基于云计算的计算机信息安全技术分析

吴雄燕
（玉林市信息中心 广西 玉林 537000）

摘　要　随着云计算技术的快速发展和广泛应用，数据安全、隐私保护和访问控制方面的信息安全需求和挑战，成为云服务提供商和用户面临的主要问题。针对该问题，文中提出了基于云计算的信息安全策略和技术，包括先进的数据加密方法、强化的身份认证机制、精细化的访问控制策略以及基于云环境的入侵检测和防御系统，旨在全面提升云计算环境中的数据保护和系统安全性。实验结果表明，该安全策略和技术在云计算环境中提高了数据保护水平和系统安全性，降低了安全威胁和风险，增强了整个云服务体系的安全性和用户信任度。

关键词：云计算；信息安全；数据加密；身份认证；入侵检测
中图分类号　TP309.2

Analysis of Computer Information Security Technology Based on Cloud Computing

WU Xiongyan
（Yulin Information Center，Yulin，Guangxi 537000，China）

Abstract　With the rapid development and wide application of cloud computing technology, the information security requirements and challenges in data security, privacy protection and access control have become the main problems faced by Cloud as a Service providers and users. In response to this problem, this paper proposes cloud-based information security strategies and technologies, including advanced data encryption methods, enhanced identity authentication mechanisms, refined access control strategies, and cloud-based intrusion detection and prevention systems, aiming to comprehensively improve data protection and system security in cloud computing environments. The experimental results show that the security strategy and technology improve the level of data protection and system security in the cloud computing environment, reduce security threats and risks, and enhance the security and user trust of the entire Cloud as a Service system.

Keywords　Cloud computing，Information security，Data encryption，Identity authentication，Intrusion detection

0　引言

云计算作为一种新兴的计算模式，已成为数据处理和存储的重要平台[1]。其通过提供可扩展、灵活且成本效益较高的解决方案，促进了信息技术的应用和创新[2]。然而，随着云计算的普及，信息安全问题逐渐成为该领域中的一个核心关注点[3]。在数据安全、隐私保护和访问控制方面，云计算面临着一系列的挑战和风险。云服务的多租户特性和资源共享机制提高了资源利用率，但也带来了数据隔离和保护方面的挑战[4]。此外，云计算模式的动态性和分布式特征，加剧了数据管理和安全监控的复杂性。因此，探索和实现云计算环境下的信息安全策略，成为保障云服务安全运行和用户数据安全的关键[5]。本文旨在分析云计算环境下的信息安全问题，提出了具有针对性的安全策略和技术解决方案，为云计算环境提供了全面的安全保障，以应对不断增长的安全威胁和挑战。

1　云计算技术概述

1.1　云计算的定义和特征

云计算作为信息技术领域的创新，提供了一种全新的数据处理和存储方式。它允许用户通过互联网访问可共享的计算资源，如服务器、存储设施、应用程序和服务。云计算的核心特征包括资源的弹性伸缩、资源池化和按需自助服务。用户可以根据需求，灵活地扩展或缩减资源配置，从而实现成本效益最大化。资源池化允许不同用户共享相同的基础设施资源，而按需自助服务特性则使用户能根据需求自主获取和配置资源，无需受时间和地点的限制。

1.2　云服务模型

云计算服务模型主要分为 3 种，分别是基础设施即服务（Infrastructure as a Service，IaaS）、平台即服务（Platform as a Service，PaaS）和软件即服务（Software as a Service，SaaS）。云服务模型的实现流程如图 1 所示。

