



面向云计算的网络体系结构下数据传输机制

摘要

分析目前云计算架构下的传输机制,针对网络传输机制中缺少对链路上的任务需求的耦合相关性,提出未来面向云计算的网络体系结构下数据传输机制,分别从网络传输延迟、传输可靠性和云节点存储安全性进行研究,并针对每个瓶颈提出相应的修改方法,从而构建了一个支持不同服务质量需求的云架构,该架构支持现有的网络异构融合,满足可控可管可扩展等需求,适用于新型网络通信信息基础设施。

关键词

云计算;网络架构;TCP/IP;网络时延

中图分类号 TP316

文献标志码 A

收稿日期 2014-09-23

资助项目 广东省教育科学“十二五”规划信息技术专项(13JSN060)

作者简介

姚光伟,男,讲师,主要从事计算机实验及物理模拟实验方向研究.yaogw2008@126.com

¹ 韩山师范学院 潮州师范分院,潮州,521000

0 引言

云计算是一种灵活的 IT 资源组织和提供方式,它能够对大规模的服务器资源进行灵活的调配,快速响应众多用户的并发请求或作业.许多大型跨国企业已经着手将自己的业务迁移到云计算平台之上^[1].到目前为止,谷歌、IBM、亚马逊、阿里巴巴等全球知名公司都相继在自己的数据中心建设相应的云计算中心,并把它们作为未来主要的发展战略,而新兴的互联网公司则考虑将目光转向如亚马逊、Dropbox 等提供的公有云上处理自己的业务.云计算的高可用性、易扩展性和服务代价小等优点,很快就获得了广大 IT 企业用户的青睐.但是随着云计算的快速发展,伴随着移动互联网和大数据的发展,必然对数据中心网络提出了更高的要求.

在面向云计算的网络体系结构数据传输机制中,各种软硬件设施及各网络节点之间的资源传输机制由应用服务运营商和网络运营提供商共同协调运行,而当前应用最广泛的 TCP/IP 协议模式,其用户终端仅仅能满足为网络本身提供尽力而为的数据转发服务,这种以终端互联和资源共享为代表的网络设计模式在一定程度上已阻碍了云计算的发展.随着云计算技术的推广应用及社会对互联网依赖程度的日益增强,互联网接入方式和网络功能定位将产生前所未有的改变,传统的网络传输机制在实现云计算的细粒度化管理、可靠性任务调度以及安全可控性等方面,无法从根本上保证云架构下网络的互联性、高质量、可融合及异构、可信、可管、可扩展等高等级需求.

本文在分析当前互联网体系架构存在的根本性问题的基础上,对现有的网络技术的局限性和云计算的推广实现存在的瓶颈进行了系统调研,对比分析了网络延时、传输可靠性、节点的安全存储对云计算环境下网络传输的制约作用,并进行改进设计,提出了未来面向云计算的网络体系结构下的数据传输机制.

1 云平台网络架构的设计要求

云计算可根据用户作业需求,将任务资源实时动态地分配到相关计算资源节点上,使用户无需再购买昂贵的软硬件设施,转而采用租赁的方式来获取相应的应用和资源使用权.计算资源及服务按照需求迅速提供给用户,从而实现用户实时按需、便捷地访问共享资源池(如计算设施、存储设备、应用程序等)的计算模式^[2].但在云计算环

境中各个角色要求的侧重点各不相同,网络运营商机期望网络平台具备高效的传输机制、良好的可靠性和健壮性,而网络用户则希望能够更加灵活地定制自己的业务,实现网络的自适应应用,如对于金融股票等要求实时快速响应,而对于邮件发送则允许延迟等,应用提供商则希望网络平台能够确保信息安全,实施有效监管.网络体系架构模式如图 1 所示.

