权限给其他用户来制定和实施一项政策.受限制的代表团可以在很大程度上减少电网的安全漏洞.

我们根据其中的原因使用下面的形式.代表的方法可用于调用一个方法(m)或执行代表授权的任务.有时委派的权利可能会被用来访问对象(O)或云平台电子证据存储资源.委派权限可以是无界的(∞),或在一段时间(t)内它可能是有界的.在所有这些情况下,委托人必须传递一些凭证作为访问权限的证据.

2.2.1 方法调用的无界委派访问途径—(D_m, ∞)

在这种委派访问权限的类型中,委托方授予访问权限来调用一个代表委托人基础上的方法.这种方法就是一个执行任务的函数响应.这意味着,只有一种方法可以调用,以及对资源的访问只有在这些资源是这些访问的目标时才是可能实现的.对于方法限制的代表团,委托列出了可以调用的方法和向委托传递凭据.考虑到委派的访问是静态的^[7-8],这种委派接入的类型可以通过显式方法枚举、编译器自动化或方法的抽象来实现.在动态授权的情况下,委托需要根据委托的信任度产生委派凭据.

2.2.2 方法调用的委派访问(D_m, t)—有界

对于这种类型的委派访问权限,委托方授予委托的访问权限.这里的唯一区别是,该方法调用受时间界限的限制.

2.2.3 对象的授权访问(D_o, ∞)—无界

这一类限制代表团的方法是十分相似的.对象不过是一种如计算能力、内存或信息的资源.如果对象访问与方法调用没有关系,这意味着对象或资源访问是通过路径来实现的,而不是方法的调用.此类别指定无限时间的对象代表团.由于我们通过信任值到达委派接入,我们可以有一个值得信赖的对象和代表团建议的间接实现方法,如果对象是值得信赖的,那么没这些对象方法调用的凭据是没有必要的.还有一类值得信赖的对象,委派凭据需要的是系

统对象(对象表示主机、调度、存储单元等).

2. 2. 4 对象的授权访问(Do,t)—有界

访问对象的时间依赖代表在云平台电子证据存储中防止重放攻击. 当委托对象的访问基于时间限制时,确定数量的时间作为代表团凭据的时间. 时间限制的代表团的缺点是,我们不能预测执行的操作或任务可能会持续多久,这意味着操作可能会在过期后仍继续委派凭据.

图 4 给出了格式受限制的委派凭据的调用方法、对象、时间限制的访问或所有类别的信息.

Delegator Name	:
Delegator Name	:
Category of Delegation(method/object)	:
Class of Delegated Access Type	:
(bounded/unbounded)	

图 4 云平台电子证据存储中委派访问的证书形式

术语“名称”是指一个有意义的名字,因为我们正考虑在两个站点之间的代表团. 考虑到特定信任级别的云平台电子证据存储实体和委托类(无限或有限)或对象的限制(无界或界)的类似方法,它可以决定是否通过该网站的委派凭据或使用第二个模糊过程. 图 5 给出了第二阶段的模糊推理过程,我们设想此任务的示意图. 其中的转换是 $T2: (\eta, C) \rightarrow D$, 其中 C 是代表团的类.

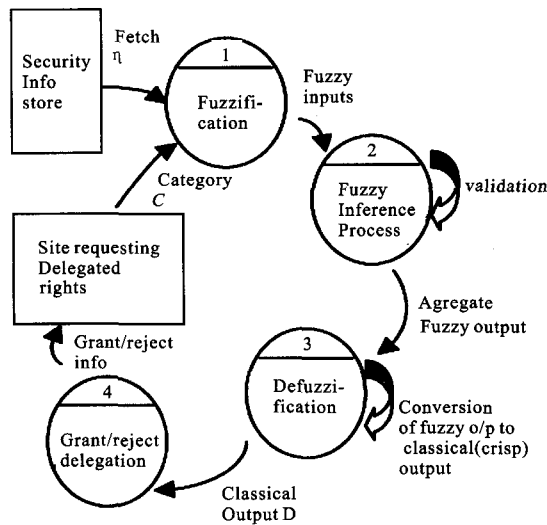


图 5 模糊途径的第二阶段

我们确定了上下文中不同的访问权限. 在四类代表团的限制中,我们属于这一类,因为大多数云平台电子证据存储资源对象与要求较高的信任(无限)有关. 类是对象的限制代表团(有限)、代表团的方法(无限)和方法代表团(有限).

