

虚拟云桌面的访问控制算法研究

朱一茹

(温州商学院 实验实训中心, 浙江 温州 325000)

摘 要: 针对云桌面访问控制的问题, 提出一种基于统计学的虚拟云桌面访问控制算法, 对虚拟云桌面数据进行加密处理并对加密的过程进行分析, 在此基础上, 通过建立描述并发用户负载访问虚拟云桌面的排队论模型, 并分析了基于统计学的虚拟云桌面访问控制算法过程, 从而完成访问控制, 在保证用户访问需求的同时, 最大程度地利用虚拟云桌面资源. 实验证明, 所提访问控制算法能够有效保证虚拟云桌面数据的安全, 提高了访问控制的响应时间, 且访问控制的精度较高.

关键词: 虚拟云桌面; 访问控制; 算法研究

中图分类号: TP393

文献标识码: A

文章编号: 1000—7180(2017)11—0114—05

Research on Access Control Algorithm of Virtual Cloud Desktop

ZHU Yi-ru

(Experimental Training Center, Wenzhou Business College, Wenzhou 325000, China)

Abstract: For the cloud desktop access control problems, put forward a virtual cloud desktop access control algorithm based on statistics, the virtual desktop cloud data encryption processing and the process of the encryption is analyzed, on this basis, through the establishment of virtual cloud desktop access concurrent user load of queuing theory model, and analyses the virtual cloud desktop access control algorithm based on statistical process, so as to complete the access control, in that users access requirements at the same time, using virtual desktop cloud resources to the greatest extent. Experiments show that the proposed access control algorithm can effectively guarantee the safety of the virtual desktop cloud data and improve the response time of the access control, and access control precision is higher.

Key words: virtual cloud desktop; access control; algorithm research

1 引言

计算机互联网技术已被广泛应用于人们生活中的各个领域^[1]. 人们对计算机性能要求的增强, 导致计算机主机更新换代频繁, 从而造成网络资源浪费^[2]. 这种情况下, 云计算技术应运而生, 且快速发展, 尤其是私有云的广泛应用, 云计算的相关虚拟化技术越来越成熟^[3]. 虚拟云桌面是云计算虚拟化技术的重要产物, 虚拟云桌面的发展给用户带来新的挑战. 在虚拟环境下, 用户的虚拟云桌面处于云计算的中心位置, 用户利用瘦客户端与云计算中心进行连接, 从而得到自己的云桌面, 而且在云计算中心,

网络和虚拟交换机是多个用户共用的, 因此需要对用户的瘦客户端进行注册认证, 通过对虚拟云桌面访问控制, 从而保证数据安全^[4]. 目前大多数虚拟云桌面访问控制算法都是通过介绍访问控制理论, 分析虚拟云桌面中访问控制算法的体系框架, 从访问控制模型、基于 ABE 密码体制的访问控制以及云中多租户和虚拟化访问三方面完成虚拟云桌面访问控制^[5], 但这种算法成为当前进行虚拟云桌面访问控制的主要算法^[6], 随着虚拟云桌面的发展应用, 该课题受到相关专家学者的重视. 随着这研究内容的深入, 产生了丰硕的研究成果^[7].

文献[8]提出了一种支持动态授权和文件评价

的访问控制算法. 该算法通过动态授权机制实时监控已授权用户,实现用户之间的相互监督;在此基础上,通过文件评价机制实现动态更新文件解锁阈值. 算法利用 Hash/索引数据库,从而保证文件在系统中的唯一性. 在该算法中,用户授权值会随着其他用户行为动态变化,且用户可以通过对文件进行评价以消除恶意再分享. 但这种算法运行过程较为复杂,难以推广使用. 文献[9]提出了一种基于开放逻辑 R 反驳计算的访问控制算法,首先通过基于精化树描述用户和用户关联,利用基于叶结点用户访问冲突判断,采用开放逻辑 R 反驳计算分析精化树用户关联属性,从而实现访问控制. 但这种算法存在访问控制过程复杂,访问控制的耗时较长的问题. 文献[10]提出了一种基于属性的虚拟云桌面访问控制算法,首先设计了一个带权重的密文策略属性加密方案,并且提出了基于该加密方案的虚拟云桌面的访问控制算法. 通过引入属性权重概念, WCPABE 可以动态反映虚拟云桌面中各个属性的重要程度,增强虚拟云桌面数据拥有者对虚拟云桌面的访问控制;提出了 3 种基于 WCPABE 的访问控制策略;提出了 WCPABE 在虚拟云桌面加密模型,保证对虚拟云桌面访问控制的有效性,增强了虚拟云桌面中数据的安全性,同时解决了多用户私钥分发与管理问题. 但这种算法存在访问控制的准确性不高的问题.

