# 基于无干扰理论+的云计算环境信任链传递分析方法

齐能1，谭良1,2

1（四川师范大学计算机学院，成都，610068）

2（中国科学院计算技术研究所，北京，100190）

**摘要**：云安全是目前云计算研究的热点之一，作为云安全基础的可信计算，目前仍存在一些关键问题有待解决。针对现有云环境信任链模型过粗且逻辑不完全合理，缺乏实用的形式化分析方法等问题。本文提出一种新的基于无干扰理论的云环境信任链分析方法，首先建立一个具有瀑布特征的可信云环境信任链模型，然后按照云计算环境运行特征，对原有无干扰理论中的安全域、动作等定义进行扩充，并将动作主体和动作对安全域以及系统状态的影响等扩展到无干扰理论中；最后应用此扩展的无干扰理论来分析可信云环境信任链传递模型，用形式化的方法证明当符合非传递无干扰安全策略时，云环境安全域之间的信息流受到安全策略限制，隔离了域之间的干扰，满足此条件时用完整性度量方法所建立的云环境信任链才是可信的、有效的。

**关键字：**云计算；无干扰理论；信任链；安全策略

**A Formal Method Based on Noninterference Plus for Analyzing Trust Chain of Cloud Computing Platform**

QI Neng1, TAN Liang1,2

*(College of Computer Science, Sichuan Normal University, Chengdu, Sichuan, 610068) 1*

*(Institute of Computing Technology, Chinese Academy of Sciences, Beijing, 100190)2*

**Abstract：**The cloud security is one of the hot topics in the research of cloud computing. As is well known, trusted computing is the supporting technology for cloud security. However, unfortunately, there are still some key issues to be addressed for trusted computing. With respect to the issue of the roughness and incomplete-reasonableness of current trusted train and the lack of the practical formal method in the cloud computing platform, this paper puts forward a new cloud platform formal method base on noninterference theory. Firstly, this method builds a trusted train model with waterfall characteristic in the trusted cloud computing platform. Then according to the running characteristic of cloud computing platform, this paper extends some basic definitions based on the original noninterference theory, such as security domains,actions. And this paper extends the actions’ subjects and the actions’ influences on the security domains and system status to the noninterference theory. Finally, this paper analyses the trusted train of trusted cloud computing platform by using the extended noninterference theory.And this paper proves the information flow among the domains of cloud platform can be limited by security policy and can isolate the interference among the domains when the cloud platform meets the intransitive noninterference policy,which is mainly analyzed by the formal method.As a result, the trusted train of cloud computing,is credible and valid,which is built after integrity measurement.

**Key Words:** Cloud computing,noninterference theory,trusted train,security policy

## 引言

当前，云计算受到了学术界和工业界的广泛关注。随着云计算的不断普及，安全问题已经成为制约其发展的关键因素之一[1-3]，越来越多已应用到云计算的可信系统受到来自不同方面的实质攻击。Gartner 的调查结果显示，70%以上受访企业的CTO认为近期不采用云计算的首要原因在于对云计算中数据安全与隐私问题的担心。Amazon、Google等世界级大型云计算应用厂商近年来不断爆出的各类安全事故，更加剧了人们对于云计算安全的担忧。RSA 首席技术官Bret Harman 指出：“基础设施安全是云计算安全的三个重要研究方向之一”。惠普云计算专家Goldsack 则认为，“对于基础设施安全，必须增强其安全性和隐私性”。可信计算作为增强信息系统安全和隐私的重要技术，将其融入到云计算当中，并以可信赖的方式为云计算提供基础设施安全服务已成为目前云计算研究的重要方法[1-6]。

随着可信计算经过十多年的发展，国内外许多学者对其理论、模型、算法、系统、测评等展开了深入细致的研究，取得了丰硕的成果[7-15]。然而，作为云基础设施安全的关键理论和技术，可信计算自身仍然存在一些关键科学问题有待突破。如何在云计算环境下要对构建平台信任的基石——信任链进行形式化建模与分析，以确保平台信任的可验证，是一个解决云计算环境信任链的重要问题[18]。这个问题不解决，基于可信计算的云安全就仍然存在着安全隐患。针对于云计算环境下的可信计算平台信任链即分析方法主要存在以下问题。

首先，针对于云计算环境可信平台信任链，现有的信任链模型过粗且逻辑不完全合理，主要表现在：(1）目前对可信云环境的基础—可信虚拟平台模型的研究中，大部分把虚拟机管理器（VMM）和OS相关部分作为虚拟机的可信信任根（vRT），这样显然是不精细，在此基础上进行的信任链分析也显然存在逻辑上不完全合理的问题。（2）虚拟平台信任链与虚拟机信任链是两条不同的信任链，即在整个云计算平台以及客户虚拟机启动过程中存在两条完全分隔的信任链，一条是可信虚拟平台在启动时的信任链，另一条是客户虚拟机在启动时的信任链，这两条信任链在度量层次和度量时间上均是分离的，无法向用户展示一条完整的信任链。

其次，针对于云计算环境下的信任链传递分析方法，已有的研究无法正确的表示可信云计算环境下的信任链传递验证过程。一方面，已有的形式化分析方法主要关注通信协议的安全性分析，比如BAN逻辑[19]、应用π演算[20]等，它们不适合应用系统内部程序的安全性分析（比如云环境中不同的安全域等），而且现有针对可信平台信任链的形式化分析通常或者侧重于本地信任链的构建与验证[21,22]，或者侧重于信任属性的远程证明[23-25]，因此不够全面且不具有普适性；另一方面，由于虚拟化平台的特性（如多虚拟机并发、内存隔离、访问控制等），使得针对普通可信平台的分析方法不能直接应用于可信云计算环境。

