 DOI: https://doi.org/10.12349/iser.v6i7.6701

Research on the Security and Reliability of Software Engineering in Cloud Computing Environments

Tao Lu

Heilongjiang University, Harbin, Heilongjiang, 150080, China

Abstract

With the continuous development of the times and the advancement of technology, the development of cloud computing technology has brought numerous challenges to software engineering in terms of security and reliability. This paper focuses on the cloud computing environment, analyzing a series of security challenges such as data security and privacy protection, identity verification and access control, as well as reliability challenges such as system availability and load balancing. It also discusses security guarantee technologies such as encryption technology and key management, identity authentication and authorization mechanisms. The research results show that only by comprehensively applying multiple technologies and methods can the security and reliability of software engineering in cloud computing environments be effectively improved, providing a reference for the development of related fields.

Keywords

Cloud Computing; Software Engineering; Security; Reliability

云计算环境下软件工程的安全性与可靠性研究

卢涛

黑龙江大学，中国 · 黑龙江 哈尔滨 150080

摘　要

随着时代的不断发展，科技在不断进步，随着云计算技术的发展，软件工程在安全性以及可靠性层面遭遇了诸多难题，本文着重关注云计算环境，剖析数据安全与隐私保护、身份验证与访问控制等一系列安全性方面的挑战，还涉及系统可用性、负载均衡等可靠性挑战，对加密技术与密钥管理、身份认证与授权机制等保障技术展开了探讨。研究结果显示，唯有综合运用多种技术与方法，才可切实提高云计算环境下软件工程的安全性和可靠性，为相关领域的发展提供参考。

关键词

云计算；软件工程；安全性；可靠性

1 引言

在数字化时代，软件工程作为构建信息系统的基石，其安全性直接关系到数据保护、系统的稳定运行及用户的隐私安全。随着网络攻击手段越来越复杂多变，软件工程中的安全问题已成为不容忽视的挑战。因此，深入研究软件工程与云计算技术的融合，成为保障信息系统安全性的关键路径。通过理论分析，期望为软件工程领域提供一套系统性的安全融合策略与实践指南，以应对日益严峻的信息安全威胁，促进软件产业的健康发展

2 云计算基础与软件工程概述

2.1 云计算的定义

云计算作为一种计算模式，借助网络实现对分布式计算资源，例如服务器、存储、网络以及软件等的统一管理与调度，以服务形式交付给用户。从技术角度来讲，依靠虚拟化、分布式计算以及大规模资源管理等技术手段，实现资源的动态分配以及灵活扩展。在服务模式方面，主要包含基础设施即服务、平台即服务以及软件即服务[1]。云计算类似“计算资源的自来水厂”，用户不用了解背后复杂的基础设施，仅需依据需求获取计算能力、存储资源或者应用服务，具有超大规模、虚拟化、高可靠性、通用性、高可扩展性以及按需服务等特性，其关键技术涉及分布式存储、分布式计算、虚拟化技术等。

2.2 软件工程的基本原则与方法论

软件工程的基本原则能保障软件开发有高效性、可靠性以及可维护性，常见的有抽象原则，凭借简化和概括问题，提取出本质特征。模块化原则，把软件系统划分成独立的模块，以此降低复杂度，信息隐藏原则，即隐藏模块内部的细节，只暴露必要的接口。模块独立性原则，让模块间耦合度低且内聚度高，一致性原则，保证整个系统的设计和实现风

【作者简介】卢涛（2005–），男，中国天津人，本科，从事软件工程研究。

格保持统一，完备性原则，保证系统功能完整无缺。可验证性原则，方便对软件进行测试与验证。软件工程的方法论是指导软件开发的整体框架，包含瀑布模型，它把开发过程划分成需求分析、设计、编码、测试、维护等阶段，然后依次推进，敏捷开发方法，强调快速迭代、客户协作以及适应变化，增量模型，逐步增添软件功能，螺旋模型，将风险评估融入开发过程，适合复杂大型项目等，不同的方法论适用于不同的项目场景与需求 [2]。

3 云计算环境下软件工程的安全性挑战

3.1 数据安全与隐私保护

在云计算环境当中，数据的存储以及传输会面临诸多安全风险，从软件工程的角度来看，要在系统设计阶段构建起覆盖全生命周期的数据安全防护体系，在数据存储方面，借助加密算法以及密钥管理机制来保障数据的安全性，比如采用 AES 高级加密标准对静态数据给予加密，并且借助密钥管理服务也就是 KMS 来实现密钥的生成、轮换以及销毁。当进行数据传输时，应用 TLS/SSL 协议来建立安全信道，以此防止数据在网络传输过程中被窃听或者篡改，软件工程还需要引入数据脱敏与匿名化技术，针对敏感数据像身份证号、银行账户等进行变形处理，在契合业务需求的同时保护用户隐私，在代码实现过程中，要严格依照“数据最小化”原则，避免出现非必要的敏感数据采集与存储，凭借代码审查以及静态分析工具比如 SonarQube 来检测数据安全漏洞，保证数据安全策略在软件开发过程中可得到有效落实。