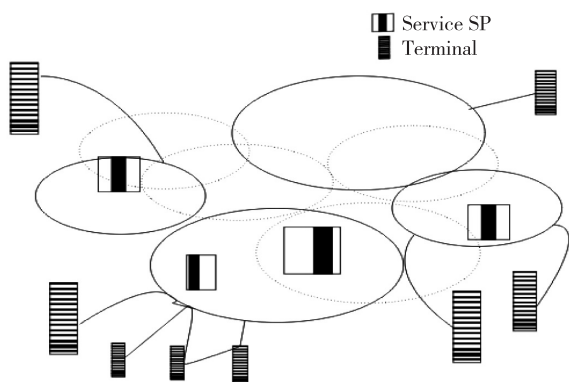


图 1 云平台网络体系架构

Fig. 1 Process diagram of network architecture towards cloud computing

网络运营商机期望能够充分、实时地获取各节点的网络传输状况,如云节点负载率、路由协议收敛性等网络参数和网络业务运行数据,并在此基础上有针对性地节点数据流进行调节和引导,以充分发挥云节点基础设施及各节点链路上的利用率^[2];确保应用提供商和网络用户在内的网络参与者的行为始终处于可控、可管和可信的状态,使网络活动中的各个角色能够有效分工,任何操作都不影响其他业务的正常运转.

用户希望能够更加灵活、方便地为自己定制一套个性化的服务,包括业务操作、用户访问响应、上传/下载带宽、数据包路径要求、数据加密等级和云端的数据安全等一系列在直观上就能够体验到的指标参数,以使个性化这一真正的客户价值属性得到充分满足.

应用提供商最关心的是云节点信息存储的安全性,希望在便捷、实时、准确地获取网络运行状况数据的基础上,实现对网络服务资源的存储安全管理,以保证数据被合法的用户使用,同时达到对网络环境参数进行灵活调整、针对性定制及针对不同权限的用户在数据和密文安全条件下被合法访问利用.

未来面向云计算的网络传输机制不仅应满足可控、可管、可扩展和可信任的要求,而且还应充分考

虑延迟、可靠性、安全可控性的要求.因此,未来的数据传输机制应当遵循以下几个原则:1) 传输可靠性原则.随着下一代互联网建设及发展,高速长距离网络将成为其主流网络,但数据传输过程还是不可避免地存在着诸如随机的网络延时、数据包丢失等问题,这是急需解决的问题.2) 网络自适应原则.网络用户期待可以随心所欲地定制满足自身需求的业务,以实现网络的自适应.3) 模型安全性原则.云计算的数据在传输过程的安全性必须重视,而且也会影响到云技术的推广,特别是针对内部的一些机密性文件数据,如果泄密,影响极其严重.

2 云平台的传输可靠性

传输延时是研究网络传输机制必须面对的问题.文献[3-4]提出地理位置相近的网络设备拥有相似的网络时延.文献[5]研究了网络中某些地理区域之内节点之间 RTT(往返时延)与物理距离之间的约束性,但缺乏对跨区域节点之间 RTT 与物理距离关系的研究.本文通过 TSLNN(带有时间戳的线性神经网络)进行网络延时预测,利用时间戳技术来捕获从传感器发送的数据包到接收器获取的数据包之间的时间间隔,并标记该时间间隔为网络延时 τ .图 2 为理想状态下的多线程输入、单线程输出并在线程输出端增设线性网络结构作为延时探测器的流程.

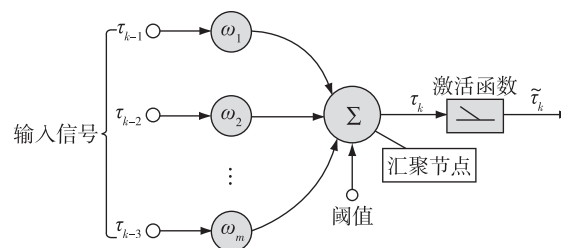


图 2 基于云平台多线程输入的线性网络结构流程

Fig. 2 Process diagram of network architecture based on multithreading input under cloud computing

云端传输延时的探测步骤:首先,通过模拟云平台中网络捕获的 3 个连续采样周期的实际网络延时值 λ_{k-1} 、 λ_{k-2} 和 λ_{k-3} ,并将其作为多线程网络的输入,接着,预测这 3 个期望的采集样品的网络延时值,并获取延时期望值 $\hat{\lambda}_k$,多线程网络输入的线性网络的输出如下:

$$\lambda_k = \alpha_1 \lambda_{k-2} + \alpha_3 \lambda_{k-3} + \delta, \quad (1)$$

其中, α_i 为权值, δ 为阈值,其激活函数采用线性函数.