本文针对以上问题，首先建立了一种具有瀑布特征的信任链模型TC-QT，该模型以虚拟化硬件层物理可信平台模块（TPM）为起点，在可信虚拟平台TPM到特权域Domain0启动信任链和可信虚拟机信任链之间加入可信衔接点，该模型中可信衔接点具有承上启下的瀑布特征，能满足云环境的层次性和动态性特征，保证了整个可信虚拟平台的可信性。其次，本文按照云计算环境运行特征，对原有无干扰理论中的安全域、动作等定义进行扩充，并将动作主体和动作对安全域以及系统状态的影响等扩展到无干扰理论中。最后基于建立的TC-QT模型，应用此扩展的无干扰理论来分析可信云环境信任链传递模型，用形式化的方法证明当符合非传递无干扰安全策略时，云环境安全域之间的信息流受到安全策略限制，隔离了域之间的干扰，满足此条件时用完整性度量方法所建立的云环境信任链才是可信的、有效的。

## 相关工作

目前，可信云计算条件下的信任链形式化方法以及无干扰理论，得到了国内外学者的广泛深入和研究，本文就目前对可信云环境下的信任链模型、信任链形式化分析方法以及无干扰理论的相关研究进行了以下总结和分析。

针对于可信云计算环境下信任链模型的构建过程，主要包括三个方面。其一是通过对TCG链式信任链模型的扩展，实现可信云环境下可信度量以及信任传递。Scarlata[26]等提出在构建信云环境时，通过可信测量构建从CRTM可信根到每个客户虚拟机的信任链，就可以证明每个客户虚拟机是可信的。John[27]对信任链扩展上提出了“Transitive Trust Chain”信任链模型，并且简要的指出了信任链传递过程为TPM 🡪VMM🡪TVEM manager 🡪TVEM🡪 VM OS🡪应用程序。Shen[28]等根据TCG动态度量方法提出了一种基于Xen的可信虚拟机在 DRTM下的信任链构建，其具体的构建过程为：CPU🡪可信代码🡪Xen VMM🡪Dom0（vTPM Manager🡪Domain Builder）🡪 Guest 0S 🡪Guest Application。此类信任链模型，无法正确的对可信云计算环境的具体的运行机制进行描述，信任链模型逻辑不清楚。其二是通过研究可信云平台和可信虚拟机两部分的信任链，构建可信云环境下的信任链模型。常德显[29]等提出可信云环境信任链包括按照信云环境的功能层次从硬件TPM层🡪TCB层🡪vRT层🡪用户虚拟机层的信任链模型。Zhang[30]等提出一种基于无干扰的可信域层次信任链模型，并且指出分别度量物理主机和VM的方式，即首先度量从物理的TPM到物理主机的应用程序，然后度量VM的vTPM和应用程序。此类信任链模型存在vRT及层次间的连接定义比较模糊以及不能向用户虚拟机呈现一条完整的信任链模型的问题。其三是树形或者星形的信任链模型。一部分学者认为TCG的链式信任链可信度量方式在虚拟化环境下是难以有效构建的。朱智强[31]提出了一种安全可扩展的星型信任度量结构，在信任度量时只需要信任根（RT）对管理域节点进行度量即可。曲文涛[32]等提出了一种解决RT负担的改进方案，带链式结构的星型信任链模型，设计了MDn节点分担了RT的部分度量负担。此种信任链模型存在负担重的RT或其他节点。综上，大部分针对于可信云计算环境中的信任链研究大部分都是对系统的信任链构建过程，缺少一种针对于可信云计算平台的信任链分析方法，没有对可信云计算环境系统符合的安全策略以及定理进行说明和验证。

针对于确保平台信任可验证的信任链形式化建模与分析的方法，目前的研究大部分是基于传统的可信计算平台。陈书义[21]等人利用一阶逻辑对可信计算平台启动过程进行建模以分析其信任传递过程，并提出长度受限的信任链模型。张兴[22]等人基于无干扰模型对信任链进行了建模分析，从系统信息流控制角度验证满足传递无干扰安全策略的信息流才能构建有效的信任链。上述方法主要针对普通可信计算平台，并不能直接适用于云计算环境下信任链形式化分析。虽然Zhang[30]等人利用无干扰理论对可信云计算环境信任链进行了形式化分析和验证，但是此种信任链分析方法是建立在不连续的可信云计算信任链模型上，不能够对可信云计算环境进行正确的形式化验证。常德显[29]等人基于扩展安全系统逻辑的分析方法也存在Zhang中的问题。

针对于无干扰理论的研究，目前大部分的研究是基于信息流的无干扰模型从动作和运行结果的角度建立系统安全策略模型**。**张兴、赵佳[33,34]等在Rushby[35]的无干扰理论的基础上将系统安全域集实体化为进程集，给出了进程运行的可信条件，推导出系统运行可信定理，保证了终端的安全，但是其模型中的没有针对动作的详细定义，不适合验证可信云环境信任链。刘鹏威[36]等提出了基于非传递的无干扰理念的二元多级安全模型，在Rushby无干扰理论的基础上重新定义了清除函数，将传递的元干扰理论过渡到非传递的无干扰理论，并依据BLP和Biba模型保护了信息的机密性和完整性，然而同样存在赵佳中的问题。陈菊[37]等从进程数据和代码完整性检测出发，利用无干扰理论保证进程之间的操作合法，试图在不安全的操作系统中建立安全的应用支撑。徐甫[38]等扩展了非传递无干扰理论，并试图通过重新定义静态干扰和动态干扰，使其支持进程自身代码的修改，但是其静态干扰和动态干扰的定义过于抽象，难以和实际的终端系统相对应，因此并不能在实际上完成其所描述的支持自身代码修改的功能。秦晰[39]等提出了一种容忍非信任组件的可信终端模型，该模型利用可信组件对非信任组件的输出进行封装，保证了非信任组件在终端上的存在不会造成严重的安全威胁，实现了域间隔离和无干扰，保证了结果的可预测性和可控性，但是并没有针对安全域进行详细的描述。上述对无干扰理论的研究，均没有考虑到云计算运行中时的安全域、动作所属主体以及动作对安全域和系统状态的影响进行详细的说明，比如针对于安全域，在运行中各个安全域可能是独立也可能是通过组件绑定在一起。