3.2 身份验证与访问控制

云计算所有的分布式特性，针对身份验证以及访问控制的软件实现环节，提出了更为严苛的要求，软件工程领域需要运用多因素认证也就是 MFA 技术，以此来强化身份验证的可靠程度，它会综合考量密码、生物特征以及硬件令牌等诸多因素去开展身份核验工作，降低身份被冒用的风险。在微服务架构当中，借助身份认证网关像 Keycloak 这样的工具，达成统一的身份管理目标，可为各个服务给予标准化的认证接口，解决分布式环境下出现的身份一致性问题，至于访问控制层面，基于角色的访问控制即 RBAC 与基于属性的访问控制即 ABAC 这两种模型，在代码里达成细粒度的权限管理，举例来说，借助注解或者拦截器针对 API 接口开展权限校验。引入服务网格比如 Istio 的流量认证机制，实现服务之间通信时的身份验证以及授权，避免出现未授权的服务调用情况，构建起从用户直至服务的全链路访问控制体系。

3.3 安全性标准与合规性要求

云计算环境里的软件工程要符合多样化的安全性标准以及合规性要求，需要把合规性要求融入到软件开发的整个流程当中，在需求分析阶段的时候，要明确系统所要遵循的安全标准，像 ISO 27001、等保 2.0，把合规性要求转变成具体的功能需求以及技术指标，到了设计阶段，依据安全标准来做架构设计，比如为了契合数据主权要求，要在代码里实现数据本地化存储的逻辑控制。在开发过程中，借助合规性检查工具，像 OpenSCAP 对代码进行实时扫描，保证编码规范符合安全标准，禁止使用存在安全漏洞的函数库，在测试阶段，除了功能测试之外，还要增加合规性验证测试，模拟安全标准里的审计要求，验证系统是不是有完整的日志记录、安全事件追踪等功能。而且软件工程要建立持续合规监控机制，借助自动化脚本定期检测系统配置和安全策略是不是符合最新的合规性要求，及时发现并且修复合规性漏洞，保证系统一直契合安全性标准。

4 云计算环境下软件工程的可靠性挑战

4.1 系统可用性与故障恢复

在云计算分布式架构里，软件模块之间的依赖关系较为复杂，单点故障有可能借助调用链引发级联失效，从软件工程角度出发，要在架构设计阶段引入容错机制，像采用断路器模式来防止故障扩散，当某服务调用失败率超出阈值时会自动熔断，以此避免雪崩效应，在代码实现方面，要强化异常处理逻辑，区分可恢复性异常和致命性异常，针对可恢复性异常设计重试策略并设定合理的重试间隔与次数，防止因频繁重试而消耗过多资源。软件工程中的混沌工程实践同样关键，借助主动注入故障来验证系统的容错能力，持续优化故障恢复流程，保证系统在复杂故障场景下依旧可保持高可用性。

4.2 负载均衡与资源管理

云计算环境里资源有弹性伸缩特性，这对软件的负载感知以及调度能力提出了更高标准的要求，软件工程要在负载均衡模块当中实现动态权重调整算法，依据服务器的实时负载状况，包含 CPU 利用率、内存占用情况、I/O 响应时间等各项指标来动态地调整分配权重，以此避免静态负载均衡算法所存在的滞后性问题。在资源管理层面，借助容器编排技术，像 Kubernetes 所有的软件定义能力，达成资源的细粒度分配以及动态调度，比如依据 Pod 的资源请求与限制配置，再结合 Horizontal Pod Autoscaler 依据 CPU 或者内存指标来自动进行扩缩容操作 [3]。

4.3 可靠性评估与监控技术

云计算系统有动态性，这要求软件工程构建的是自适应的可靠性评估模型，而不是基于静态历史数据统计的模型，可以引入机器学习算法，针对实时监控数据开展训练工作，建立起预测性评估模型，可提前识别潜在风险。在监控技术实现方面，运用分布式链路追踪技术，从用户请求入口直至后端服务进行全链路埋点，以此精准定位故障节点与性能瓶颈，解决传统监控工具无法跨服务追踪的难题。软件工程还要设计智能告警关联分析机制，借助规则引擎与机器学习相结合的方式，对海量告警实施聚类与关联分析，过滤冗