由于云计算的资源分布及实际环境错综复杂,不同线路在不同时刻的网络负载都存在不可预期的变化,且每个节点配置、容量和吞吐量等性能也不尽相同,因此,为适应复杂网络的变化,必须使云平台上检测到的网络延时值更接近现场的网络状况.当时间戳技术捕获到一个最新的网络延时值时,其对应节点上的阈值都会实时动态做相应的更新.

云平台网络采用训练 wid-row-hoff 算法学习规则.取样本为 $\{p(k-1), \lambda_k\}$, 其中, 向量 $p(k-1) = [\lambda_{k-1}, \lambda_{k-2}, \lambda_{k-3}]^T$ 为云平台网络的输入, λ_k 为期望的相应输出, 而取实际输出的值与期望值的差为训练误差 $e^2(k)$, 其相应的方差为

$$e^2(k) = [\hat{\lambda}_k - \lambda_k]^2, \quad (2)$$

参数 k 是第 k 个采样轮回周期. 由式(2) 可得, 训练误差的方差的梯度为

$$\frac{\gamma e^2(k)}{\gamma \alpha_m(k)} = 2e(k) \frac{\gamma e(k)}{\gamma \alpha_m(k)} = -2\lambda_{k-m} e(k), \quad (3)$$

$$\frac{\gamma e^2(k)}{\gamma \delta(k)} = 2e(k) \frac{\gamma e(k)}{\gamma \delta(k)} = -2e(k), \quad (4)$$

其中, m 为采样数, $m = 1, 2, 3, \dots$. 基于近似梯度下降法, 相应的权值向量 $\mathbf{M}(k) = [\lambda_1(k), \lambda_2(k), \lambda_3(k)]^T$ 和阈值 $\delta(k)$ 分别调整为

$$\mathbf{M}(k) = \mathbf{M}(k-1) + 2\alpha e(k) \mathbf{p}(k-1), \quad (5)$$

$$\delta(k) = \delta(k-1) + 2\alpha e(k), \quad (6)$$

式中, $\delta(k)$ 为第 k 个采样周期的阈值.

3 网络自适应性

在云计算服务中, 用户作业需求呈现多样性. 不同的业务对于网络的服务质量要求也是各不相同的, 这些需求包括分组丢失率、传输时延、传输可靠性等. 例如, 股票、基金等业务对实时性、可靠性要求就相对苛刻, 反之, 如 E-mail 方面的业务则可接受适当的传输时延和极短暂的节点故障. 因此, 当用户提出多样化需求时, 网络节点应能够迅速响应并自动给出有效的资源分配方案, 以确保节点的自适应性.

3.1 问题假设

假设模型中有 P 个虚拟网络 $A_{\text{NET}} = \{a_{\text{net}}(1), a_{\text{net}}(2), \dots, a_{\text{net}}(n)\}$, 同时向有限资源的 InP 请求资源分配, 设资源分配概率矩阵 $\mathbf{P}_{mn} = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & & \vdots \\ p_{m1} & \cdots & p_{mn} \end{pmatrix}$, p_{ij} 表示虚拟网 $a_{\text{net}}(i)$ 接入资源 s_i 的

概率, 且 $\sum_{i=1}^m p_{ij} = 1$, 因此当满足下面条件时, 表示 InP 有足够的资源分配给 A_{NET} :

$$\sum_{j=1}^p p_{ij} \times t_j \leq r_i, \quad \sum_{i=1}^m \sum_{j=0}^p p_{ij} \times t_j \leq \sum_{i=0}^m S_i, \quad (7)$$

t_j 为 $a_{\text{net}}(i)$ 的资源需求量, r_i 为物理链路 l_i 对 InP 的重要程度.