综上所述，目前针对于可信云计算环境的信任链构建模型存在逻辑上不合理、缺少实用的信任链分析方法，并且原有的无干扰理论也不能直接对可信云环境信任链进行分析。如何建立一个正确的信任链模型，以及去和对无干扰进行扩充，使其可以对信任链模型进行形式化分析，是目前急需解决的问题。

## 基本定义

遵从Rushby等人的描述，本文以自动机（或叫状态机）的形式，并在安全域、动作等对无干扰进行扩充，在动作主体、动作主体对安全域和系统状态的影响扩展到无干扰理论中，给出无干扰的基本定义如下。

**定义1.** 系统M由如下要素构成：

1. 一个包含唯一初始状态的状态集。约定使用等表示系统状态；
2. 一个由系统中所有原子动作组成的动作集，约定用等表示原子动作；
3. 一个由系统中所有发出原子动作的动作主体集，每一个主体可能发出不同的动作，相同的动作也可能由不同的主体发出。即每一个属于中的动作都有一个包含于中的主体集。即动作的主体集。
4. 一个由系统中所有行为构成的行为集。其中，行为表达为原子动作序列的形式，约定用希腊字母等表示行为。一个行为的示例是，其中是连接符；
5. 一个输出集，其中包含了使用动作进行观察时所看到的结果；
6. 每一个原子动作以及原子动作的主体都有自身所属的并且不可再分的Min安全域，这些安全域构成的集合称为Min安全域集；安全域中的主体向系统发出操作动作与系统进行交互，并且能够观察到相应的结果。安全域的划分可以限制系统中的信息流动。并且根据云计算环境运行机制，安全域集的某一子集也可能单独成为运行的一个组合安全域，这些由子集组成的组合安全域称为，且中任意两个元素可能存在交集。即对于，有。且对应与系统状态，域也有相应的状态，用表示域状态集合，约定使用分别表示安全域的状态在系统状态为本安全域状态，显然有

。

1. 安全策略和。安全域集之间可以有信息流动，信息是否能够在特定域间流动由安全策略和决定，和分别称为干扰和无干扰关系，两者互为补集；
2. 动作主体到动作的映射函数：。返回一个特点动作所属的动作主体；
3. 安全域到动作的映射函数：。返回一个特定动作所属的Min安全域，并且必然，使得。
4. 单步系统状态函数：。.单步函数描述的是系从前一个状态，由某一安全域某一动作主体执行某个动作之后，应该到达的后一个状态；在系统存在安全域中的主体，执行动作之后，对系统的改变为。同理，动作对动作所属安全域的改变单步域状态函数为，在安全域在下的主体，执行动作之后，对安全域改变为。

且单步状态函数满足以下条件：

。

1. 行为结果函数：。行为结果函数给出了：在状态使用特定的动作所观察到的行为执行结果。
2. 行为执行函数：。如果用表示空动作序列，则可以表示为右递归的形式：

对于系统状态：



对于安全域状态：

。

需要强调的是，无干扰模型将输入定义为行为，也就是原子动作的连接序列。本文遵从原有的无干扰理论，对系统进行描述。

**定义2** .系统视图。

系统视图对应于实际机器M，其关注于存储单元(内外存单元、芯片存储单元等)及其取值，以及可观察存储单元、可修改存储单元等内涵。

1. 存储单元集。机器的每一个存储单元都有一个名字。所有存储单元名字的集合构成存储单元集，又叫做名字集。
2. 系统视图值集。每一个存储单元在特定的状态都会有一个特定的值。具体的取值可以由下面的内容函数计算。所有取值的集合构成值集。
3. 系统视图内容函数。

**定义3** .域视图。

域视图对应于M中的安全域，是M视图的子集。

对应于系统状态等相关内容函数，域视图有以下表示：

1. 域视图值集。安全域中每一个存储单元在特定的状态都会有一个特定的值。具体的取值可以由下面的域视图内容函数计算。所有取值的集合构成值集。
2. 域视图内容函数。
3. 域视图观察函数和域视图修改函数。观察函数和修改函数分别给出了特定的安全域所能观察和修改的存储单元的集合，其中是幂集计算。

**定义4** .主体视图。

1. 在整个系统M中，域中有很多可以发出动作的主体，即

。

亦有。

仅次于安全域的单位为动作主体，动作主体对应系统中的存储单元在域不同状态下，由动作发出后，其存储单元也会改变。

主体视图值集。动作主体每一个存储单元在特定的状态下都会有一个特定的值，其中有。具体的取值可以由下面的主体视图内容函数计算。

1. 主体视图内容函数。
2. 主体视图观察函数和主体视图函数。不同的主体能观察和修改的存储单元的集合不同。

**定义5.**关系称为是等价关系，当且仅当同时满足输出一致性和（弱）单步一致性。

1. 输出一致性：。

在系统视图上：。

并且由可得域视图的输出一致性：

。

1. （弱）单步一致性：

对于传递安全策略，需满足单步一致性：

。

对于非传递安全策略，需满足弱单步一致性：

。

与单步一致性相比，弱单步一致性增加了条件，这个条件很重要。这是因为：弱单步一致性对应的是非传递无干扰，因此其除了要考虑直接干扰关系之外，还要考虑间接干扰关系上的“单步一致性”。注意：本文中遵从Rushby的符号表达，约定使用表达蕴含关系。

