基于云计算的 IT 数据中心安全问题研究

张威[1] 李飞[1] 赵龙生[1]

（国电南瑞科技股份有限公司信息系统集成分公司 江苏南京 211102）

摘要：伴随近年来我国社会经济迅速发展，也推动了科学技术水平的持续提升，信息化技术不断深入社会各行各业，并在各个领域及实际工作中得到广泛应用。与此同时，云计算以及 5G 无线网络技术的发展结合，也进一步推动信息化技术的发展更新。然而从实际情况来看，信息化技术实际运用过程中在法律、技术以及监管等方面还面临着一系列安全问题，直接威胁我国网络用户的信息安全。基于此，本文主要针对基于云计算的 IT 数据中心安全问题进行研究。

关键词：云计算；IT 数据中心；安全问题

云计算，主要是借助因特网向用户提供各种云数据服务、运算以及虚拟化储存等功能。云计算体现出显著的多用户性、开放性、灵活性等特征，能够将各种各样计算资源集中融合并上传至云端计算资源库，完成统一管理、调度，各个用户可借助应用程序访问云端，获取所需的一系列数据、资源、应用程序等。然而由于云计算所具备的动态性、复杂性等特征，并且面临对海量使用用户，一旦缺少良好的身份认证以及验证机制，将做许多黑客以及非法用户侵入，从而威胁到正常用户数据安全[1]。同时由于云计算主要借助云端虚拟资源库向用户提供相关需求和服务，其体现的跨地域性、虚拟性特点也导致许多用户难以验证云储存可信性，存在较多的安全漏洞。基于此，本文主要探究基于云计算的 IT 数据中心安全问题，并探讨相关解决策略，从而实现对云计算服务的持续优化。

一、基于云计算的 IT 数据中心安全问题

1.用户和云之间缺乏完善的身份认证机制

云计算作为一种服务平台体现出共享性的特征，借助因特网向用户提供各种数据访问以及交互等服务。然而由于网络所属于一个虚拟空间，加上云计算的跨地域性、开放性等特点，也会让许多非法用户和恶意软件能够在网络上始终保持隐匿，难以被定位追踪。导致大量非法用户以及黑客侵入用户账号，对用户数据信息进行篡改、泄露，并用于非法途径[2]。因此用户和云端之间的身份认证机制是有效保障 IT 数据安全的重要基础，一旦缺乏完善的身份验证机制，非法侵入者将会很容易冒充用户身份直接进入用户云空间开展非法活动。同时还可能导致用户和欺诈黑云之间进行错误的交互，相关的恶意软件、网络钓鱼软件借助黑云来非法得到用户数据和隐私信息并加以利用。

2.缺失健全的云端静态数据储存监管机制

云计算服务的静态数据储存通常外包至相关云服务商，由于服务较为透明，用户很难基于 Web 前端交互界面来对云服务商可信性进行评估，也难以确定云服务商有无根据服务协议来储存和处理相关数据。特别是在缺少完善的数据储存验证机制时，一些非法云服务商常常出现篡改或者恶意窃取用户储存在云端的隐私数据和应用的情况[3]。同时由于一些技术、人为、管理等因素影响，云服务商储存服务器不可避免地发生异常现象，导致数据丢失或者泄露。但因为自身利益考量，很少有云服务商会主动承认这此类失误。因此云端数据安全储存以及服务受到大多数用户的重点关注，为了实现对云服务商行为的有效监管，确保数据储存可靠、完整性，需要构建起针对用户的静态数据储存服务验证信任机制。

3.云端动态数据安全保护机制仍有漏洞

基于云计算服务的 SAAS 云应用，其也属于用户借助 Web 来储存数据以及开展各种访问服务的基础。而云计算作为一种共享式虚拟资源库服务模式，主要借助 IT 计算资源来进行集中管理、调度，向用户提供所需要的各种服务。单一 SAAS 云服务提供服务期间会对不同用户数据进行处理，而多用户使用的虚拟资源也经常被绑定到相同的物理资源上，在这一共享资源服务模式下，多用户也会借助公共服务程序完成相应数据储存和访问，被共享访问的 SAAS 云应用也成为争夺权限的中心[4]。若存在安全保护不完善的情况，一些恶意软件以及代码容易造成数据安全保护机制不能正确执行或者被干扰，使得非法用户对同一物理主机上的其他用户进行侵入、窃取和泄露隐私数据，从而对 IT 数据中心安全造成严重威胁。

二、基于云计算的 IT 数据中心安全问题解决对策

可信云计算平台基于可信传递“”的服务理念之下，主要目的在于构建起用户对于云服务商的信任，从而保证云服务的可靠性和安全性，这也是现阶段云安全研究的重点方向之一。相关研究人员借助可信计算技术构建起了一种优化的远程自动信任协商证明方案，有效提高了云计算环境的安全性[5]。同时还有研究人员通过可信云计算技术设计了相关云安全的新型架构。笔者结合目前有关研究结果，基于可信云计算框架之下，构建起一种全方位的数据安全保护系统。

1.数据安全系统整体框架

基于可信云计算框架之下，构建其 IT 数据安全保护系统，主要依托于可信计算技术，通过物理保护机制以及密码技术形成相应的可信根，并以此为中心，逐渐开展可信拓展，形成相应的可信链，从而保证整个云环境体现出良好的可信性[6]。其中涵盖了用户和云之间的双向认证机制、静态数据储存验证机制以及动态数据安全保护机制，以上三个子系统可作为可信计算基。数据安全保护系统主要涵盖以下 5 个维度，详细功能如下。