在云平台的资源传输机制中, 每一物理链路上可能承载着多种不同应用的资源数据及不同虚拟链路, 同一虚拟链路也可能承载不同应用的资源数, 且每条虚拟链路上的资源利用率也不尽相同, 因此, 需要分析 InP 与虚拟网络之间的资源映射问题, 并根据业务类型把虚拟网划分为不同的服务类型和方案, 以提高用户的满意度.

假设用 n_i 表示链路 l_i 上的节点数, l_i 表示链路的长度, C_{iq} 表示 l_i 上第 q 个节点的处理能力, 令等效时延 $T_{\text{EDi}} = \sum_{q=2}^{n_i} \left[\frac{\alpha}{bl_i} + \beta C_{iq} \right]$, 其中 α, β 是参照调节因子, 虚拟网络运营商可参照网络运营的实际状况设定链路距离与相对应节点处理能力的比例权值. 本文为每个物理链路定义了另一个权重因子来表示链路的质量, 则 $w_i = T_{\text{EDi}} / \sum_i T_{\text{EDi}}$, 向量 $\mathbf{W} = \{w_1, w_2, w_3, \dots, w_n\}$ 表示每条链路的质量权重.

3.2 自适应传输

当物理网络资源供过于求时, 即满足式(7) 时, 它可以接受一定范围的时延, 但是对业务传递的可靠性要求非常高, 这时分组丢失率、误码率将是其最重要的参考指标, 则此类型业务的效用函数为

$$U^j(w_i, s^j) = \sum_{i=1}^m \left\{ w_i \exp(s_i^j) - s_i^j \sum_{q=2}^{n_i} \left[\frac{\alpha}{bl_i} + \beta C_{iq} \right] \right\}. \quad (8)$$

视频流媒体等服务对分组丢失、时延就没有这么高的要求. 如用户在线观看世界杯直播, 出现延迟 1 s 到达或传输过程中丢失一帧图像, 并不会给观众带来任何影响, 但此类业务处理应具有大流量、高速、实时等特性, 所以对于视频数据流的传输一般要求较高的带宽, 其业务处理效用函数为

$$U^j(w_i, s^j) = \sum_{i=1}^m \left\{ w_i \exp(s^k) + s_i^j lb - lbs_i^j \sum_{q=2}^{n_i} \left[\frac{\alpha}{bl_i} + \beta C_{iq} \right] \right\}, \quad (9)$$

l 为参照调节因子, b 为传输链路上的权值比重. 虚拟网络运营商可参照网络运营的实际状况设定链路距离与相对应节点处理能力的比例权值.

4 云模型的安全性

保证数据传输的机密性也是云环境下数据传输过程中亟待解决的问题,支持不同用户访问不同级别权限的云数据模型已成为眼下研究的重点.为了实现数据在密文安全条件下被合法用户访问利用,现有的密钥管理主要有文献[6-7]提出的不同云计算环境中多用户访问控制模型,为了保证数据机密性与可用性,模型以数据拥有者作为用户访问请求处理的中心节点,这势必要求数据拥有者必须保持在线,当某一节点的用户访问量急增时,资源所在的链路及易导致拥塞,甚至整个网络瘫痪等负面影响. Yang^[8]提出了以云服务器为中心节点、支持多用户访问的可搜索加密方案,但该方案中所有用户具有相同的访问权限和解密密钥,对于用户的动态变化管理复杂.为避免用户动态变化而对数据重复加密,实现不同的访问权限的多用户能够高效、灵活解决数据传输过程动态用户的密钥管理问题,本文采用 UACL 和 UDACM 技术,利用云服务器与数据拥有者的自协调能力实现用户访问权限的逻辑控制和密钥的有效管理,减轻了系统动态用户密钥管理的复杂度.

首先云端服务器对每个数据块 D_i , 提取其关键词 k_i 并根据统计公式计算每个关键词相关度 R_i . 关键词加密检索算法分为 4 个部分:

1) 关键词的提取及相关度的计算. 首先数据拥有者对云节点上捕获到的每个数据包提取关键词. 其中, D_i 表示明文数据包值, 取标识头作为关键词并做相应统计, 取 D_{len} 为数据 D_i 的长度, 则

$$R_i(k_i, D_{len}) = \frac{1}{D_{len}}(1 + \ln f),$$

其中 f 为关键词 k_i 在数据 D 中的频率.

