题目：具有瀑布特征的可信虚拟平台信任链模型及其分析方法

1. 引言

1.1研究背景及意义

云计算是可以使用户按照使用量付费并且获得高效的、快捷的网络服务的新型资源共享模式，其主要目的是在提高网络、服务器、硬盘存储、软件等共享资源利用率的同时，使云租户不再关注硬件资源的管理和维护，云租户只需要在硬件资源上投入很少的管理维护工作就可以得到很高的资源回报。云计算的高效的资源处理能力也带动了大数据、人工智能等相关领域的发展。目前在云计算提高商，比如国外的Intel，IBM，微软，以及国内的腾讯，阿里巴巴都拥有非常成熟的云计算技术和应用服务。云计算的快速发展同时也给云计算带了除传统信息安全、网络安全之外的安全问题，其中，如何向云租户证明云计算底层平台的安全性、虚拟机的安全性是一个非常重要的问题。而可信计算是保障信息系统安全最为重要的技术手段之一，它通过提供数据保护、身份认证、远程证明以及完整性度量等特性提高包括底层物理资源、应用软件等在内的计算平台的可信性和可靠性。因此，将可信计算技术应用在提高云计算环境的安全性是工业界和产业界必须重视。

1.2国内外研究现状

1.3本文主要工作

1.4论文组织结构

1. 理论知识

2.1虚拟化技术

2.1.1半虚拟化

2.1.2全虚拟化

2.1.3流行的虚拟化架构

1. Xen
2. KVM

2.2可信云计算

2.2.1可信计算

2.2.2云计算安全

2.2.3可信云计算

2.3形式化分析方法

2.3.1形式化分析

2.3.2安全系统逻辑（LS2）

2.3.3无干扰理论

2.4本章小结

1. 具有瀑布特征的可信虚拟平台信任链模型

3.1具有瀑布特征的可信虚拟平台（TVP-QT）

3.1.1传统的可信虚拟平台

a.TVP架构

b.缺点与不足

3.1.2TVP-QT架构

3.1.3TVP-QT优点

3.2TVP-QT信任链模型

3.2.1信任模型

3.2.2信任链属性

3.3基于扩展LS2的信任链分析

3.3.1扩展LS2及基本假定

3.3.2m信任链的本地验证及远程证明

1. 本地程序执行
2. 本地可信属性描述

3.3.信任链远程验证

1. 远程验证程序执行
2. 信任链属性的远程验证

3.4实例系统分析

3.5本章小结

1. 基于无干扰+的云计算信任链传递分析方法

4.1无干扰理论缺点

4.2扩展无干扰理论（无干扰+）

4.2.1基本定义

4.2.2优点

4.3基于无干扰+的可信虚拟平台信任链传递模型

4.3.1基于无干扰+的TVP-QT描述

4.3.2基于无干扰+的TVP-QT信任链分析

4.4基于无干扰+信任链传递判定定理

4.4.1云计算下的信任链传递判定定理

4.4.2TVP-QT信任链安全分析

4.5实例系统分析

4.6本章小结

1. 相关实验及分析

5.1实验环境

5.2TVP-QT平台构建

5.3TVP-QT信任链构建

5.4TVP-QT安全验证

5.5本章小结

1. 结论及展望