2 虚拟云桌面的访问控制算法研究

2.1 云计算和虚拟桌面技术的研究

虚拟云桌面技术是云计算和虚拟桌面技术相结合的产物,首先对云计算技术和虚拟桌面技术进行介绍,完成对虚拟云桌面的分析.

在云技术技术中,最重要的是服务资源、存储资源、网络资源等汇集组成的资源池. 云计算金属通过对这些资源进行汇总,并统一管理,结合用户需求,为用户提供起所需资源.

根据云计算的发展现状和应用范围,利用云计算定义得出云计算的应用特点.

(1) 按需服务的特点

云计算技术将所有信息资源汇集到资源池进行统一管理,并以用户需求为导向,提供起所需资源,因此云计算技术具有良好的伸缩性.

(2) 虚拟化的应用特点

由于云计算技术提供给用户其所需信息资源,但这些资源往往是云计算进行虚拟划处理后的虚拟资源,需要用户自己下载使用.

(3) 规模宏大的应用特点

在云计算技术中,由于没有屏蔽资源的差异性,因此云计算资源池中的资源规模宏大.

根据上述服务特点,可以将云计算技术分为将软件作为服务、将平台作为服务、将基础设施作为服务三种类型.

NIST 通过独立于供应商的体系结构,利用云计算概念,制定云计算原则,完成云计算参考构架,并将参考构架分为云计算构架中成员及其作用的介绍部分,以及管理和提供资源服务的云服务架构的组成部件部分.

云计算经过最初的概念阶段,再到产品阶段,到如今的普遍应用,其地位在不知不觉间发生重要转变,作用越来越明显. 虚拟云桌面技术作为云计算的新的利用方式,在云计算领域中占据重要地位,在我国云计算行业中的重要地位也深入人心.

虚拟云桌面并不是一个软件,是一个刚兴起的云平台项目,是提供基础设施作为云计算服务的解决方案,由于其出现符合社会发展需要,在很短时间内就得到相关专家学者的重视.

虚拟云平台是一种为所有用户提供其需求的、容易实施的云计算平台的技术. 虚拟云平台是任何单位或组织,都可以使用一些标准化的硬件基础资源.

2.2 虚拟云桌面数据加密技术

为保证访问控制的有效性,保证虚拟云桌面数据的安全性,首先对虚拟云桌面数据进行加密处理.

考虑报虚拟云桌面安全性问题,本文通过制定访问策略,构建访问控制算法的方式来保证服务的安全性. 由于对密钥安全性的考虑,虚拟云桌面中数据的所有者利用 CP-ABE 算法对访问者的属性进行加密. 定义 $Encrypt()$ 表示加密函数, T 表示虚拟云桌面中文件 F 的访问结构控制树,则通过加密函数实现对该虚拟云桌面中数据的加密:

$$CT = Encrypt(PK, \{K_f, K_{sign}/K_{verify}\}, T) \quad (1)$$

式中, CT 表示虚拟云桌面中数据加密函数的运行结果即虚拟云桌面中数据生成的密文,以虚拟云桌面中数据所有者定义的主密钥和分析得到用户的属性集及其子集 S ,可以利用函数 $KeyGen()$ 以用户的实际属性情况为依据,从而生成对应的虚拟云桌面用户密钥:

$$SK_i = KeyGen(MK, S_i) \quad (2)$$

利用公钥 K^+ 将生成的密钥 SK_i 发放给用户,并保证其安全性.