2) 索引生成算法 E_{kwenc} . 数据拥有者选取函数 $F: \{0, 1\}^* \rightarrow G_1$, 将原始明文映射到群 G_1 相应离散点上, 该过程是可逆的. 随机选取整数对每个 k 计算 $r_i F(k_i)$, 并利用主密钥 e_0 对生成元 P 加密生成 $r_i e_0 P$, 密文对 $(r_i F(k_i), r_i e_0 P)$ 即为密文索引, 利用保序加密算法计算 $E_{opc}(R_i, k_{opc})$ 作为密文索引属性^[9].

3) 询问门限生成算法 E_{query} . 用户 U_i 利用密钥 d_{U_i} 将所要搜索的关键词 k_i 进行加密, 计算得到 $d_{U_i} F(k_i)$, 随机选择整数 l 并计算 $ld_{U_i} F(k_i)$, 同时对生成元 P 计算 lP , 密文对 $(ld_{U_i} F(k_i), lP)$ 即为密文查询门限.

4) 关键词检索. 云平台服务器收到 M_{UC} 之后, 根

据 UACL 判定用户 U_i 是否为获得相应权限的 U_{ser} , 若具备相应访问门限, 则对拥有相应权限的 U_{ser} 对进行代理加密运算: $E_{proxy} = ld_{U_i} d_{U_i} F(k_i') = le_i' d_i' d_{U_i} F(k_i')$, 并确定该 U_i 具备访问权限的数据范围, 在可访问的权限范围内通过双线性进行计算并验证等式 $e(le_i' d_i' d_{U_i} F(k_i'), r_i e_0 P) = e(r_i F(k_i), lP)$ 的可行性. 由双线性的性质可知, 若 $k_i' = k_i$ 则有: $e(le_i' d_i' d_{U_i} F(k_i'), r_i e_0 P) = e(F(k_i'), P)^{le_i' d_i' d_{U_i} e_0 r_i} = e(F(k_i'), P)^{l r_i} = e(r_i F(k_i), lP)$. 对所有匹配数据加密后的关键词相关度密文 $E_{opc}(R_i, k_{opc})$ 进行比较, 得到相关度最大的前 k 项作为检索结果.

云端服务对明文数据根据关键词采用不同加密算法加密, 形成用户访问控制列表 (User Access Control List, UACL) 和用户-数据访问控制矩阵 (User-Data Access Control Matrix, UDACM), 并将加密结果及 UACL、UDACM 发送给数据使用者. 当用户向云端发出检索请求, 云端则利用用户访问控制列表、数据访问控制矩阵算法搜寻对应具备访问权限的 U_{ser} 是否拥有匹配的数据, 并对比关键词匹配相似度最大的数据 k 项值. 该算法可有效解决针对不同权限用户发放不同等级的密钥, 使用户按照数据拥有者对用户和数据的逻辑划分进行访问, 并大大减轻了数据拥有者的计算负担.

5 数值仿真实验

5.1 数值实验

分别从粤东不同地点获取 3 个云节点组成转发节点集进行数值实验. 假设随机的云节点链路上数据传输的成功率原始值为 $\{p_{s1}, p_{s2}, p_{s3}\} = \{0.8, 0.6, 0.4\}$, $\{p_{D1}, p_{D2}, p_{D3}\} = \{0.8, 0.6, 0.4\}$. 取 3 个连续传输方式下初始化数据包数目 ($m = 3$), 并记录其对应冗余码数据包数目 ($M_0 = M = 5$). 为评估 3 种传输方式的抗干扰特性, 以 $S-R_1$ 链路为例, 改变该链路包丢失率 $e = 1 - p_{s1}$, 并观察链路质量对 3 种传输方式下传输延迟、传输可靠性及模型安全性的影响.