作者简介：吴雄燕（1981—），本科，工程师，研究方向为信息安全、云计算等。

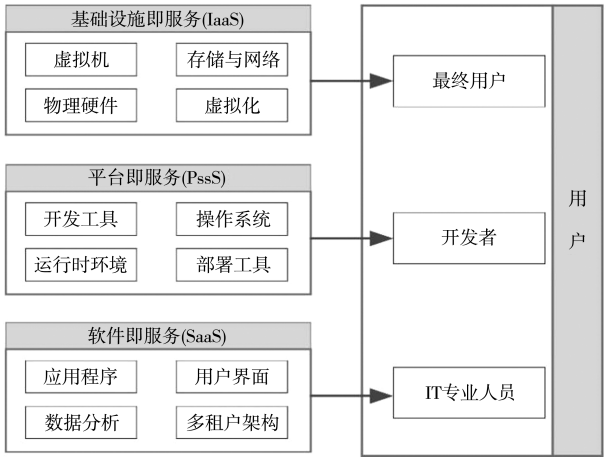

图 1　云服务模型的实现流程

基础设施即服务可以为用户提供虚拟化的计算资源，如虚拟机和存储空间，使用户能在云端运行操作系统、应用程序等。平台即服务提供了编程语言、工具和服务的集合，使开发人员能更快速地开发或部署应用。而软件即服务直接向最终用户提供应用软件服务，用户无需管理底层的基础设施，通过网络连接即可使用应用程序。

2　基于云计算的信息安全技术

2.1　系统整体框架

系统整体框架有 4 个核心组成部分，即数据加密技术、身份认证机制、访问控制策略、入侵检测和防御系统。数据加密技术可以确保云中的数据在传输和静态存储时均得到保护。身份认证机制可以验证和管理用户身份，确保只有得到授权的用户才可以访问云资源。访问控制策略可以定义用户可访问的资源类型和范围，进一步增强安全性。入侵检测和防御系统负责监控云环境，以识别和响应潜在的安全威胁。系统的整体框架如图 2 所示。

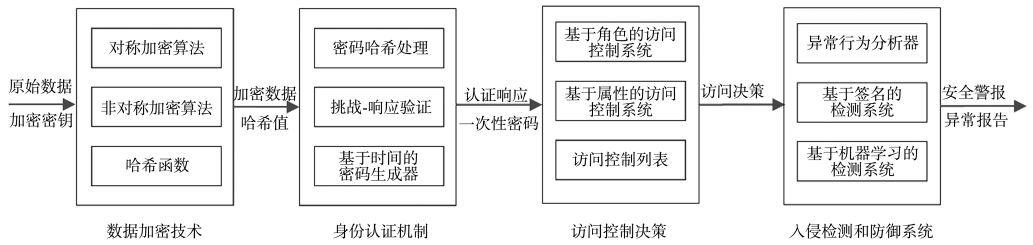

图 2　系统整体框架

该框架旨在为云计算提供一个全方位的信息安全解决方案，使云服务提供商和用户能更有效地管理其安全风险，同时保持云计算的灵活性和扩展性。通过综合应用这些技术，可以显著提高云环境中的数据、资源的安全性。

2.2　数据加密技术

数据加密技术通常分为对称加密和非对称加密。对称加密使用相同的密钥进行数据的加密和解密，该方法的加密强度依赖于密钥的保密性。对称加密的数学模型如式(1)所示：

$$C=E_k(M)=M\oplus k \tag{1}$$

其中，C 表示密文，M 是明文，E_k 是以密钥 k 进行的加密操作，⊕表示按位异或操作。

解密过程如式(2)所示：

$$M=D_k(C)=C\oplus k \tag{2}$$

其中，D_k 是以密钥 k 进行的解密操作。

非对称加密使用一对密钥，即公钥和私钥。其中，公钥用于加密，私钥用于解密。该方法的安全性基于密钥对的数学构造。基于模运算的加密和解密过程如式(3)所示：

$$C=E_{k_{public}}(M)=M^e mod n \tag{3}$$

其中，M^e 表示消息 M 的 e 次幂，n 是模数。

2.3　身份认证机制

身份认证机制负责验证用户的身份，防止未经授权的访问，保护敏感数据。常用的身份认证方法有哈希函数、挑战-响应机制和基于事件的一次性密码方法。

基于哈希函数的方法通常如式(4)所示：

$$H=\text{hash}(\text{Password}\oplus\text{Salt}) \tag{4}$$

其中，Password 是用户的密码，Salt 是一个随机生成的字符串，用于提高密码的安全性，⊕表示按位异或操作。

在挑战-响应机制中，服务器会向客户端发送一个挑战，客户端则使用密钥计算响应并返回，如式(5)所示：

$$\text{Response}=\text{hash}(\text{Challenge}\oplus\text{Key}) \tag{5}$$

其中，Challenge 是服务器发送的挑战，Key 是共享的密钥。

基于时间的一次性密码算法可以生成一个基于时间的一次性密码，用于双因素认证，如式(6)所示：

$$\text{OTP}=\text{truncate}(\text{hash}(\text{Key}\oplus\text{Timestamp})) \tag{6}$$