$Decrypt()$ 函数是与 $Encrypt()$ 函数对应的虚拟云桌面数据的解密函数, 当访问者对加密密文进行访问时, 对访问者手中的密钥与加密密文进行匹配, 通过解密函数得到解密密钥和验证密钥, 通过将访问者提供的签名密钥 $E(F)$ 与数据的解密密钥进行核实, 从而比较匹配, 当完成匹配时, 用户获取加密密文信息资源, 实现利用, 否则, 用户返回登录界面, 从而完成信息读取过程。

访问控制策略是意向使用权限管理策略, 虚拟云桌面数据的拥有者可以将数据的使用权限分配给其他用户, 也可以根据实际情况对其他用户的使用权限进行管理。

从上述读写权限过程可以看出, 虚拟云桌面数据服务中是以 K_{sign} 和 K_{verify} 为依据进行提供数据权限访问操作, 用户利用操作权限, 实现对虚拟云桌面数据的操作, 实现对虚拟云桌面数据的加密, 其安全性主要体现在:

(1) 基于数据安全性考虑, 本文中, 将数据管理权限交给虚拟云桌面数据的拥有者, 虚拟云桌面数据拥有者对虚拟云桌面数据进行管理, 从而保证虚拟云桌面数据的安全。

(2) 为保证虚拟云桌面数据的机密性, 在加密模型中, 在客户端实现对虚拟云桌面数据的加密、解密操作, 通过这种客户端到客户端的数据加解密方法, 保证了虚拟云桌面数据传输以及存储的可靠性。并且, 通过 K_{sign} 保证了数据的完整性。

2.3 基于统计学的虚拟云桌面访问控制算法

为了防止多人同时对虚拟云桌面进行访问导致的碰撞, 本文首先建立并发多媒体负载访问控制模型。在对虚拟云桌面发送的访问请求较多时, 通过这些请求进行回击, 形成虚拟云桌面的访问请求流 stream, 以访问请求到达的时间为依据, 依次进行虚拟云桌面的访问, 形成并发多媒体负载。每个用户开始对虚拟云桌面访问时刻服从泊松分布。当 stream 中同时发送请求的用户过多时, 可认为到达虚拟云桌面的访问请求时间间隔服从参数 λ 的指数分布, 其中 λ 表示访问请求到达虚拟云桌面的平均速率, 当 stream 由 N 个同时访问的用户组成时:

$$\lambda = \frac{N}{T} \quad (3)$$

设定 T_{serv} 表示虚拟云桌面的访问服务时间, 其服从指数分布 μ 的独立同分布, 其中, μ 表示虚拟云桌面处理访问请求的平均速度, 则有:

$$\mu = \frac{1}{E(T_{\text{serv}})} \quad (4)$$

当 stream 中同时发送请求的用户数量过多时, 需要使参数 λ 足够大, 保证虚拟云桌面处理用户访问请求的速度。上述过程可以用 $M/M/1$ 的排队模型进行描述。

当用户的访问请求到达虚拟云桌面时, 如果虚拟云桌面此时没有其他访问需求, 则可以立刻得到访问服务, 否则, 将用户的访问请求放在等待队列的尾部进行排队, 直到得到访问服务。虚拟云桌面的响应时间是指用户发送请求到完成服务之间的时间, 其主要由等待时间和服务时间两部分组成。

将同时发送访问请求的用户汇集为 stream, 为了保证 stream 中所有用户需求都得到满足, 要保证 stream 中所有用户访问请求的响应时间超过 d 的比例小于 P 即可。

根据排队理论, stream 中对虚拟云桌面的访问请求的到达速率及虚拟云桌面的平均服务时间共同决定用户对虚拟云桌面的访问请求响应时间概率分布, 因此, 可以通过对虚拟云桌面的访问请求响应时间大于截止期限 d 的统计概率与 stream 中并发多媒体应用数量 N 的关系的推导, 完成基于统计学的虚拟云桌面访问控制算法。

P_n 表示虚拟云桌面的访问请求中 $M/M/1$ 排队模型的稳定状态概率, 其代表的是排队序列中用户发送虚拟云桌面访问请求的数量为 n 的概率, 根据稳定状态流量等式, 进行递归计算得到 P_n :

$$\mu = \frac{1}{E(T_{\text{serv}})} dP_n = (1 - \rho)\rho^n, \quad n = 0, 1, \dots \quad (5)$$

式中, $\rho = \frac{\lambda}{m\mu}$, $m\mu$ 表示访问请求处理的平均速度。则请求响应时间 S 可以表示为

$$S = \sum_{k=1}^{L^a} D_k \quad (6)$$

式中, L^a 表示用户发送的请求达到虚拟云桌面时其前面的访问请求数量; D_k 表示其中第 k 个访问请求需要的服务时间。由于 L^a 和 D_k 相互独立, 利用基于 L^a 的条件概率, 计算关于虚拟云桌面访问请求的响应时间 S 大于 d 的统计概率:

$$\begin{aligned} P(S > d) &= P\left(\sum_{k=1}^{L^a+1} D_k > d\right) \\ &= \sum_{n=0}^{\infty} P\left(\sum_{k=1}^{n+1} D_k > d\right) p(L^a = n) \end{aligned} \quad (7)$$

