基于改进期望值决策法的虚拟机可信审计方法

田俊峰[1,2]，张永超[1,2]
（1. 河北大学网络空间安全与计算机学院，河北 保定 071002；2. 河北省高可信信息系统重点实验室，河北 保定 071002）

摘 要：虚拟机运行环境是否可信是云计算推广和有效使用的关键因素，为此将风险决策方法中的期望值决策法加以改进，重新定义了它的使用场景，将审计方案的成本、收益数值化，提出一种基于改进期望值决策法的虚拟机可信审计方法。该方案为用户虚拟机提供几种安全保护级别，根据用户为虚拟机选用的安全保护级别，自主选取最优的审计方案。采用虚拟机自省（VMI, virtual machine introspection）技术获取需要审计的虚拟机信息；采用设计的加密机制保护用户选用安全保护级别的安全性，从而保证审计方案的安全性。最后，仿真实验结果表明了方案具有较好的性能和有效性。

关键词：可信审计；可信计算；风险决策法；虚拟机自省
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018110

Trusted auditing method of virtual machine based on improved expectation decision method

TIAN Junfeng[1,2], ZHANG Yongchao[1,2]
1. School of Cyber Security and Computer, Hebei University, Baoding 071002, China
2. Key Lab on High Trusted Information System in Hebei Province, Baoding 071002, China

Abstract: Whether the cloud computing environment is credible is the key factor in the promotion and effective use of cloud computing. For this reason, the expected value decision method in risk decision-making was improved. The usage scenarios was redefined, the cost and benefit of audit scheme was digitized, and a virtual machine trusted auditing strategy based on improved expectation decision method was proposed. Several levels of security protection for the user virtual machine was provided, and the optimal audit scheme was selected autonomously according to the security protection level chosen by the user for the virtual machine. The virtual machine introspection (VMI) technology was used to obtain the virtual machine information that needs to be audited. The designed encryption mechanism was used to protect the security of users selected security protection level, so as to ensure the security of user virtual machine selection audit strategy. Finally, the simulation results show that the scheme has good performance and validity.

Key words: trusted auditing, trusted computing, risk decision method, virtual machine introspection

1 引言

云计算[1]具有的高伸缩性、位置无关性、低成本等特点使用户可以专注自身业务逻辑的部署，而不用关心具体物理设备的位置。云计算的这些特点使用户可以随接随用，灵活性高，在云计算发展的前期很大程度上促进了云计算的推广和使用。

在越来越重视信息安全的当今，云计算的推广和使用，很大程度上取决于云计算运行环境是否安全可信[2-3]。云计算的特点也正是造成云计算可信问

收稿日期：2017-09-20；**修回日期**：2018-05-20
基金项目：国家自然科学基金资助项目（No.61170254）；河北省自然科学基金资助项目（No.F2016201244）
Foundation Items: The National Natural Science Foundation of China (No.61170254), The Natural Science Foundation of Hebei Province (No.F2016201244)

题的根源所在：云用户将数据和运行环境部署在云端，从而失去了对其的直接控制能力。这些依托于云端的服务和数据可能会受到以下几方面的威胁。

云计算可能遭受来自外部的攻击，导致服务中断或相关信息的泄露[4]；由于云计算中的虚拟机是由物理主机虚拟化而来，不同用户使用的虚拟机可能来自同一物理主机，用户可能遭受侧信道攻击等手段的威胁，导致信息泄露[5]；云提供商是云服务的提供者，云用户可能遭到云提供商的内部窃取，导致信息泄露[6]。

针对以上威胁，迫切需要一种既可以保护虚拟机用户隐私安全，开销又在虚拟机用户的可承受范围内的解决方案。基于此，本文提出了基于改进期望值决策法[7]的虚拟机可信审计方法，将可信计算技术[8]、虚拟机自省加密技术和可信审计技术有机地结合起来，保护用户虚拟机运行环境的可信性。通过虚拟机自省技术获取审计方案需要的虚拟机运行信息，避免获取信息模块在用户虚拟机中容易遭到攻击和篡改的威胁；提出一种加密机制，使每个用户都有唯一的密钥用于查询用户所属虚拟机的相关信息，避免采用虚拟机自省技术破坏多租户隔离机制并且保证用户虚拟机选用审计方案的安全性；把风险决策方法中的期望值决策法加以改进并应用到可信审计方案的选取上，根据虚拟机用户为虚拟机运行环境选取的安全保护级别，为虚拟机用户选取符合其安全需求的最优审计方案。虚拟机用户为虚拟机运行环境选取的安全保护级别不同，经计算得到的最优审计方案则不同，从而改变了一直以来用户只是被动地接受相关安全措施的局面。