余告警并确定根因，防止因告警风暴致使运维人员决策失误，提升故障处理效率以及系统可靠性管理水平。

5 云计算环境下软件工程的安全性与可靠性保障技术

5.1 加密技术与密钥管理

随着网络技术的不断发展，网络已经成了人们生活中不可缺少的一部分，而在网络时代下，计算机信息安全问题也日益受到人们的关注和重视。因此，将软件工程和云计算技术进行结合是当前时代发展的必然结果。在云计算的环境里，加密技术以及密钥管理是保障数据安全和隐私的关键办法，数据于存储、传输以及处理的过程当中都要借助加密技术来防止未授权的访问，对于静态数据运用 AES 等高级加密标准来实施存储加密，对于传输的数据借助 TLS/SSL 协议达成端到端加密，对于计算过程中的数据可采用同态加密等技术来保证隐私性[5]。

5.2 身份认证与授权机制

在云计算环境中，身份认证与授权机制是构建安全访问体系的根基所在，要解决多租户、跨域访问等复杂场景之下的身份管理难题。在身份认证这一方面，传统的单因素认证，像是密码这种方式无法契合需求了，需要采用多因素认证也就是 MFA，将生物特征、硬件令牌、动态口令等多种验证方式组合起来。借助指纹识别再结合手机短信验证码的方式来实现强身份认证，以此抵御 Credential Stuffing 等攻击。对于跨云平台或者跨组织的身份交互而言，可以借助安全断言标记语言也就是 SAML 或者 OAuth 等协议来实现单点登录也就是 SSO，避免用户进行重复认证，并且减少凭证泄露的风险，授权机制则需要构建细粒度的访问控制模型，基于角色的访问控制 RBAC 可依据用户角色来分配权限，而基于属性的访问控制 ABAC 可以结合用户属性、环境条件等动态调整权限，依据 IP 地址、时间戳等环境因素来决定是否允许访问。

5.3 安全信息与事件管理（SIEM）

安全信息与事件管理即 SIEM 系统，在云计算环境里充当安全中枢，它把分散的安全数据和事件整合起来，实现对安全威胁的实时监控、分析以及响应。在云环境中，各种各样的设备、应用以及网络组件会产生数量众多的日志数据，SIEM 系统可借助标准化采集接口像 Syslog、API 等，实时收集服务器、网络设备以及安全设备等的日志信息，并且运用归一化处理技术，把异构数据转变为统一格式，方便集中分析。它的核心功能有实时事件关联分析，借助预先设定规则或者机器学习算法识别潜在威胁，比如检测同一个 IP 地址出现多次失败登录尝试并触发告警，安全态势可视化，以仪表盘、拓扑图等形式呈现整体安全状况，协助安全人员直观了解风险分布，事件响应自动化。

5.4 可靠性设计模式与架构

云计算环境中，可靠性设计模式以及架构属于保障系统稳定运行的关键所在，要从架构层面融入容错、弹性以及可恢复性设计。在架构设计这个方面，微服务架构会把系统拆分成可独立部署的服务单元，以此避免单体应用出现单点故障问题，再配合服务网格达成流量管理与故障隔离，分布式架构借助多节点冗余部署，采用副本机制保证数据一致性与可用性，联合地域多活架构实现跨区域容灾，当某个数据中心发生故障时会自动切换到其他区域。在可靠性设计模式上，熔断模式在依赖服务出现故障时可快速切断调用，防止级联失败，限流模式利用令牌桶、漏桶等算法控制请求速率，避免因为过载致使服务不可用，缓存模式减轻后端压力并且提升响应速度，重试模式针对暂时性故障自动进行重试，提高操作成功率，混沌工程凭借主动注入故障来验证系统的容错能力，持续优化可靠性设计。建立完善的故障注入测试机制，在开发和测试阶段模拟各类异常场景，保证架构设计有可靠性，最终达成云系统在复杂环境下的高可用性与稳定性。

6 结语

本文针对云计算环境下软件工程的安全性与可靠性挑战展开了全面的分析，并给出了对应的保障技术。研究结果说明，运用先进加密技术、完善身份认证机制、高效 SIEM 系统以及合理可靠性设计模式与架构，可有效应对这些挑战，未来随着云计算技术持续发展，有必要强化对新兴技术的研究及应用，不断提高软件工程的安全性与可靠性，适应不断变化的应用需求。

参考文献

[1] 霍庆路. 基于云计算的教育软件开发架构与实现方法研究 [J]. 软件, 2025, 46 (04): 77-79.

[2] 陈琨. 信息技术与计算机软件工程的融合应用 [J]. 数字通信世界, 2025, (04): 117-119.

[3] 张效强. 云计算在高职实践性软件开发教学中的应用 [J]. 家电维修, 2024, (08): 28-30.

[4] 陆彦妤. 软件工程中的安全问题与信息安全技术的融合研究 [J]. 信息与电脑(理论版), 2024, 36 (14): 111-113.

[5] 杨嘉康. 大数据时代下软件工程技术的应用研究 [J]. 电子元器件与信息技术, 2022, 6 (11): 148-151.