

探讨云计算技术在计算机安全存储中的应用

栾妍 乔贝

(山东外事职业大学 山东 264500)

摘要: 云计算技术实际上就是计算机、互联网技术的整合, 具有着经济、市场价值, 真正意义上的实现了让互联网技术、服务商品化融入到各个领域, 尤其是针对计算机安全存储领域中, 其产生的作用非常大, 是需要引起足够重视的。通过将云计算技术应用到计算机安全存储过程中, 让其具有的积极性作用真正发挥出来, 为后续的发展打下了良好的基础。

关键词: 云计算技术; 计算机; 安全存储

引言

云计算技术应用到计算安全存储中, 必须要树立起积极的观念, 建立起科学、规范化的技术模式, 借助于云计算技术提高计算存储的安全性, 让计算机安全存储系统得到良好的运行, 以更好的达到预期效果。社会各界中越来越关注数据库中的隐私保护, 为了保证计算机存储的安全性, 未来还需要不断研究云计算技术。

一、云计算技术

(一) 概念

云计算技术实际上就是依托于互联网, 进行使用的一个过程。一般情况下, 借助于云计算技术, 互联网动态扩展, 提供虚拟资源。云计算和传统计算机运算系统是存在着非常大的不同之处, 通过应用云计算, 使得运算能力得到加强, 已经达到了每秒十亿次, 主要是借助于天气中存在的变化来实现预测, 模拟核爆炸的基本趋势, 用户可以实现结合自身的需求情况借助于手机、电脑来借助于大数据技术来获得相应的服务, 用户可以借助于个性化的定制情况来开发出相应的服务, 从中获得软件服务, 借助于科学化服务方式的基础上, 实现了有效的处理。近几年在发展过程中, 云计算技术得到了广泛的应用, 有很多的网络运营商也在开发云服务, 使用云服务的用户也一直处于不断增长的趋势^[1]。

(二) 关键技术

1. 对身份进行认证

计算机安全存储过程中通过应用云计算技术, 实现了对身份进行识别的技能。实际上对身份进行有效识别的技术也是存在着不同之处的, 如, 首先, 借助于密码来进行识别。在该种技术中, 需要用户借助于系统中所要求的来输入正确账号、密码, 这一过程就是为了对使用者身份进行核实, 大多数的情况下都是借助于密钥的方面来进行认证, 通过这种方式在很大程度上保证了用户信息的准确性, 用户在使用过程中的合法性。其次, 借助于智能卡进行识别。这种技术要求了用户在使用过程中要使用包含了自己身份的智能卡, 在这个卡中具有较强的稳定性, 虽然稳定性较强但是却容易发生偷盗的情况, 面临着一定的不安全风险。再次, 借助于 kerberos 进行身份认证。该种认证方式在安全性能方面是比较好的, 采用的是和第三方资源进入到授权服务第三方协议, 最终生成加密钥匙, 使用的用户只要是正确的输入证件, 才能对身份进行有效识别。最后, 借助于 KPIs 进行身份验证。该种认证技术借助于通过是否和个人信息匹配度高的密钥、公共钥匙来进行解密, 通过这种方式可以在很大程度上提高计算机个人身份的安全性^[2]。

2. 数据加密处理

对称、不对称加密技术属于目前最经常使用到的一种加密技术, 其中在对称加密技术中, 就是借助于相同加密密钥来进行加密、解密处理, 在速度、效率以及安全性方面都是受到相同加密算法进行处理的, 这就需要对密钥的有效管理; 不对称加密技术实际上就是有设置出一个或相对的公开、私密密钥。其中在公开密钥角度上就是用来对数据进行加密处理, 私密密钥就是用来解密的, 具有的特点是算法方面非常得复杂, 数据的安全性都必须依赖于算法、密钥, 虽然加密、解密并不比相似的加密更快, 但是这种密钥却是存在着很大的安全性。通过经这两种数据加密技术, 可以更好地弥补数据安全中存在的漏洞, 保证云计算应用中更加的安全。

3. 对数据所进行备份

通过将数据进行备份处理, 保证了电脑中网络的安全性, 避免出现数据丢失的情况。如, 有很多公司中的机密文件都会存到硬盘驱动器上, 但是由于容量上的限制, 不可能将所有的文件都放到硬盘驱动器上。借助于备份的方式, 保证数据更好实现存储, 就算硬盘上数据发生了丢失的情况, 也可以及时地对备份数据进行补充, 让存储设备更加的安全。

4. 实现密钥管理

云计算技术中最为重要的一部分就是密钥管理, 将密钥进行分享以后, 让信息、数据、文件实现共享, 如密钥管理主要是应用于百度云中, 文件进行分享过程中保证了存储的安全性, 针对共享文件或者是信息实现了加密处理, 这时只有输入正确的密钥才能打开。通过这种方式, 转移、分享文件会具有一定的隐私性, 在很大程度上提高了一定的安全性^[3]。