2　相关工作

采用可信审计的思想解决云计算中虚拟机运行环境的可信性问题，相关学者对此做了大量的研究工作，取得了不错的成果。

Berger 等[9]基于 Xen 虚拟机管理器，在虚拟化平台上利用硬件虚拟化技术创建多个虚拟的可信平台模块（TPM, trusted platform module）实例，与每个虚拟机一一对应，利用虚拟 TPM 管理器管理各个虚拟机中虚拟的 TPM 实例。硬件虚拟化在提供便利的同时，也增加了被恶意攻击的危险。

刘川意等[10]采用可信审计技术和可信计算技术判定虚拟机的可信性，利用虚拟可信平台模块（vTPM, virtual trusted platform module）保证不变组件的可信性，利用可信审计技术保证可变组件的可信性。

Kursawe 等[11]认为现有 TPM 的可信链过长、实现过于复杂，为此重新定义可信的边界，基于硬件实现了更加灵活的 uTPM，但是对远程认证的数据做签名，使 uTPM 的硬件信息存在暴露的威胁。

Stumpf 等[12]对硬件 TPM 划分多个控制模块，每个控制模块用于构建一个虚拟机环境，使每个虚拟机的 TPM 状态互不影响，从而达到复用 TPM 的目的。但是在这种机制下可信链过于复杂，传递非常耗时。

England 等[13]基于虚拟机管理器，使用虚拟机共享 TPM 的技术，为各个虚拟机应用传递可信链，保证虚拟机应用的可信性。不足之处：每次验证虚拟机应用的可信性时，可信链都要从物理 TPM 经过虚拟机，最后到达虚拟机的应用中，这样会重复验证部分可信链，而且验证时间很长。

林杰等[14]利用完整性度量架构技术[15]可以度量虚拟机的部分信息，判断虚拟机运行时的完整性。不足之处：可以度量的虚拟机信息较少，使度量结果存在偏差。

杜瑞忠等[16]针对保护云存储中用户数据机密性的问题，提出了一种在云服务提供商加密数据的云存储方案。通过虚拟机隔离技术来构造封闭计算环境，可以阻止操作系统中不良应用以及云管理员的攻击，有效防范数据泄露。

郭晓勇等[17]提出了基于收敛密钥的 BLS 签名算法，并利用可信第三方存储审计公钥和代理审计，实现了对审计签名和审计公钥的去重，减轻了客户端存储和计算负担。

采用决策法思想选取审计方案，利用审计方案解决相应问题，相关学者也做了卓有成效的研究工作。

王惠峰等[18]提出了一种自适应数据持有性证明方法，基于文件属性和用户需求动态调整文件的审计方案，使文件的审计需求和审计方案的执行强度高度匹配。

Kolhar 等[19]提出利用密码算法和第三方审计相结合来保护数据的完整性和隐私性，避免了数据在云计算存储和第三方审计过程中造成的隐私泄露。

Rodríguez 等[20]提出了一种新的图形矢量计算方法，通过修改直觉过程来适应不同的管理决策。根据不同的需求，选择最适合的 IT 项目风险管理

方法，该方法采用均值方差计算，通过对模糊层次分析法的图解方法得到用于评价的权重。

上述方法中，利用可信审计思想解决云计算中虚拟机运行环境可信性的问题，需要改动用户虚拟机，在用户虚拟机中安装功能模块和程序，不利于透明性；利用决策法思想选取审计方案解决相应问题，具有存在可扩展性差、资源浪费的缺点。本文采用基于改进期望值决策法的虚拟机可信审计方法来解决虚拟机运行环境可信性的问题，不需要改动虚拟机；可以根据需求添加新的审计方案和审计策略，具有可扩展性；可根据用户对虚拟机不同的安全需求，选用相应的审计方案，避免过度使用安全策略。根据用户为虚拟机运行选用的安全保护级别，为虚拟机用户推荐符合其要求的最佳审计方案，合理地利用了用户虚拟机的资源，避免了资源的浪费。

3 可信审计方案的构建和选取

在云计算的模式下，用户的服务运行在云端，以云提供商提供的物理服务器虚拟化出的虚拟机为载体。虚拟机可能会遭到安全威胁[21]，诸如窃取服务攻击、恶意代码注入攻击、交叉虚拟机侧信道攻击、定向共享内存攻击等。所以要保证云计算的可信，需要保证物理服务器和虚拟机在启动时的可信性以及云计算运行环境的可信性。本文假设启动时云计算是可信的，用基于改进期望值决策法的虚拟机可信审计方法来保证云计算运行环境的可信性。