根据 PASTA 定理, 求得 P_n 为

$$P(L^a = n) = P_n = (1 - \rho)\rho^n \quad (8)$$

将上式代入式(7),并根据 $\sum_{k=1}^{n+1} D_k$ 实际是 $Erlang-(n+1)$ 分布,得到:

$$P(S > d) = \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{(m\mu d)^k}{k} e^{-m\mu d} (1-\rho)\rho^n = e^{-m\mu(1-\rho)d}, d > 0 \tag{9}$$

将式(3)~(5)代入式(9)得虚拟云桌面的访问请求响应时间大于截止期限 d 的统计概率与 $stream$ 中同时发送访问请求的用户数量 N 的关系:

$$P_N(S > d) = e^{(\frac{N}{T-E(T_{serv})})d} \tag{10}$$

根据上式可得到基于统计学的虚拟云桌面访问控制算法.虚拟云桌面为了满足 $stream$ 中的用户需求:响应时间大于 d 的访问请求的比例小 P ,从而保证 $stream$ 中同时发送访问请求的用户数量 N 满足: $P_N(S > d) < P$.

3 实验结果与分析

为了证明本文提出的基于统计学的虚拟云桌面访问控制算法的有效性和可行性,以 Intel P4 2G 处理器为硬件环境, MATLAB2008a 为平台,通过模拟算法实际运行,比较本文提出的虚拟云桌面访问控制算法和文献[8]、文献[9]所提虚拟云桌面访问控制算法实际运行情况,从而完成本次实验.

首先对比三种虚拟云桌面访问控制算法的能耗,通过运行这三种算法,设能耗的单位为焦,其计算过程如式(11)所示.

$$Q = IAT \tag{11}$$

式中, Q 表示算法运行能耗; A 表示电源电压; I 表示运行电流; T 表示运行时间.通过计算,得到三种算法的能耗对比,对比结果如图1所示.

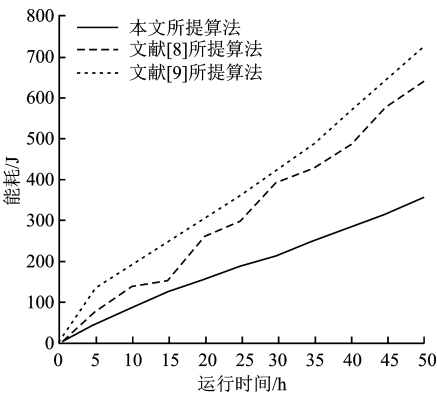


图1 三种算法能耗对比

通过图1可以看出,本文所提算法的运行能耗较低,由于本文涉及的算法过程较为简单,因此需要的能耗较少,比较节能.

对三种算法的响应速度进行对比,为保证实验的准确性,进行了500次实验,得到响应速度对比如图2所示.

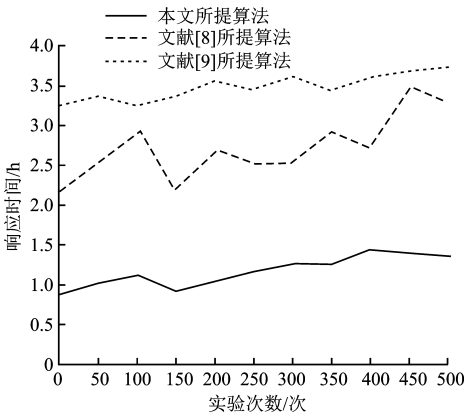


图2 三种算法响应时间对比

通过图2可以看出,本文所提算法响应时间较短,说明本文所提响应速度快,因此对虚拟运作面的访问控制速度快,由于本文所提算法建立了用户负载访问虚拟云桌面的排队论模型,防止多用户同时访问给虚拟云桌面带来的负担,从而提高了算法的响应速度.

最后对三种访问控制算法访问控制的准确性进行对比,为保证实验的准确度,进行了500次实验,其准确度(%)的计算方法如下所示.

$$d = \frac{S'}{S} \times 100\% \tag{12}$$

式中, S 表示访问控制的总次数, S' 表示访问控制准确的次数,通过实验及计算,得到三种算法访问准确度对比,对比结果如图3所示.