5. 删除码技术

该技术属于一种新型的技术, 在网络程序的快速发展下, 让一些存储在网络上的编码得到了有效的管理, 对发生错误的编码实行解码。

(三) 必要性

计算机网络属于具有一定综合性、先进性的, 传统安全存储技术是不能满足于计算机安全存储中的具体要求达到。计算机网络是非常先进的, 只要是具有一定的资源、数据, 就能够进入到多个系统中, 让更多的网络数据都面临着不安全性的状态。随着云计算技术的出现, 将以上问题进行了解决, 这是不需要将数据存储到应破案中的, 反而是将其存储到云空间, 在云空间上保证了数据的隐私性以及安全性, 只要是通过云空间来获得相关的数据, 此过程中就需要获得多个层次的安全认证, 通过采取这样的方式保证数据在存储过程中的安全性。

二、计算机安全存储中存在的安全隐患

在计算机中, 对于数据进行储存基本上是可以分为两种形式, 分别是直接将信息数据放到 U 盘中、信息储存在硬盘上, 不管是哪一种方式都是存在着弊端的, 容易遭受病毒的侵害以及发生数据丢失的情况。计算机数据在进行储存过程中, 运用云计算可以直接借助于网络来访问 URL, 最终获得 PC 储存数据, 让信息得到良好的储存, 然而这并不代表着安全, 其中也是存在着一些安全上的问题, 具体的表现是: 云计算虽然有加密技术, 但是对于云计算供应商来说是没有作用的, 这样就相当于将云技术服务进行了垄断, 虽然能够提供商业上的信息, 但是却难以保证数据信息不丢失。基于这种情况, 制定了《关于下一代互联网“十二五”发展建设意见》, 其中有提出了需要不断加强云计算技术在实际应用过程中的安全性^[4]。

三、云计算技术在计算机安全存储中的具体应用

(一) 可取回性证明算法

在具体应用该类算法过程中, 所使用的相关机制是响应、验证, 这都是计算机算法, 应用中就是为了纠正编码, 尤其是借助于云计算技术查询相关数据时, 可以先验证数据信息, 然后再向云端发生挑战, 此时运算就可以结合用户的挑战来做出响应。这一过程中, 用户可以结合计算机作出的响应情况来判断出云端数据中的安全性, 要是没有通过验证, 就表示在数据中心上的文件受到了破坏,

针对这种情况就需要及时地进行修复。要是遭受破坏的数据,数值处于阈值内,可以借助于变慢来将原始数据进行恢复;这一过程中,要是验证已经通过了,用户就可以实现到云端上进行处理,尤其是计算机运行时,这时是很容易导致计算机数据受到损失,而编码就可以对这种情况进行恢复。在这样一个过程中,就可以借助于可取回性证明算法,保证用户能够验证运算数据库系统,将符合完整、安全性的标准进行明确,分析出其中存在的失误之处,这样更有利于进行管理。

(二) MC-R 端

为了能够保证在云端上更加安全的存储数据,一般就会使用 MC-R 端,借助于多元化的方式来保证对数据的管理,让数据更加的安全。云计算技术中对 MC-R 端进行应用中,首先,对用户 MC 进行加密处理,将云计算技术采用合适的方式应用于网络安全存储系统中,对网络系统中是否存在隐患展开分析,对具体的问题展开探究,并做到严格管理。在应对黑客过程中,就需要做到合理的预防,预防借助于程序、客户端中存在的漏洞会进入到数据中,避免数据遭受到泄露的情况。其次,在数据库、云端角度上,就需要加强管理工作的开展,以更好的创建数据隐私、伪装管理模块,以建立出完善的数据管理模块,真正发挥出以上模块中的作用。经过相互之间的协调性发展,真正意义上实现了安全存储管理。最后,实际工作开展过程中,也是需要应用 RSA,全面分析出大数据中具有的消耗,以这种方式来建立起加密和解密模块,并保证其是完善的,并实现严格的管理、协调。此外,对用户实际情况也需要做到引导,建立起 RSA 密钥以后,数据信息可以实现自动的出巡到其中,MC 加密算法下,保证数据实现了有效的加密处理,在将其传到云端以后,实现了数据的安全性,并真正实现安全管理,让整个系统都更加的安全。

四、提高计算机安全存储的策略

(一) 优化云计算信息库防火墙设备

计算机安全存储过程中,通过运用云计算技术,保证了数据的安全性,预防出现丢失、泄露的情况,为了能够保证数据存储过程中的安全性,可以优化云计算信息库防火墙设备。防火墙在计算机系统中可以保证数据的安全性,也能抵挡病毒、攻击,这对于提高计算机防御功能具有非常重要的作用。因此,将云计算技术应用于计算机安全存储过程中,需要安装高性能的防火墙。如,对于防火墙设备应用虚拟化保护措施过程中,需要将保护性的措施作用于计算机终端,这样在保证计算实现独立运行的同时,还能实现实时监

