

云计算网络安全现状与思考

吴 雷

芜湖职业技术学院 安徽芜湖 241000

摘 要: 本次研究中, 为了进一步提升网络运作安全, 重点结合云计算背景展开了分析工作。在此基础上, 首先概述了云计算的内容, 随后就云计算背景下的网络安全现状展开了研讨, 包括网络技术、环境等, 随后提出了几点网络安全建设的策略, 旨在借此更好地促进网络安全管理水平提升。

关键词: 云计算; 网络安全; 实名认证

Current situation and thoughts of cloud computing network security

Lei Wu

Wuhu Vocational and technical college, Wuhu, Anhui, 241000

Abstract: In this study, in order to further improve the security of network operation, we focus on the analysis work combined with the background of cloud computing. On this basis, this paper first summarizes the content of cloud computing, then discusses the current situation of network security under the background of cloud computing, including network technology and environment, and then puts forward some strategies for network security construction, in order to better promote the improvement of network security management level.

Keywords: cloud computing; Network security; Real-name authentication

引言:

当前的大数据背景下, 网络信息安全系统的构建, 离不开网络安全环境的营造, 如此才能为网络安全管理工作水平的提升带来帮助。但目前, 在云计算基础上, 网络信息安全保护工作的推进过程中仍旧存在较多的不足, 继而影响网络用户的通信安全及上网安全, 对于重要机构乃至核心部门的数据安全也会造成负面影响。鉴于此, 本次针对云计算网络安全现状与思考这一内容进行深入分析具有重要现实意义。

1. 云计算概述

云计算在计算方法中, 类属于分布式计算, 其计算期间, 需要通过功能强大的网络“云”实现, 以此将海量的数据进行分解, 期间利用计算机处理程序, 将海量数据处理程序分解成数个小程序进行独立系统运行模式

的计算^[1]。随后, 将经由数个独立小程序计算所得出的数据结果, 统一汇聚至多部服务器所组成的总系统中, 并由系统将数据统计结果快速反馈至网络用户端^[2]。但是, 随着时代的发展, 当前的云服务已经并非是传统的单一性分布式计算手段, 而是在此基础上充分融合了效用计算、并行计算、虚拟化以及网络存储等多元化的计算技术, 提升计算效率及精确性的同时, 也充分为网络用户提供了更优越的上网体验。

2. 云计算背景下网络安全现状分析

2.1 网络技术安全现状

网络安全管理工作开展过程中, 网络技术的应用安全, 已经成为整项管理工作的核心内容。站在我国当前网络技术的全面发展视角来看, 云计算模式之下的网络技术应用存在着较多的不足, 包括技术应用不完善, 用户登录系统过程不安全等问题随之开始出现^[3]。例如, 在部分用户登录各类网络、App客户端时, 经常出现网页登录骤然停止或是系统运行中断类问题, 影响用户用网安全的同时, 导致用户不得不随时面临网络安全的被

课题项目: azcg 171 吴雷 基于分布式架构的双活数据中心在继续教育网络中的应用 一般课题 芜湖职业技术学院

动故障。此外,在云计算背景下,想要全面将用户的网络安全管理水平提升,针对既有网络技术进行优化已经成为重中之重。但目前,我国在该方面仍旧存在较多的不足之处,影响了网络安全建设效率,有待后续不断针对既有的技术进行强化和完善。

2.2 网络环境安全现状

网络资源管理中,安全技术的应用成效,在很大程度上会受到网络环境安全把控效果的影响。在当前盛行的云计算网络发展背景下,计算机PC端所遭受的恶意攻击乃至黑客袭击均对用户的网络安全构成了极大的威胁,继而影响了用户网络环境的构建和营造^[4]。与此同时,在云计算模式操作下,大部分计算机中的网络应用均具备大量的数据计算和存储应用,且该部分应用之中还会囊括海量的数据计算信息,该类信息也会一同存储于计算机应用之中,经过数据分析还可发现,所存储的信息往往呈动态化的控制状态存在,对于网络环境安全的构建形成了一定的难度,因此想要从根源上保障网络环境的安全性,技术人员必须就现阶段的网络环境安全处理技术进行不断的升级优化。详细分析来讲,目前我国的网络环境安全建设方面,仍旧存在人力、物力、财力等多方面的资源投入不足的问题,导致网络用户被黑客攻击、网址诈骗类事件层出不穷。由此可见,未来重点针对网络环境安全建设做好管理工作十分有必要。