**定义6.**间接干扰关系。

对于非传递安全策略而言，安全域虽然不能直接干扰安全域（因为），但是，仍然可以间接对进行干扰(因为)。若将定义1当中的干扰关系称作是“直接干扰关系”，则可以定义“间接干扰关系”如下:



**定义7.**干扰源集。

干扰源集的递归定义如下:

，且



，且。其中，。

干扰源集的含义是:抽取所有对安全域有直接或间接干扰关系的安全域形成集合。

**定义8.**弱预期函数。

，且

。

其中，，

。

弱预期函数的含义是，“将所有对安全域有直接或间接的干扰关系的动作保留，并将除此以外的所有动作删除”，从而得到在非传递无干扰安全策略控制下的预期行为。 **定义9.**域集等价关系:。

并且Rushby定义了系统满足非传递性无干扰策略的判定定理。

**定理1 .**系统满足非传递性无干扰策略的判定定理。

设M 是一个视图隔离的系统，有一个具有非传递性的～>策略，并且M满足：输出一致性、弱单步一致性和局部干扰性，则M 满足非传递性无干扰策略。

## 云计算环境下信任链传递模型分析

### 4.1目前

由可信的定义可以看出，可信的核心内容在于组件行为的可预测性。组件行为各有不同：对应用程序来说，它的行为包括输出屏幕信息、显示图片、发出声音、创建网络连接等等；对内核来说，它的行为包括产生进程、管理内存、访问控制等等。这些不同的行为都符合有限状态自动机模型的抽象描述：一个状态确定的系统，其行为是可以预测的，即一个固定的输入队列可以有一个固定的输出队列，也就是这些行为都可以通过信息系统的状态和输出来表现。而且，从组件外部来看，它们只能通过输出来表现。

因此根据可信的定义，一个初始状态确定、输入确定的有限状态自动机系统是一个可信系统。但在现实系统中，组件的状态除了取决于自身（通常是代码、堆栈、数据），还受其所处环境的影响（包括硬件平台、操作系统、系统中其它的组件的影响），也就是说组件不是一个状态孤立的有限状态自动机，而是一个部分状态受其它关联组件控制的状态机。系统是否可信由其组件和组件之间的交互所决定。这里的组件可以是一个硬件模块、软件模块、应用程序等。组件的可信性可以由图-的模型表示，模型包括4个元素：组件、输入、输出和组件间的干扰。组件运行是否可信，用组件输出是否符合预期来表示，因此一个组件运行可信取决于3个因素：

（1）完整性因素。即组件本身没有被篡改过；

（2）输入因素。组件的输入在允许范围内；

（3）干扰因素。其它组件对其状态没有干扰。



图1 组件间干扰造成运行不符合预期示意

可见：如果组件本身没有被篡改，并且组件间不存在干扰，则组件的输出符合预期，系统中组件的运行是可信的。所以，如果要使信任链传递有效，必须消除组件之间的干扰。

并且在针对云计算环境的运行机制，

### 4.2具有瀑布特征的信任链传递模型

本文为解决上文对目前云计算环境下信任链传递出现的逻辑不完全合理，信任链展示不完整等问题，建立了了一种具有瀑布特征的云计算环境下的可信虚拟平台架构（TVP）TVP-QT，并对TVP-QT信任链传递模型进行了构建，建立了拥有可信衔接点的TVP及其完整的信任链模型。该模型以虚拟化硬件层物理TPM为起点，在可信虚拟化平台信任链和可信虚拟机信任链之间加入可信衔接点。当信任链从可信云平台传递到可信衔接点时，由可信衔接点负责对可信虚拟机的vTPM及相关组件进行度量，之后再将控制权交给虚拟可信平台模块(vTPM，virtualization trusted platform module)，由vTPM负责对虚拟机的VBIOS，VMOS到VM应用进行度量。该模型中可信衔接点具有承上启下的瀑布特征，能满足云环境的层次性和动态性特征，保证了整个可信虚拟平台的可信性。

 图2 TVP-QT运行架构

首先本文对TVP-QT架构进行描述。从功能上看TVP-QT运行架构可以主要分为5个层次，硬件信任根TPM可作为虚拟化平台的底层，从物理上保障虚拟化平台；第二层主要包括VMM及管理域相关组件，我们把管理域记作Dom0，针对不同的VMM，Dom0的启动会有不同的方式。例如，Xen 的管理域启动相关组件包括运行中涉及的VOSLoader、VOS等组件，这层次可以作为TVP-QT的可信计算基（TCB）。值得指出的是，与已有的TVP不同，我们只把Dom0 kernel看成是可信基，这显然更为合理，因为Dom0实际上是整个虚拟化平台的管理域，含大量的应用程序，这些管理程序无法采用TCG链式度量，且也很容易受到攻击而改变[23][24]。第三层是我们重点设计的可信衔接点，可信连接点位于Dom0，是Dom0的一组应用程序，包括VM的创建组件VM Builder、 vTPM实例的创建模块vTPM Builder以及VM-vTPM映射组件VM-vTPM Binding，且作为vRT的一部分，在信任链上按照VM Builder🡪vTPM Builder🡪 VM-vTPM Binding的顺序依次进行度量。可信衔接点可对TVP-QT的第一、第二层与第四、第五层进行有效衔接，保证TVP-QT信任链构建的连贯性，起到承上启下的作用，具有瀑布特征。第四层为vTPM。vTPM作为可信虚拟机部分的虚拟信任根，是由可信衔接点为虚拟机创建的vTPM实例，它可利用TCG的动态度量信任根（DRTM）机制启动，作为虚拟化平台应用进程的一部分。最上层为用户虚拟机层次，是可虚拟化平台上与用户密切相关的虚拟机部分，其运行时组件包括VBIOS、VOSLoader、VMOS、应用程序(APP)等相关组件。