1.1 可信云计算平台

在这一平台上，主要是将 TPCM 可信根作为逻辑的出发点，并以此为中心从上到下构建起多层可信链，建立起可信云计算平台，为用户和云之间打造出双向认证以及静态数据储存的验证机制，同时还包括 SAAS 云应用中的动态数据安全保护机制，从而向用户提供相应的可信支撑[7]。

2.2 可信第三方认证平台

可信第三方认证平台和可信云计算平台之间主要开展节点交互，通常负责的是可信节点的身份管理。并对云计算用户相关身份数据进行认证以及保护，向用户和云之间的跨云身份认证、静态数据储存提供认证和验证支撑等服务[8]。

2.3 依托于 3PAKE 跨云认证子系统

跨云认证子系统主要基于 3PAKE 认证协议的基础之上，主要通过已经在私有云中完成认证的用户身份信息，构建起和公有云之间的双向认证机制，可以实现对多用户身份的精准识别，从而有效抵御黑客侵入以及非法用户冒名使用的现象。

2.4 静态数据储存验证子系统

静态数据储存验证子系统，主要是建立在云计算数据服务所具备的外包性以及云服务商可信性难以评估的基础之上，形成用户可以验证的云储存信任机制，来对云服务商静态数据储存行为进行全方位监管，从而保证静态数据储存的完整性，精准性。同时还可对数据开展备份，当发生数据丢失以及泄漏现象时，用于数据的修复。

2.5 基于 SAAS 云应用的动态数据保护子系统

基于 SAAS 云应用的动态数据保护子系统，主要针对的是云计算所体现的多用户性这一特征，形成分散信息流所控制的 DIFC 模型，通过细粒度可信实体来对动态数据开展相应的追踪以及签注，有效保护和隔离各个用户的动态数据，从而有效预防数据被非法用户进行篡改并加以利用。

（下转第 72 页）

（上接第 64 页）

2.2 数据安全保护系统的开发环境

Eucalyptus 是一种建立在 linux 基础上的软件架构，主要通过计算集群以及模块化设计弹性达到云计算的目的。在这一架构中，可以由云计算研究者按照自身需要选择相应的硬件、网络、储存等资源集合，体现出良好的迁移性和扩展性。本次研究中主要使用的是基于 Eucalyptus 架构的可信云计算技术的数据安全保护系统。其中，主要使用相对较小的局域网模拟搭建出 IT 数据保护系统的云环境，所设置的主机数量达到 7 个。其中前端一共布设 4 台，分别用于云管理员、客户端、集群管理服务器（为这台主机配备了 CC 组件化框架基础库以及储存控制组件）以及云服务的 WebPortal 门户（为这台主机配备了 CLC 云控制器以及 Warlus 储储存控制器）。后端一共布设了 3 台主机，其中 2 台用于计算储存器（其中 1 主机主要负责各种虚拟机实例计算服务的运行，另外 1 台主机主要负责数据储存访问），另外 1 台作为储存服务器，主要负责将第三方认证平台引入其中。

三、结语

综上所述，云计算作为当前一种广泛应用的技术以及服务模式，体现出显著的共享性、虚拟化等特征，能够将各种各样软硬件 IT 资源上传并储存到云端，并借助网络向广大用户提供各种数据资源以及应用等服务。然而由于身份认证、静态数据储存验证机制等方面的不足，以及 SAAS 云应用共享技术依然存在漏洞等一系列安全问题，对云计算的大面积推广产生较大阻碍。通过采取可信云计算，可以借助可信跟信任链构建起用户对云计算服务的信任机制。笔者在本次研究中，将其作为基于云计算的 IT 数据中心安全问题解决的一个思路，并将 3PKKE 跨域云认证机制引入其中，有效解决当前用户和云端交互之间所存在的认证安全问题。此外根据数据安全储存认证和共享进程所存在的不足，提出数据安全验证、保护机制等方法，实现从各个维度对 IT 数据中心安全问题的有效解决，从而切实提高了云计算的数据以及服务安全性。

参考文献：

[1]崔云龙,吕书林,任高强.基于云计算的 IT 数据中心安全问题分析[J].工程技术,2021(11):0144-0145.

[2]彭扬剑. 基于能源互联网企业云计算数据中心的安全关键技术研究[J]. 自动化技术与应用,2020,39(7):46-50.

[3]沈建国. 基于云计算环境下的网络安全研究[J]. 襄阳职业技术学院学报,2020,19(1):85-89.

[4]但凝云. 基于云计算环境下计算机网络安全问题的研究[J]. 计算机产品与流通,2017(10):71.

[5]刘雯雯. 基于云计算环境下的计算机网络安全存储系统的设计与实现[J]. 电脑知识与技术,2022,18(12):38-40.

[6]陈德. 云计算技术环境下计算机网络安全分析[J]. 佳木斯职业学院学报,2021,37(3):137-138.

[7]薛峰. 基于云计算环境下计算机网络安全问题与建议[J]. 信息记录材料,2021,22(9):65-66.

[8]凌旺,闵啸,赵亮. 基于大数据云计算网络环境的数据安全问题研究[J]. 电子元器件与信息技术,2022,6(1):238-239.

张威（1982-），男，汉族，湖北武汉人，学士，工程师，主要研究方向：IT 基础架构，IT 智能运维，电网数字孪生等。

李飞（1988-），男，汉族，陕西榆林人，学士，主要研究方向：工业互联网、电力数字孪生技术、5G 及物联网技术等。

赵龙生（1986-），男，汉族，黑龙江七台河人，学士，工程师，主要研究方向：电力自动化系统、电网数字空间、分布式存储等。