2.3 网络法规安全现状

现阶段,我国综合互联网处理技术已经逐渐跻身于国际前列,但是,由于我国在互联网技术领域的起步时间相对比较晚,所以对应的网络法规安全管理工作开展并不到位,导致网络用户的用网安全以及用网规范问题随之产生,从而无形中生成各类网络安全问题,造成网络用户信息安全受到威胁^[5]。此外,在网络法规安全现状调查中也可发现,现有的网络安全管理法规界限划分并不明确,尤其是在定义恶意攻击方面,使得用户网络安全保障并不可靠。例如,在面对网络恶意攻击事件时,基于云计算模式下的网络数据存储呈海量增长模式递进,一旦对应的网络安全技术规范存在缺失或漏洞,必然给予不法分子以可乘之机,影响网络用户的上网安全。

3. 云计算网络安全建设的思考

3.1 做好网络程序研发的规范管理

网络安全保障中,云计算技术的应用价值提升到最高,就必须做好网络程序研发的规范管理工作(如图1所示)。目前的网络研发技术构成,主要包括两方面,一种是代理服务,另一种是应用程序,两者对网络安全的提升起到了重要的促进作用^[6]。具体的技术实践之时,

代理服务技术的支持下,可以对网站访问速度的增长发挥促进作用。与此同时,代理服务技术的介入,也可宏观调控网站访问的运行速度,以此为网络数据的安全性提升带来保障。此外,网络应用程序研发和更新,可以高度提升计算机对于病毒识别的敏感性,从而在遭遇病毒侵入时,第一时间识别,并弹屏警示用户,借此将网络安全管理质量提升,优化安全隐患的处理效率,达成云计算有效利用的目标。

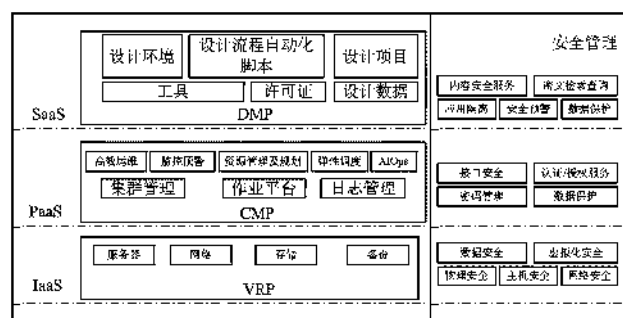


图1 云计算网络程序开发流程

3.2 构建完善的网络实名认证系统

在进行网络安全管控时,实名认证系统的构建,可以有效对云计算期间网络上对用户不正当攻击加以控制。详细来讲,进行网络实名认证系统的搭建时,首先要求网络用户享有独立的IP地址,避免因个人误操作、不良网络行为而诱发网络安全问题随之出现。面对此种情况,实名认证系统管理人员需要以此进行反向追踪,并对其进行警告和处置,预防相类似的问题再次出现。此外,当网络用户完成实名认证之后,信息共享可以通过技术监管的形式实现,以此作为云计算网络技术应用地开展基础,且此时由于云计算系统运行而产生的影响网络安全的危险因素可以被有效遏制,预防其对网络用户信息安全构成威胁,上述一系列实名认证过程中,网络安全共享信息监控的主要方式是抓取网络关键词和信息流,从而实现提升云计算背景下网络安全的管理目标。

3.3 搭建网络安全系统

进行网络安全系统的搭建时,应该做好下述几项工作:

其一,为计算机增设锁屏功能,以此在屏保方案的保护下,对网络数据安全性能提升带来帮助。

其二,针对计算机之内IP隐藏地址的隐藏程序进行云计算挖掘,并做好对应的研发与落实工作,预防出现IP泄漏类网络安全问题。

其三,作为网络管理部门,应该全面完善现有的网络安全管控体制结构,以此为云计算模式直线的网络应用技术的安全性提升带来保障,构建安全的网络环境。

3.4 可信云云计算技术的应用

随着国民出行消费付款模式的不断优化,目前支付宝已经成为大部分人付款选择方式,不仅快捷,且安全性也比较高。但是,为了避免其出现网络安全问题,影响收付款的安全性能,就需要重点应用可信云云计算技术完成对应的技术管理工作,借此对支付宝用户端进行改造和完善,提升支付宝的应用安全。具体的技术操作如下:

其一,设置完善的可信云客户端及管理平台。在客户端之上,将可信模式识别、融合验证以及密码学技术应用其上,用于保障支付宝云管理平台的网络安全。

其二,在支付宝可信云客户端之上,增设管理平台互动认证系统,所有用户均可通过客户端登录网页,当平台用户完成密码和ID的验证工作后,会将该用户的可信云证书回传回来,期间客户端会直接针对用户的生物信息特征、签名进行绑定,提升用户登录的网络安全性。

3.5 健全数据加密技术

为了充分提升云计算网络安全管理水平,还需重点做好对应的网络数据加密技术的应用工作。具体来讲,应该做好可信计算机数据安全数据的处理工作。想要保障可信计算平台中所有用户的信息安全,就必须确保用户数据的合法性,因此要求严格依照用户访问权限去把控其访问状态,实现“不同级别登录享有不同权限”的网络安全管理目标(如图2所示)。此外,为了确保整体网络数据系统访问的安全性,还必须针对其信息访问规则进行细化,以此为更多网络用户构建可信赖、高度安全的网络环境。

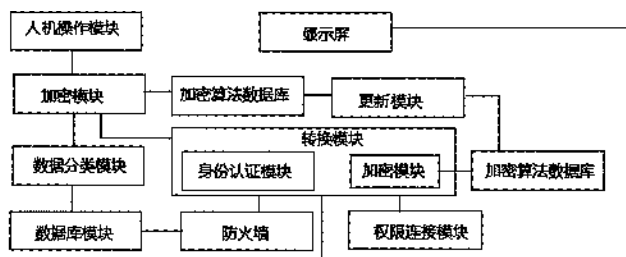


图2 基于云计算的数据加密技术处理

4. 结束语

综上所述,云计算网络安全管理中,想要全面提升管理工作质量,一方面应该积极搭建网络安全系统,以此系统的构建为网络安全提供保障。另一方面,则需要针对现有的网络安全加密技术进行不断的完善和优化。此外,还应将网络安全处理精力投放在网络程序开发的规范管理工作,如此才可确保用户网络安全在云计算大背景的影响下,得到更为显著的安全保障,最终为我国安全、稳定的网络环境建设奠定坚实的基础。

参考文献:

- [1]陈海红.探讨新时期云计算环境下的计算机网络安全技术[J].数字通信世界,2021(1):175-176,33.
- [2]王彩玲,宋冰.基于云计算的网络安全态势感知技术研究[J].常熟理工学院学报,2021,35(2):59-64.
- [3]吴家存.谈“云计算”环境中的计算机网络安全[J].信息记录材料,2022,23(1):95-97.
- [4]丁朝晖,张伟,杨国玉.基于动态伪装技术的网络安全防御系统研究[J].电子技术应用,2022,48(1):129-132.
- [5]傅江辉.基于云计算的社交网络安全隐私数据融合方法[J].济南大学学报(自然科学版),2021,35(1):29-33.
- [6]孙海波,石峰.浅析云计算在电视台融合媒体服务平台的应用[J].广播电视网络,2022,29(1):72-74.
- [7]刘莉莉,吕斌.新形势下网络安全等级保护2.0体系建设探索与实践[J].信息安全研究,2022,8(2):196-199.
- [8]徐航,张冬冬.大数据技术在网络安全分析中的应用[J].数字技术与应用,2022,40(1):240-242.