其中，Key 是与用户关联的秘密密钥，Timestamp 是当前的时间戳，truncate 函数用于从哈希结果中提取一次性密码。

2.4　访问控制策略

访问控制策略可以确保只有得到授权的用户才能访问敏感数据和资源。访问控制策略分为 3 种，分别是基于角色的访问控制、基于属性的访问控制和访问控制列表。基于角色的访问控制模型通过将权限与角色关联，然后将角色分配给用户，来控制其对资源的访问。基于属性的访问控制可以根据用户属性、资源属性和环境条件来定义访问规则。

2.5　入侵检测和防御系统

在云计算安全中，入侵检测和防御系统(IDS/IPS)常被

用于检测、阻止恶意活动和攻击。

异常检测系统通过分析网络行为的统计模型来识别异常活动。其通常以网络流量的统计特性为基础，如式(7)所示：

$$Z=\frac{X-\mu}{\sigma} \tag{7}$$

其中，X 是观测值，μ 是平均值，σ 是标准差，Z 是标准化分数，用于确定数据偏离正常行为的程度。

基于签名的检测系统依赖于预定义的攻击模式(签名)来识别已知的恶意行为。签名匹配式如式(8)所示：

$$M=\sum_{i=1}^{n}\delta(s_i,p_i) \tag{8}$$

其中，s_i 是攻击签名中的元素，p_i 是网络流量中的相应元素，δ 是匹配函数，n 是签名中的元素数量，M 表示匹配的程度。

在 IDS/IPS 中，机器学习技术常被用于建立行为模型，并预测潜在的安全威胁。这通常会涉及分类算法，如式(9)所示：

$$y=f(x;\theta) \tag{9}$$

其中，x 是输入特征向量，y 是预测结果，θ 是模型参数，f 是学习的分类函数。

通过这些技术手段，云计算环境的安全性得到了显著增强，从而为用户提供了更加安全和可靠的服务。

3 实验设计与结论分析

3.1 实验环境

本文的实验环境采用亚马逊云服务 Amazon Web Services，AWS 的 EC2 实例 t2.large 型号，运行 Linux Ubuntu 20.04 LTS 操作系统；数据库服务器采用 MySQL 8.0 版本；数据加密和身份验证使用 OpenSSL 1.1.1 库；入侵检测系统采用 Snort IDS 3.0。

3.2 实验结果及分析

该研究对基于云计算的信息安全技术进行了详细的测试和评估，特别关注了数据加密、身份认证、访问控制和入侵检测系统的性能。表 1 展示了在这些关键安全领域中的实验结果，包括各项技术的响应时间、准确率等关键性能指标。

表 1 实验结果

安全技术类别	响应时间/ms	准确率/%
数据加密	120	99.6
身份认证	90	98.3
访问控制	70	98.6
入侵检测	50	97.8

表 1 结果证明，这些技术的综合应用不仅可以增强云环境的安全性，也为用户提供了可靠的保护，在实际云计算应用中具有的巨大潜力和实用价值。

4 结语

本文深入探讨了基于云计算的信息安全技术，涵盖了数据加密、身份认证、访问控制、入侵检测等关键领域。实验结果显示，这些技术在响应时间、准确率等关键性能指标上表现优异，可有效防御各种安全威胁，保障了云计算环境的安全性和可靠性。总体而言，这些技术不仅提升了云服务的整体安全水平，也为云计算用户提供了更加安全、高效的使用体验。未来，随着云计算技术的不断发展，加强和优化这些安全技术将是提高云环境安全性的关键。

参考文献

[1] 王娜.基于云计算的计算机信息安全技术分析[J].信息记录材料，2023，24(9)：115-117.

[2] 农佳明.大数据技术在计算机信息安全领域中的应用[J].自动化应用，2023，64(10)：242-244.

[3] 赵云.云计算在计算机网络安全中的应用[J].电子技术，2023，52(3)：352-353.

[4] 刘洪亮.云计算中网络信息安全技术的应用研究[J].科技资讯，2021，19(20)：10-12.

[5] 王浩亮.云计算环境下计算机信息安全与保密技术[J].电子技术与软件工程，2021(9)：247-248.