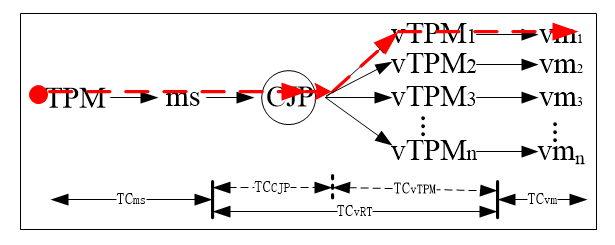


图3 虚拟化平台可信环境信任链构建与验证

其次，本文对TVP-QT信任链传递模型进行进一步描述。TVP-QT信任链传递模型：第一层硬件TPM（CRTM）🡪第二层TCB（BIOS🡪OSLoader🡪VMM🡪Dom0 Kernel）🡪第三层可信衔接点（VM Builder🡪vTPM Builder🡪VM-vTPM Binding）🡪第四层vTPM（vTPM实例）🡪第五层可信虚拟机（VBIOS🡪VOSLoader🡪VMOS🡪APP），将TVP-QT信任链分为三部分，第一部分就是虚拟化平台，包括TVP-QT信任链的第一层和第二层，第二部分是可信衔接点CJP，就是TVP-QT信任链的第三层，第三部分是用户虚拟机，就是TVP-QT信任链的第四层和第五层。

并且本文构建的TVP-QT架构及其信任链传递模型具有以下优点：

（1）TVP-QT信任链模型具有瀑布特征。CJP将分离的两条信任链链接起来，保证TVP-QT信任链构建的连贯性，起到承上启下的作用。

（2）TVP-QT信任链模型解决了虚拟平台信任链与虚拟机信任链的衔接问题。虚拟化平台存在两条信任链，其一是虚拟平台在启动时的信任链，其二是客户虚拟机在启动时的信任链，这两条信任链在度量层次和度量时间上均是分离。这两条信任链如何衔接？已有的TVP信任链模型对这个问题没有具体回答，比较笼统。而是TVP-QT信任链模型回答得具体清楚。

以上的TVP-QT的优点可适应于云计算环境的运行机制，以及能够更加方便的对其进行形式化分析。

### 4.3TVP-QT信任链模型定义

本文结合第三节扩展后的无干扰理论，以及针对具有瀑布特征的信任链传递模型，给出云计算环境下的信任链传递模型的形式化描述。

遵循本文第三节对Rushby等以及扩展后的无干扰定义，对可信虚拟平台进行定义，方便后文的形式化分析。

**定义11** TVP-QT是具有可信功能的虚拟化计算平台，主要包括2类功能组件：TVP-QT:={MS, RT}，MS表示虚拟化平台所有主机类型集合，包括构成虚拟化平台的基本组件VMM、管理域内核、可信衔接点及用户虚拟机等，它们是利用虚拟化技术为用户提供资源与服务的主体；信任根（RT，root of trust）是构建 TVP信任环境的基础，也是 TVP 的核心组件，对虚拟化平台来说，它包括硬件TPM 、可信衔接点CJP和 vTPM。

对于 TVP 的主机 MS，根据其类型进一步细化为 MS:={ms, vm}，其中，ms:={VMM, Dom0Kernel，CJP}，特指底层的VMM、Dom0Kernel和可信衔接点CJP（trusted joint point），它们是 TVP 的TCB 的主要组成部分。vm:={vm1,…,vmn}，表示虚拟化平台上层的用户虚拟机vm 集合。且vmn可以划分为vmn:={VBIOS,VOSLoader,VMOS,APP}.

相似地，TVP的信任根也进一步分类为RT:={TPM, vRT}={TPM,（CJP，vTPM)}，其中，TPM 是硬件信任根，主要用于为物理平台提供信任保障，它拥有非易失存储及密钥存储等固有特性；vRT 包含CJP和vTPM，在功能实现上可表现为ms中内核组件或独立的可信组件，这里将其抽象为一个独立功能组件，通过特定的映射关系与硬件信任根TPM关联以确保其可信性。其中vTPM是软件形式的TPM，具有TPM的安全功能；CJP 是可信衔接点， CJP依赖于物理TPM，用来衔接底层虚拟化平台ms和顶层的虚拟机vm。

即从功能角度上：

TVP-QT:= {(TPM, ms), (vRT1, vm1),…, (vRTn, vmn)}

= { (TPM, (vmm, Dom0 Kernel, CJP) ),((CJP, vTPM1),vm1), …,( (CJP, vTPMn), vmn) }

对应于第三节无干扰理论的相关概念，其中TVP-QT为系统M，安全域为M中涉及到的每一个度量层次。

其中={TPM,vmm,Dom0 Kernel, CJP,vTPM1,vm1,...vTPMn,vmn}={TPM,vmm,Dom0 Kernel, CJP,vTPM,VBIOS,VOSLoader,VMOS,APP};