5.2 仿真实验

本文设置在同一参数情况下, 用 Matlab 进行蒙特卡罗仿真实验, 源节点发送 10 000 次原始数据包, 通过目的节点统计捕获成功解编码的次数验证面向云计算的网络体系结构下数据传输机制. 在图 3 中, 不难发现, 经过优化后的云环境下网络可更准确地选择节点平均剩余能量较多且能耗较低的路径, 有

利于均衡利用网络节点能量,进而降低传输延时性能.由仿真实验还可获知传输可靠性略逊于上述的理论分析,这是由于做理论分析时,考虑编码对仿真实验的影响不大,因此并未充分考虑目的节点收到的编码数据包的编码之间的线性相关性.

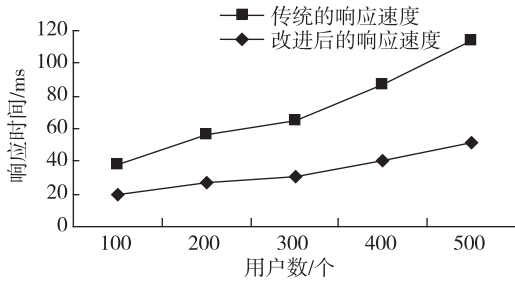


图3 云平台网络的响应速度对比
Fig. 3 Comparison of response time

图4是可靠性数据交换性能测试结果.实验结果表明,网络传输可靠性随时延的增加而提高,超过一定值后性能改善效果趋于稳定.增加 M 意味需发送更多数据包,这会消耗更多的网络资源,在选择最低通信能耗路径作为最优路径的过程中,改进的算法计算出了路径的实际能耗,可获得比原算法更准确的最优路径.

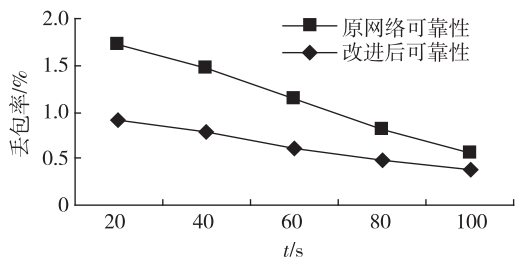


图4 网络可靠性比较
Fig. 4 Comparison of network reliability

图5反映了模型中每次用户动态变化密钥更新的数目.文献[9-10]为保证数据安全性,当用户发生

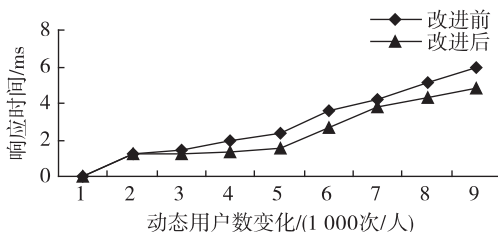


图5 模型安全性比较
Fig. 5 Comparison of model's security

动态变化时需要更新与该用户相关的所有用户的密钥,因此随用户动态变化次数逐渐递增时,节点密钥管理复杂、效率低下.由图5可知,本文设计的网络体系架构中,对于用户属性的变更仅仅需更新其对应的用户访问控制列表中相应代理加解密密钥即可,因此各云节点密钥管理将更加灵活高效.

6 下一步研究计划

本文主要对面向云计算的网络体系结构下数据传输机制进行深入分析,通过仿真实验对这些协议做相应的改进分析,证明了改进后云平台网络传输具有良好效果.但在工作中依然还有一些不足,有待进一步研究:

1) 用户友好性和稳定性.通过协议分析及测试不难发现,大部分的协议需要通过 Iperf、Netperf 等工具检测网络带宽问题,由于初始值需要手动设置且不便控制(如初始速率值设置过小,则不能利用网络带宽,设置过大,则极易造成链路拥塞,甚至整个网络瘫痪等负面影响),因此下一步工作将考虑实现能自适应地调节初始速率.

2) 多点传输模式转变.随着 e-science 各种应用的发展,高速光网络的通信模式将改变由传统的点到点传输结构向多点混合传输过渡.因此,如何有效控制多链路传输的节点负载均衡及相应服务,并保持均衡的并发数据量和较低的丢包率是多链路传输面临的挑战.