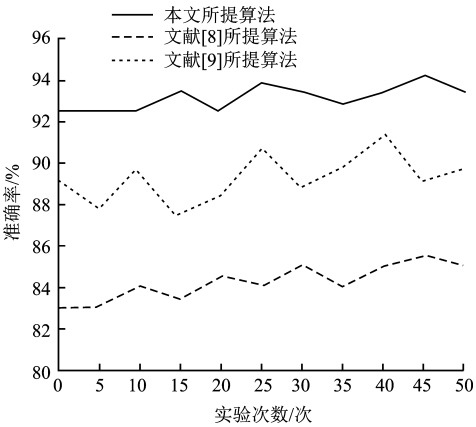


图3 三种访问控制算法访问控制准确度对比

根据图3可以看出,本文所提访问控制算法的控制的准确度较高,由于本文对虚拟云桌面进行分析,提出的访问控制算法适在虚拟云桌面环境下使

用. 综上所述,本文所提算法响应速度快,控制效率较高,由于能耗较低,所以控制成本较低,由于控制的准确度高,说明本文所提算法控制的效果较好,因此具有较强的使用价值.

4 结束语

虚拟云桌面作为云计算技术的重要应用方案,随着云计算技术的发展,特别是私有云技术的应用,对虚拟云桌面的管理越来越受到人们重视. 访问控制是对虚拟云平台管理的重要内容. 针对传统虚拟云桌面访问控制算法存在的不足,本文提出一种基于统计学的虚拟云桌面访问控制算法,实验证明,本文所提算法的访问控制准确度较高,实用性较强.

参考文献:

[1] 马洁. 基于 AWS 的访问控制系统设计与实现[J]. 电子设计工程,2016,24(6):182-184.

[2] 于会松,孟照旭,黄华晔,等. 基于映射的角色访问控制模型的设计与实现[J]. 计算机仿真,2016,33(4):292-295.

[3] 周明快. 基于 CP-ABE 的云计算改进属性加密安全访问控制策略设计[J]. 计算机测量与控制,2015,23(1):

297-299.

[4] 黄正鹏. 基于分布式 B 树编译的高效并发访问控制算法[J]. 科技通报,2015,31(8):81-83.

[5] 王廷,喻建平,黄敏强. 云存储访问控制中的快速属性基加密方案[J]. 科学技术与工程,2017,17(1):54-60.

[6] 张欣晨,杨庚. Hadoop 环境中基于属性和定长密文的访问控制方法[J]. 计算机工程与应用,2015,51(23):87-93.

[7] 冯朝胜,秦志光,袁丁,等. 云计算环境下访问控制关键技术[J]. 电子学报,2015,43(2):312-319.

[8] 张悦,郑东,张应辉. 支持动态授权和文件评价的访问控制机制[J]. 计算机应用,2015,35(4):964-967.

[9] 吴迎红,黄皓,吕庆伟,等. 基于开放逻辑 R 反驳计算的访问控制策略精化[J]. 软件学报,2015,26(6):1534-1556.

[10] 黄保华,贾丰玮,王添晶. 云存储平台下基于属性的数据库访问控制策略[J]. 计算机科学,2016,43(3):167-173.

作者简介:

朱一茹 女,(1980-),助理实验师. 研究方向为计算机信息管理. E-mail: xuexiao0528@163. com.

(上接第 113 页)

[5] Matthew J. Gadlage, Ronald D. Schrimpf. et al. Single event transient pulse widths in digital microcircuits [J]. IEEE TRANSACTIONS ON NUCLEAR SCIENCE, 2004,51(6):3285-3290.

[6] SAPONARAS, FANUCCIL, TONARELLIM , et al. Radiation to lerant SpaceWire router for satellite on board networking[J]. IEEE Aerospace and Electronic Systems Magazine, 2007, 22(5):3-12.

作者简介:

刘 欢 女,(1983-),硕士,高级工程师. 研究方向为 IC 设计.

陈卫国 男,(1983-),博士,高级工程师. 研究方向为 IC 设计.

王剑峰 男,(1971-),硕士,研究员,副总工程师. 研究方向为 IC 设计、Soc 设计.

吴龙胜(通讯作者) 男,(1968-),博士,总工程师. 研究方向为 IC 设计、Soc 设计. E-mail: wls771@163. com.