={ms,vm,TPM,vRT}={TPM,TCB,TJP,vTPM,vm}={MS,RT}；

由上式可见，域中组件是无交集的，而在中就会存在有交集的安全域ms和vRT，在此安全域层面上来看，现有的利用无干扰理论对信任链进行分析的方法也是存在部分缺陷的，没有考虑到真实的“安全域”是可能存在交集的情况。

### 4.4TVP-QT信任链传递**形式化**描述

本文基于扩展后的无干扰理论，对TVP-QT信任链模型进行形式化描述。由于扩展后的无干扰理论从系统主图、域视图、主体行为视图由一个整体系统向系统内的主体进行细分，本文针对TVP-QT信任链传递模型，从以下方面对信任链进行形式化描述。

**定义12：**信任关系可以用以下二元关系表示：（针对于安全域级），（针对于组合安全域级），（针对于动作主体级）。，若，则表示域对域进行了可信度量，并且度量成功，域对域是信任的，然后进行控制权的转移。

首先，按照Min安全域的信任传递方式，可以表示以下式子：



其中表示为可信虚拟平台的可信度量根：即图2中TPM下的CRTM。

按照组合安全域的信任链传递方式，可以表示为以下公式：



基于可信计算技术的装载前度量技术实现的可信链可以这样形式化地描述：

；

表示如果由安全域通过摘要运算获得的摘要值与预期值相等,则安全域信任组件,信任关系将由传递至系统控制权也转移到其中digest(A,B)表示安全域A对安全域B进行摘要运算的结果，expect(A)表示组件A的完整性预期值，表示控制权从A转移到B。

同理对应组合域有：

。

## 云环境下下无干扰信任传递判定定理

单纯的通过完整性验证实现的信任链传递是否有效无法进行验证。只有当系统具有特定的安全机制，满足一定的安全策略，组成系统的各安全域之间的信息流动受到一定安全策略限制，使得组件的运行不受干扰，这时，用完整性度量方法所建立的信任链才是有效的。非传递无干扰关系描述的是一种隔离性要求比较严格的通道控制安全策略，具有非传递无干扰关系的系统组件之间只有直接干扰关系，不存在间接造成的干扰关系。信任链传递模型关键之处是验证系统中是否满足非传递无干扰关系，但从非传递无干扰关系的定义出发很难进行验证，本文给出无干扰信任传递判定定理，用于判定可观测的系统状态和输出在满足什么条件时，信任链的建立和传递才是有效的。

下面本文分别从系统、安全域（和）、动作主体三个角度对本文提出的信任链模型应该满足的安全策略进行描述和分析验证。其中，从系统角度描述系统符合的安全策略，则需要对安全域的输入和系统状态的论述。同理，从安全域角度描述安全策略，则需要对动作主体的输入和对系统状态的进行论述。

**定理2** TVP-QT系统满足非传递无干扰关系的判定定理。

1. 系统的域满足输出一致性。即一个内部操作动作造成的输出影响只依赖于发出动作域的系统视图。且满足一下条件：



1. 相对于（1），系统的动作主体满足输出一致性。即一个安全域内的操作动作造成的输出影响只依赖于发出动作动作主体的系统视图。

；



1. 系统中发生的一个动作造成的对系统状态影响只与发出该动作的域的上一状态系统视图相关联。

；



1. 相对于（3），系统中发生的一个动作造成的对安全域状态影响只与发出该动作的动作主体的上一状态系统视图相关联。

；

1. 系统中，如果一个动作改变了其动作主体的值，则发出该动作的主体一定可以写、访问该主体的系统视图，并且可以写、访问该动作所在的域的系统状态。

；



1. 系统内对系统内的系统状态的操作有以下关系。



1. 系统内若发出某一动作，则该动作的动作主体，所属域唯一确定的。

，在系统状态，必然存在，，可唯一确定。

证明：

根据无干扰给出的定理1，系统需要满足输出一致性，单步一致性，局部干扰性即可。

（1）证明输出一致性：

（2）证明单步一致性：

需要证明：

①

②

式②是在域状态下的单步一致性，是在式①动作主体在域状态的延伸，本文在此只证明式①。

，存在下式：



若，由定理2条件（2）可得：

；

若，由定理2条件（2）可得：

，

其他情况下：；

又由也可得



（2）证明单步一致性：

即证明：

亦可从其逆否命题证明：

，。

由定理2条件（3）可得

，

由定理2，可得成立。

（3）对动作确定性的证明。

上述给出了一个计算机系统满足非传递性无干扰关系的形式化规范，也给出了一种判定可信计算平台信任链传递关系的有效方法。

## 实例系统分析及验证

我们基于开源的虚拟机监视器( VMM) 系统Xen，结合本文第三节介绍的TVP-QT平台，利用虚拟隔离实现了一个满足非传递无干扰的系统。它将应用完全隔离，各应用之间不能直接共享信息，所有隔离域之间的信息交换均通过虚拟机监视器进行。并在此平台下，验证了TVP-QT信任链是符合非传递无干扰判定定理。

（http://wangzan18.blog.51cto.com/8021085/1727106备用）

该实例系统基于 XEN半虚拟化平台，如图4，其中，vRT被分散在dom0、vTPMmanager域和vTPM域。本节我们根据第3节中对TVP-QT信任链的描述：第一层硬件TPM（CRTM）🡪第二层TCB（BIOS🡪OSLoader🡪VMM🡪Dom0 Kernel）🡪第三层可信衔接点（VM Builder🡪vTPM Builder🡪VM-vTPM Binding）🡪第四层vTPM（vTPM实例）🡪第五层可信虚拟机（VBIOS🡪VOSLoader🡪VMOS🡪APP），将TVP-QT信任链分为三部分，第一部分就是虚拟化平台，包括TVP-QT信任链的第一层和第二层，第二部分是可信衔接点CJP，就是TVP-QT信任链的第三层，第三部分是用户虚拟机，就是TVP-QT信任链的第四层和第五层。



