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

根据NIST定义，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提供技术。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的地方。

可信平台模块TPM(Trusted Platform Module, TPM)是可信计算的核心和关键技术，是可信计算机系统的信任根，通过构建从平台底层硬件到平台上层应用程序的信任链，并结合可信远程证明向平台外部实体提供可信证明。TCG（Trusted Computer Group, TCG）定义的可信计算平台的核心功能：度量、存储和报告等均依赖于TPM；可信计算平台的3个信任根：可信测量根RTM(Root of Trust for Measurement, RTM )、可信存储根RTS(Root of Trust for Storage, RTS )和可信报告根RTR(Root of Trust for Report, RTR)等均与TPM有直接的关系，其中可信测量根RTM由CRTM(Core Root of Trust for Measurement, CRTM)和TPM中的一组PCR存储器组成，可信存储根RTS由TPM和存储根密钥SRK组成，可信报告根RTR由TPM和EK组成。TCG的TPM工作组负责TPM规范的起草、修订和发布，其规范已从TPM1.0、TPM1.2发展到现在的TPM2.0。TPM2.0规范于2014年发布，在密码算法支持、密钥、授权、签名、虚拟化等方面均有些新的特点，尤其在虚拟化方面的更新推动了可信计算技术与云计算技术的结合，共同保障云计算安全，向云租户提供一个安全可靠的云服务。利用可信计算技术构建可信虚拟平台（TVP）是研究的重要方向。TVP可以利用可信计算技术对云计算平台启动过程中，不仅可以对云计算物理资源组件进行信任链可信度量，比如BIOS、操作系统内核OS、虚拟机管理器等，也可以对虚拟机启动的组件进行可信度量，比如虚拟机镜像系统、虚拟机文件、虚拟机虚拟化过程所需的OS、虚拟BIOS等。TVP的出现能够帮助云计算提供商向云租户更好的提供安全可靠的云服务。

根据中国信息通信研究院2017年7月发布的《云计算关键行业应用报告》，2016 年以 IaaS、PaaS 和 SaaS 为代表的典型云服务市场规模达到 654.8 亿美元，增速 25.4%，预计 2020年将达到 1435.3 亿美元，年复合增长率达 21.7%。我国云计算市场总体保持高速增长趋势。2016 年我国云计算整体市场规模达 514.9 亿元，整体增速 35.9%，高于全球平均水平。工业和信息化部发布的《云计算发展三年行动计划（2017－2019年）》提到我国云计算的发展目标“到2019年，我国云计算产业规模达到4300亿元”，该行动计划为我国云计算安全技术创新和产业发展指明了方向，提供了政策保障和法律依托。并且根据McAfee发布的“2017年全球云计算安全报告”显示，在过去15个月，80%的IT预算用于云应用和解决方案。云计算已经成为通过部署应用来销售服务的企业的首要事项。很多企业正在快速向云计算转移，以跟上合作伙伴和供应商的网络。无论顾客选择任何购买渠道和方式，都能提供卓越的客户体验，这也推动了云计算的部署。但是，只有23%的企业完全信任公共云可以保护他们的数据安全。由此可见目前的大部分云租户是不能完全信任云提供商提供的云计算服务，主要是由于云租户在使用云提供商提供的虚拟机时，并不能确认云计算平台上的物理主机是与云提供商按照各自操作系统官方文件进行启动的，以及租户请求的虚拟机是按照预期的配置和要求进行启动的。因为云计算环境下的虚拟机存在着包括传统信息系统安全以及新型网络安全等威胁，比如：虚拟机恶意代码攻击、虚拟机逃逸等，这些都会导致虚拟机在重新启动时的组件被篡改，在云租户对虚拟机进行重新启动时，可能无法判断虚拟机遭受操作系统、数据是否被篡改。而可信虚拟平台的构建可以利用TPM中的可信度量、可信报告等技术向用户发送关于云计算平台的可信度量结果，并且证明自身的安全性。

但是目前针对TVP的研究尚不完善，已有的TVP模型均把云计算底层资源和提供给云租户的虚拟机在构建过程中相分离，并且在利用信任链技术进行可信计算度量时，对云计算底层资源和虚拟机进行两次度量，不仅在逻辑上违背了TCG规定的链式度量方式，也在时间上产生了两条相互断开的信任链模型。

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