因此,在模糊推理过程的第二阶段,两个输入端分别是可以信任的级别(有非常低、低、中、高和非常高五个水平)和代表团的类别(有四个可能值: 0∞ 、 $0t$ 、 $m\infty$ 、 mt).

第二阶段的结果决定委派的访问(可以是 $\{(Dm,t), (Dm,\infty), (D0,t), (D0,\infty)\}$). 表 3 示出了第二阶段最有可能的规则集. 图 6 显示了如何规定规则集的信任级别. 模糊输入的信任级别和类别的代表团采取 0~100 分. 授予的输出接入的变化也表示为 0~100.

表 3 模糊引用进程的第二个阶段的规范集

Rule No	Rules
1	if $\eta = \eta_l$ and $C = mt$ then $D = Dm, t$
2	if $\eta = \eta_m$ and $C = m\infty$ then $D = Dm, \infty$
3	if $\eta = \eta_h$ and $C = 0t$ then $D = D0, t$
4	if $\eta = \eta_{vh}$ and $C = 0\infty$ then $D = D0, \infty$
5	if $\eta = \eta_l$ and $C = 0\infty$ then $D \neq D0, \infty$
6	if $\eta = \eta_m$ and $C = 0\infty$ then $D \neq D0, \infty$
7	if $\eta = \eta_h$ and $C = 0\infty$ then $D \neq D0, \infty$
8	if $\eta = \eta_m$ and $C = mt$ then $D \neq D0, t$
9	if $\eta = \eta_{vh}$ and $C = m\infty$ then $D \neq Dm, \infty$

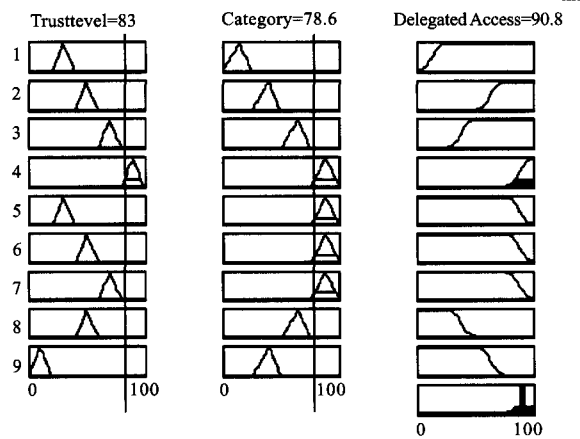


图 6 第二个模糊进程的示例

例如,对于一个非常高的信任级别(83)和对象限制(无限)的代表团类 78.6,代表团的访问是 90.8,这是九条规则所产生输出的综合. 值 90.8 下降到 $\eta = \eta_{vh}$ 范围内,这意味着实体或网站可以授予对象访问路径.

我们可以用类似的方法计算出动态的信任级别,然后将计算值与代表团的类或类型关联起来,并对委托方是否可以授予访问权限(有界或无界)做出决定. 定期更新信任值可以提高电网的安全性,并加

快第二阶段的动态进程。

3 基于 K-means 聚类算法基础上的 CGRS 资源选择算法

3.1 数字云取证问题的分类描述

问题的分类可以根据搜查的电子数据的信息进行分类,快速确定案件的方向。问题的分类并不是一个独立问题,它是数字取证分析系统的一个核心模块,直接影响到基于实务部门数字取证分析系统的快速性、精准性和实效性,能够对数字取证分析系统在电子数据检验鉴定的规范流程的答案筛选和抽取样本特征有很好的指导作用。总的来说,问题的分类任务是给定的问题通过分析然后映射到已定义好的答案类型体系里通过一个或多个类别来确定问题的答案类型,然后针对所有的答案类型形成筛选答案的策略。