图 基于Xen的TVP-QT系统

如图所示，从TVP-QT第一层到系统最上层存在着很多不同的组合安全域，比如TPM域、VMM域等，并且针对系统中的可信衔接点CJP的不同组件是存在于不同的组合安全域中。由CJP存在域不同的安全域中可知本文对安全域和组合安全域的划分是正确的。并且CJP中的某一组件若发出动作，可能存在与Dom0域也有可能存在vTPM Manager域中。并且Dom0中的组件主体发出的某一动作可能会与信任链信息流传递时与CJP中发出的某一动作相同，但是在对信任链是无干扰的，验证了在系统上对动作发出主体的定义的有效性。

由于TVP-QT系统之上可以并行运行虚拟机，根据信息流的不同情况，本文对实际系统的无干扰验证分为两种情况进行验证。

**情况1：存在一个用户虚拟机**

在此种情况下虚拟机运行在VMM之上，VMM系统上的设备驱动模型由运行于虚拟机上的前端驱动和运行于VMM之上的后端驱动组成，实现对硬件功能的使用。该用户虚拟机在运行过程中产生的信息流可以从图中的顺序进行传递。若使该虚拟机信任链有效，必须确保系统中存在非预期的干扰。

依据定理2，该系统中的I/O设备驱动程序满足如下要求：

1. 由输出一致性的定义可知，该虚拟机使用的虚拟资源可以由VMM进行分配，并且不存在其他虚拟机无干扰的动作存在。
2. 由局部干扰性定义可知，VMM系统中，虚拟I/O设备除其所在的虚拟机外其它虚拟机不能改变它的运行状态，I/O设备驱动与虚拟设备间所传输的数据对其它虚拟机是不可见和不可修改的。该VMM系统的隔离机制确保虚拟机必须采用虚拟设备接口访问后端驱动程序。
3. 由弱单步一致性可知，该虚拟机在运行过程中的动作只会对此系统进行状态的改变。

**情况2：存在多个用户虚拟机**

该情况下，在存在一个用户虚拟机之上在运行多个虚拟机，多个虚拟机需要共享设备资源，仅仅对在情况1下增加了虚拟机之间的信息流的无干扰情况。因此本文对多个虚拟机在系统中共享资源的同时进行无干扰的验证。

如图为多个用户虚拟机IO操作示意图：



图 多个用户虚拟机IO操作示意图

（1）由输出一致性的定义可知，VMM维护的虚拟资源必须具有其属于哪个虚拟机的属性标识。可以保证系统中的输出信息可以定位到某一个虚拟机，此虚拟机的不同状态下产生的操作不干扰其他虚拟机的运行。

（2）由局部干扰性定义可知，VMM系统中每个虚拟机能够访问的I/O寄存器被限制，能够禁止未授权的访问。

（3）由弱单步一致性定义可知，对于若干虚拟机共享的客体对象，VMM系统必须具有同步保护机制以防止不同虚拟机对该资源的竞争。

该系统依据非传递无干扰策略模型对传统VMM的虚拟I/O设备体系进行了改造，只要根据应用程序需求，合理划分安全域，各应用安全域的运行不受其它应用程序干扰，依据本文给出的TVP-QT信任传递模型，经过完整性验证，系统运行能够达到可信目标。

## 结束语

利用可信计算技术构建可信虚拟平台并且构建信任链模型是目前解决云计算安全一个重要的研究方向。本文针对现有云环境信任链模型过粗且逻辑不完全合理，缺乏实用的形式化分析方法等问题，提出一种新的基于无干扰理论的云环境信任链分析方法。本文首先建立一个具有瀑布特征的可信云环境信任链模型，然后按照云计算环境运行特征，对原有无干扰理论中的安全域、动作等定义进行扩充，并将动作主体和动作对安全域以及系统状态的影响等扩展到无干扰理论中；最后应用此扩展的无干扰理论来分析可信云环境信任链传递模型，用形式化的方法证明当符合非传递无干扰安全策略时，云环境安全域之间的信息流受到安全策略限制，隔离了域之间的干扰，满足此条件时用完整性度量方法所建立的云环境信任链才是可信的、有效的。最后本文基于Xen系统实现了信任链模型，并利用无干扰理论对该信任链模型进行了分析和验证，证明了扩展后的无干扰理论验证信任链模型的有效性。

## 参考文献：

[1]冯登国, 张敏, 张妍等. 云计算安全研究. 软件学报, 2011,22(1): 71-83

[2] .林闯, 苏文博, 孟坤等. 云计算安全: 架构、机制与模型评价. 计算机学报, 2013, 36(9): 1765-1784

[3] 俞能海, 郝卓, 徐甲甲等. 云安全研究进展综述. 电子学报, 2013,41(2): 371-381

[4] 丁滟, 王怀民, 史佩昌等. 可信云服务. 计算机学报, 2015, 38(1):133-149

[5] SHEN Chang-Xiang, ZHANG Huan-Guo, WANG Huai-Min, et al.Research on trusted computing and its development. Sci China Inf Sci,2010, 53(3):405-433

[6] 李晖, 孙文海, 李凤华等. 公共云存储服务数据安全及隐私保护技术综述[J]. 计算机研究与发展, 2014, 51(7):1397-140

[7] 冯登国等. 可信计算——理论与实践. 北京:清华大学出版社, 2013

[8] 冯登国, 秦宇, 汪丹等. 可信计算技术研究. 计算机研究与发展, 2011,48(8): 1332-1349

[9]杨波, 冯登国, 秦宇等. 基于TrustZone的可信移动终端云服务安全接入方案, 2016, 27(6): 1366-1383)

[10] SHEN Chang-Xiang, ZHANG Huan-Guo, WANG Huai-Min, et al.Research on trusted computing and its development. Sci China Inf Sci,2010, 53(3):405-433.