控计算机信息数据,让多台计算机都能够实现同时进行安全管理,经过互相监督,最终实现了信息数据的有效存储,所以,提高云计算技术在计算机安全存储中效果是可行的^[9]。

(二) 完善云计算数据中心信息系统

计算机安全存储中应用云计算技术,虽然保证了信息的安全性,避免出现丢失的情况,但是其中却是存在着一定的安全隐患,所以此时就需要针对云计算中存在的不同之处,得到多领域的共同发展,不断完善云计算技术。如,建立有效的信息系统,这样就算是云计算出现了问题,也能将存在的问题快速备案,并将问题归入到信息系统中,在更新存储中遇到的问题后,也为云计算技术的应用奠定良好的基础。同时,借助于身份认证的方式,将云计算数据中信中的信息进行不断的完善,具体可以采用四种技术进行,如密钥、pk、kerberos、智能 IC 卡,通过这种方式保证每一条信息都能够验证身份,用户接收到服务器认证以后,才能登录到数据中心系统,采用确认身份的方式提供更好的防护,保证网络信息数据足够安全,这在一定程度上提高了云计算技术在计算机安全存储过程中的具体效果。

结束语

云计算属于一种新型的计算模型,能够将个人在计算中存储的数据转移到计算机集群上,实现了计算机较大的存储量。然而在计算数据库中不仅数量庞大,并且也是非常复杂的,这时安全存储功能就产生了威胁,非常容易受到病毒、攻击,最终让大量的数据丢失、篡改,为了保证数据中更安全,预防数据遭受到泄露,未来对于云计算中的存储还需要进行深入地探究。

参考文献:

- [1]王利军.云计算技术在计算机安全存储中的应用研究[J].科技视界,2021(27):146-147.
- [2]左毅,郭长金,游华.云计算技术在计算机网络安全存储中的应用[J].电子技术与软件工程,2021(18):246-247.
- [3]孟大森.计算机网络安全存储中云计算技术的应用[J].电子技术与软件工程,2021(15):243-244.
- [4]孙力.云计算技术在计算机网络安全存储中的应用分析[J].数字技术与应用,2021,39(07):184-186.
- [5]陈德.云计算技术在计算机网络安全存储中的应用[J].江西电力职业技术学院学报,2021,34(06):20-21+25.

(上接第 219 页)

的价值,首先要提高技术人员的思想认知,加强风险管控意识。只有维护好网络安全,才能保护用户个人的数据信息,从而维护整个社会的和谐安定,因此,要从根源上铲除不良因素,维护网络安全。首先,用户自身要加强网络风险意识,注重个人隐私的保护,重要信息如身份证号码、手机号、银行卡账户及密码等信息绝不能轻易外泄;其次,技术人员要提高信息管理技术水平,对实际生活中可能会出现风险因素进行分析和预防,制定相应的预防对策,对于出现的问题具备解决能力。

4.2 做好计算机信息管理技术的管理工作

目前,计算机信息管理技术是维护网络安全的主要办法,因此,做好信息管理技术管理,加强其在实际生产生活中的应用十分重要。为此,要做到管理内涵和理论双管齐下,将其应用到网络安全的实际预防中。当前,计算机信息管理技术的应用越来越广泛,网络信息系统朝着现代化和科学化发展,信息管理技术也在不断地创新和完善,管理水平进一步提高。想要更好地实现信息管理技术在网络安全中的应用,必须要对网络安全防范机制有充分了解,做好信息管理工作^[9]。

4.3 建立完善的计算机信息管理技术相关制度

除了加强安全意识和做好管理工作外,还应该建立健全信息管理的相关制度。相关部门可以建立科学合理的规章制度,筹备网络

安全小组,负责日常的网络信息安全工作。同时,安全工作应该常态化,对于计算机的操作系统,应该做到定期的更新、杀毒、漏洞修复等,对于可能会遇到的风险问题,要做出预案并具备解决问题的能力。除了要防备黑客攻击或者病毒入侵外,计算机硬件系统的安全性也应该得到保障,应该及时更换功能和系统滞后的计算机,保障计算机的硬件功能能够胜任工作需要,以防硬件方面故障和问题影响信息安全。

5 结束语

信息时代的发展已经涵盖了人们生产生活的方方面面,在享受网络技术带给人们便捷生活的同时,也要意识到网络安全的重要性。只有增强计算机信息管理技术水平,才能够增强抵御网络安全风险的能力,保证数据信息不被泄露,维护好网络安全。

参考文献:

- [1]李刚.试论计算机信息管理技术在网络安全中的运用[J].无线互联科技,2016,78(2):123-124.
- [2]胡恒金.论计算机信息管理技术在网络安全技术中的应用[J].网络安全技术与应用,2016(6):2.
- [3]赵志鹏.浅论计算机信息管理技术在网络安全中的应用[J].电子世界,2016(7):82-83.