3) 终端性能影响.对于云平台的网络体系架构,由于核心网往往具备高带宽,信道经常出现空闲现象,而终端节点需要对大量的涉及到对各种数据的处理,如存储、计算等,其处理能力通常不及核心网的传输能力.随着云计算技术的深入发展,云计算网络体系架构的进一步完善,未来网络传输机制中,终端节点将是网络传输的主要瓶颈.因此,如何从提高终端性能的角度来考虑提高网络的有效利用率将是下一步工作的重点.

参考文献

References

- [1] 陈真.基于蚁群优化算法的云计算资源分配[J].青岛科技大学学报,2012,33(6):619-624
CHEN Zhen. Resource allocation for cloud computing base on ant colony optimization algorithm[J]. Journal of Qingdao University of Science and Technology: Natural Science Edition, 2012, 33(6): 619-624
- [2] 陈真.Hadoop 云平台的入侵检测系统优化设计[J].西

- 安工业大学学报,2012,32(9):716-722
CHEN Zhen. Optimal design of intrusion detection system in Hadoop cloud platform [J]. Journal of Xi'an Technological University, 2012, 32(9): 716-722
- [3] 贾翔龙, 吴刚. 分布式应用弹性支撑机制的研究与实现 [J]. 计算机工程与科学, 2014, 36(7): 1221-1225
JIA Xianglong, WU Gang. Research and implementation of elasticity supporting mechanism for distributed applications [J]. Computer Engineering & Science, 2014, 36(7): 1221-1225
- [4] 张玮, 牛正浩, 史慧玲, 等. 多目标优化的云计算虚拟集群动态调整方法 [J]. 济南大学学报: 自然科学版, 2014, 28(5): 376-381
ZHANG Wei, NIU Zhenghao, SHI Huiling, et al. Optimal Design of Intrusion Detection System in Hadoop Cloud Platform [J]. Journal of University of Jinan: Sci & Tech, 2014, 28(5): 376-381
- [5] 罗海燕, 吕萍, 刘林忠, 等. 云环境下基于模糊粗糙AHP的企业信任综合评估 [J]. 山东大学学报: 理学版, 2014, 49(8): 111-117
LUO Haiyan, LÜ Ping, LIU Linzhong, et al. Enterprises trust comprehensive evaluation based on fuzzy rough AHP in cloud computing [J]. Journal of Shandong University: Natural Science, 2014, 49(8): 111-117
- [6] Yu S C, Wang C, Ren K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing [C] // 2010 IEEE INFOCOM Proceedings, 2010: 63-71
- [7] Wang W C, Owens Z Li R, Bhargava B. Secure and efficient access to outsourced data [C] // Proceedings of the first ACM Cloud Computing Security Workshop, 2009: 55-65, doi: 10.1145/1655008.1655016
- [8] Yang Y J. Towards multi-user private keyword search for cloud computing [C] // 2011 IEEE 4th International Conference on Cloud Computing, 2011: 758-759
- [9] Nikooghadam M, Zakerolhosseini A, Moghaddam M E. Efficient utilization of elliptic curve cryptosystem for hierarchical access control [J]. Journal of Systems and Software, 2010, 83(10): 1917-1929
- [10] Zhou J T, Zheng S, Jing D L. An approach of creative application evolution on cloud computing platform [C] // Proceedings of the 2011 ACM Symposium on Applied Computing, 2011: 54-58

Data transmission scheme for network architecture towards cloud computing

YAO Guangwei¹

¹ Chaozhou Teacher's College, Hanshan Normal University, Chaozhou 521000

Abstract This paper introduces the data transmission mechanism currently practiced under the cloud computing architecture. To address the lack of coupling among tasks on the links under the network transmission mechanism, we propose an improved data transmission scheme for the future network architecture which is cloud computing oriented. In view of improvement in three aspects, namely the transmission delay, transmission reliability, and storage security of the cloud node, we build a new cloud architecture in order to meet different requirements in the Qos. Being able to integrate with current network, this scheme is characterized by controllable, administrable and extensible, which makes it applicable for the new network communication infrastructure.

Key words cloud computing; network architecture; TCP/IP; network time-lag