目前,对于问题分类的研究可以借鉴文本分类的思想,因此,本文在问题分类算法上采用贝叶斯算法来实现对问题的分类。

系统中数字取证系统中的问题包含七大类分别是,人物类(HUMAN)、地点类(LOCATION)、数字类(NUMBER)、时间类(TIME)、实体类(OBJECT)、描述类(DESCRIBE)和未知类(UNKNOWN)。再对这七种类别进行细分,共形成了六十五个细的类别。

常用于文本分类领域的 Bayes 分类器是一种概率分类器。如下所示:

$$PAnDm = PAnPDmAnPDm = PAnk \cdot \frac{1}{1DmPWkAnTFWkPDm} \quad (1)$$

式中, Dm 表示未知类别的文本; An 表示某一类别; $TF(Wk) - Wk$ 表示在 Dm 中出现的次数; $Wk - Dm$ 中出现的词; $P(An)$ 和 $P(Wk|An)$ 可以从训练集中估计。

对于不同的类别,式(1)的分母不变,如果要选择能使分子最大的类别,即认为是待分类文本的类别。虽然 Unigram 假设在实际文本中是不成立的,但是在实际应用的时候贝叶斯分类器一般情况下都能取得相对较好的结果。

第三步:将文本分到概率最大的那个类别中,比较新文本属于各类的所有概率,问题分类任务完成。

3.2 作业调度决策模块的 CGRS 资源选择算法

资源选择算法是作业调度决策模块的核心。目前,大多数像 Condor^[9]、Silver/Maui^[10]和 KBde 调度采用单点资源选择算法。然而,单一的资源不能满

足我们的 DCG 模型,因为 DCG 资源选择算法必须具有整合多站点的计算能力。

我们的基于聚类的云平台资源选择(CGRS)算法提出了一种新的多站点同步迭代应用程序的资源选择方案。图7给出多站点搜索程序的伪代码。

图7中第3行的第一种方法,称为 GCRClustering();这个方法集合所有可用 GCRs 成为不相交的子集,从而使每个子集内的网络延迟低于它们之间的子集。可用 GCRs 的聚类算法与 CGRS 算法的基础是同样重要的,我们设计了一个复杂的聚类算法的数据挖掘方法^[14],这将在下面的章节中进行阐述。

另一个核心方法是第7行的 MapAndPredict()。该方法采用了性能模型和映射策略的同步迭代应用程序来预测执行时间。由于预测的执行时间直接决定最佳时间表的正确性,所以性能模型和映射策略起着重要的作用。

```

1. BestSchedule Time=Infinite
2. Best GUGCluster=NULL
3. clusters=GCRClustering(Available GCRPool)
4. for (each cluster)
5. rearrange the GCRs in descending order of computational capacity
6. for (GCR Size=1; GCR Size++; GCR Size<=size of (cluster))
7. Current Schedule Time = MapAndPredict (cluster, GCRSize, PerfModel, MapStrategy)
8. if (Current Schedule Time<(Best Schedule Time)
9. BestSchedule Time=Current ScheduleTime
10. Best GUGCluster = Record Result (cluster, GCR Size)
11. endif
12. endfor
13. endfor
14. if (Best GUG Cluster==NULL)
15. Best GUG Cluster = Singlesite Resource Selection (Available GCRPool, Perf Model)
16. return (Best GUG Cluster)

```

图7 基于聚类的云平台资源选择(CGRS)的算法

我们的 CGRS 算法的方法与梯度分离的方法类似,因为它分离了性能模型,并采用多站点选择算法来推广应用的性能。然而,CGRS 算法在三个方面优于 GrADS 的安排搜索程序:

(1)CGRS 算法引入了比使用 GrADS 提出的域名服务更先进的聚类算法。众所周知,DNS 基础上的资源聚类算法是不合理、不准确的^[16]。该 CGRS 算法采用一种新的基于数据挖掘的聚类方法,它提供了了考的资源选择理论。

(2)CGRS 算法的复杂度为 $O(n)$, 其中 n 表示可用的 GCRs, 其前提是 GCRClustering 方法解耦和由一个单独的模块实施定期运行. GrADS 的时间复杂度为 $O(n \times 2S - 1)$, 其中 n 和 s 分别代表可用的 GCRs 和群集数. 该 CGRS 算法需要比梯度更少的时间来完成.

(3)CGRS 算法提供单一站点的调度以防多站点资源选择的无效.

如果我们的 CGRS 算法可以找到多个可用的站点, 我们介绍了利夫卡^[15]推出的回填算法. 回填算法由 SinglesiteResourceSelection() 方法实现, 它已成为大多数单场调度系统的标准.

4 结束语

文中提出的模糊的信任和委托模型(FTDM)采用了以模糊逻辑为基础的方案来确定动态代表团是否可能在一个云平台电子证据存储中; 如果有的话, 又是什么类型的网站心热级别的委派接入. 虽然我们可以有不同的方法解决这个问题, 我们认为两个站点之间的信任水平的决定因素反映了行为模式和网站请求代表团的意图. 两个模糊推理过程的阶段提供访问云平台电子证据存储中的控制问题. 在这个模型中使用规则设计的方法会得出一个有效率的动态代表团的云平台电子证据存储政策的制定. 两个站点之间的可靠关系可以扩展到使云平台电子证据存储中性能自动提高的多站点.

数字取证分析云平台资源的 CGRS 资源选择算法, 并使此算法在数字取证分析平台的可扩展环境中实施. 通过分析和实验结果验证了该方法在聚类计算中能有效降低计算资源占用, 有效降低计算时间, 在处理云数据的过程中能发挥较大的优势.

参考文献:

- [1] Mell P', Grance T. The NIST denition of cloud computing[J]. NationalInstitute of Standards and Technology, 2009, 53(6): 15-18.
- [2] Brodtkin J. GARTNER: Seven cloud—computing security risks. Infoworld, 2008.
- [3] Buyya R, Yeo C S, S Venugopal, et al. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility[J]. Future Generation computer systems, 2009, 25(6): 25-28.
- [4] Hecht S, Cockburn A. The fate of the forest: developers, destroyers, and de-fenders of the Amazon [D]. University Of Chicago Press, 2011.
- [5] Wang C, Wang Q, K REN, et al. Ensuring data storage security in cloud computing[C]//Quality of Service, 2009. IWQoS. 17th International Workshop on IEEE, 2009: 21-27.
- [6] Yilek S, Rescorla E, H. SHACHAM B, et al. SAVAGE. When private keys are public: results from the 2008 debian OpenSSL vulnerability[C]// In Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference[s. l.]: ACM, 2009: 8-10.
- [7] Dingguo feng, Min zhang, Yan zhang, and Zhen xu. The research of cloud security. Journal of Software, 22(1): 2011, 78-79.
- [8] Kandukuri B R, vr paturi, A Rakshit. Cloud security issues[C]// In Services Computing, 2009. SCC'09. IEEE International Conference on, [s. l.]: IEEE, 517520, 2009: 15-16.
- [9] 吴煜祺, 曾国荪, 曾媛. 云计算环境下调度算法的趋势分析[J]. 微电子学与计算机, 2012(09): 10-12.
- [10] 曾诚, 李兵, 何克清. 云计算的栈模型研究[J]. 微电子学与计算机, 2009(08): 7-8.

作者简介:



何月女, (1978—), 博士研究生. 研究方向为分布式计算、云计算、数字取证.



陈明男, (1949—), 博士生导师, 教授. 研究方向为计算智能、分布并行软件.