[11] ZHANG Huan-Guo, YAN Fei, FU Jian-Ming, et al. Research on theory and key technology of trusted computing platform security testing and evaluation. Sci. China Inf. Sci., 2010, 53(3): 434-453.

[12] Reiner S, Xiaolan Z, Trent J, Leendert V D. Design and implementation of a TCG-based integrity measurement architecture//Proceedings of the 2004 USENIX Security Symposium (USENIX Security’04), San Diego,USA, 2004.

[13] Joshua S, Thomas M, Christopher S, Trent J, Patrick M. Justifying integrity using a virtual machine verifier//Proceedings of the 2009 Annual Computer Security Applications Conference(ACSAC'09), Honolulu, USA,2009: 83-92.

[14] Wenjuan X, Gail-Joon A, Hongxin H, Xinwen Z, Jean-Pierre S.DR@FT: efficient remote attestation framework for dynamic systems//Proceedings of the 2010 European Conference on Research in Computer Security(ESORICS'10), Wroclaw, Poland, 2014.

[15] Frederik A, Ahmad-Reza S, Steffen S, Christian W. A security framework for the analysis and design of software attestation//Proceedings of the 2013 ACM Conference on Computer and Communications Security(CCS'13), Berlin, Germany, 2013: 1-12

[16] T. Murray, D. Matichuk, M. Brassil, et al. seL4: from General Purpose to a Proof of Information Flow Environment//Proceedings of the 2013 IEEE Security and Privacy Symposium(Oakland’13), Oakland, USA, 2013:415-249

[17] T. Murray, D. Matichuk, M. Brassil, et al. Noninterference for Operating System Kernels//Proceedings of the 2012 International Conference on Certified Programs and Proofs, Kyoto, Japan, 2012.

[18]常德显,冯登国,秦宇,张倩颖.基于扩展LS2的可信虚拟平台信任链分析[J].通信学报,2013,34(5):31-41.

[19]BURROWS M, ABADI M, NEEDHAM M R.A logic of authentication[A]. Proc of the Royal Society[C]. London, UK, 1989. 233-271.

[20] ABADI M, FOURNET C. Mobile values, new names, and secure communication[A]. Proc of the 28th Symposium on Principles of Programming Languages[C]. London, ACM, 2001. 104-115.

[21]CHEN S Y, WEN Y Y,ZHAO H. Formal analysis of secure bootstrap in trusted computing[A]. Proc of the 4th International Conference on Autonomic and Trusted Computing[C]. Berlin, Springer, 2007. 352-360.

[22]张兴, 黄强, 沈昌祥.一种基于无干扰模型的信任链传递分析方法[J].计算机学报,2010,33(1):74-81.

[23]冯登国，秦宇. 可信计算环境证明方法研究[J].计算机学报, 2008,31(9):1640-1652.

[24]冯登国，秦宇. 一种基于 TCM 的属性证明协议[J]. 中国科学,2010,53(3):454-464.

[25]谭良,陈菊,周明天. 可信终端动态运行环境的可信证据收集机制[J]. 电子学报,2013,01:77 -85.

[26]Scarlata, Vincent and Rozas, Carlos and Wiseman, Monty and Grawrock, David and Vishik, Claire: " TPM Virtualization: Building a General Framework"[C] , Trusted Computing( 2007), 2007:43-56.

[27]F. John Krautheim\*, Dhananjay S. Phatak, and Alan T. Sherman,Introducing the Trusted Virtual Environment Module:A New Mechanism for Rooting Trust in Cloud Computing[C],TRUST 2010, LNCS 6101, 2010:211–227.

[28]Shen Changxiang, Zhang Huanguo, Wang HuaiMin,etal. Research on trusted computing and its development [J].Science in China Series:E.2010,53(3):405-433.

[29]常德显,冯登国,秦宇,张倩颖.基于扩展LS2的可信虚拟平台信任链分析[J].通信学报,2013,34(5):31-41.

[30]Zhang Lei , Chen Xingshu, Liu Liang , Jin Xin.Trusted domain hierarchical model based on noninterference theory[J].The Journal of China Universities of Posts and Telecommunications .August 2015, 22(4): 7-16

[31]朱智强. 混合云服务安全若干理论与关键技术研究[D].武汉大学,2011.

[32]曲文涛. 虚拟机系统的可信检测与度量[D].上海交通大学,2010.

[33]张兴，陈幼雷，沈昌祥.基于进程的无干扰可信模型[J]..通信学报，2009，30(3):6-11

[34]赵赵佳，沈昌祥，刘吉强，等.基于无干扰理论的可信链模型[J].计算机研究与发展，200845(6):974-980

[35]Rushby J. Noninterference , transitivity , and channel-control security policies[M]. SRI International , Computer Science Laboratory , 1992

[36]刘威鹏，张兴.基于非传递元干扰理论的二元多级安全模型研究[JJ.通信学报，2009，30(2):52-58

[37]陈菊，谭良.一个基于进程保护的可信终端模型[J].计算机科学，2011，38(4):115-117

[38]徐甫.支持进程代码修改的非传递元干扰可信模型[J].计算机工程，2013，39(11):150-153，168

[39]秦晰，常朝稳，沈昌样，等.容忍非信任组件的可信终端模型研究[J]..电子学报，2011，39(4):934-939