云服务提供商负责维护管理物理服务器，为了扩大市场占有率，争取潜在用户，云服务提供商更倾向于为物理服务器和虚拟机的可信性提供支持和证据，云服务提供商可以在物理服务器中安装可信组件并以此为可信根，并且利用可信根来建立可信链，将可信链扩展到虚拟机内部，通过将虚拟机提供的虚拟可信模块（如 vTPM），作为虚拟机的可信任根来保证虚拟机启动时的可信性。

3.1 系统架构

为讨论方便，对相关术语解释如下。

进程审计策略：主要用于检测和查看用户态恶意程序的审计策略。

模块审计策略：主要用于检测内核态驱动程序和动态链接库是否遭到篡改的审计策略。

内存审计策略：主要用于字符串搜索检测内存中特定数据的审计策略。

文件审计策略：主要用于检测在用户态下虚拟机运行时对哪些文件进行操作的审计策略。

网络审计策略：主要用于检测虚拟机运行环境中网络连接以及活动状态的审计策略。

基础审计策略：为保护用户虚拟机能够检测常规的安全威胁强制用户采用的审计策略。例如，进程审计策略、模块审计策略等。

安全审计策略：除基础审计策略外，检测安全威胁效果好并且需要消耗很多计算机资源的审计策略。例如，网络审计策略等。

其他审计策略：除基础审计策略和安全审计策略之外的审计策略。例如，内存审计策略、文件审计策略等。

安全保护级别 $\theta_j(j=1,2,\cdots,n,n\leqslant 5)$ 根据虚拟机中运行的系统对虚拟机用户的收益、品牌信誉、存亡影响的重要程度以及其遭到破坏后对用户的危害程度等因素确定。

底限级 θ_1：虚拟机中运行的系统受到破坏后，会对用户的收益造成影响，但损失的收益较提升安全保护等级需要的成本忽略不计。

低级 θ_2：虚拟机中运行的系统受到破坏后，会对用户的收益造成较严重的影响，损失的收益与提升安全保护等级需要的成本基本持平。

中级 θ_3：虚拟机中运行的系统受到破坏后，会对用户的收益造成严重的影响，损失的收益远远大于提升安全保护等级需要的成本，用户品牌信誉基本无影响。

高级 θ_4：虚拟机中运行的系统受到破坏后，会对用户的收益造成严重的影响，损失的收益远远大于提升安全保护等级需要的成本，用户品牌信誉受到影响。

顶级 θ_5：虚拟机中运行的系统受到破坏后，会对用户的收益造成严重的影响，损失无法估计，用户品牌信誉受到严重影响，危及用户生存。

采用审计方案审计用户虚拟机，为用户虚拟机提供几种安全保护级别，安全保护级别越高，为虚拟机可信审计分配的资源越多，可信审计能够选用的审计策略越多，能够检测虚拟机安全威胁的种类越多。当选用的安全保护级别一定时，为防止用户盲目追求虚拟机的运行速度和审计方案的收益，忽略适当的安全需求，本文规定了各种安全保护级别必须明确采用的审计策略：底限级 θ_1、低级 θ_2 保护级别下为可信审计分配的资源较少，必须采用所有

基础审计策略；中级 θ_3、高级 θ_4 保护级别下为可信审计分配的资源适中，必须采用所有基础审计策略和一种其他审计策略；顶级 θ_5 保护级别下为可信审计分配的资源较多，必须采用所有基础审计策略和一种安全审计策略。

随着安全保护级别的提升，审计方案能够检测出虚拟机安全威胁的种类是逐渐上升的。当达到某个安全保护级别后，再提升安全保护级别，审计方案能够检测虚拟机安全威胁种类的增加量是逐渐下降的。所以，本文认为随着安全保护级别的提升，能够检测出虚拟机安全威胁种类的增加量是符合正态分布的。根据用户为虚拟机选用的安全保护级别，利用正态分布公式[22]计算出各种安全状态下的概率值以及审计方案耗费的资源成本界限值。计算各审计方案在虚拟机不同安全状况下的收益值与概率的乘积大小，其中，值最大的为符合虚拟机用户安全要求的最佳审计方案。每种审计方案审计虚拟机的一部分内容（如进程、模块、打开的文件、网络以及内存结构数据），采用虚拟机自省（VMI, virtual machine introspection）[23]技术获取审计方案审计需要的数据，根据这些数据与制定的安全规则判定用户虚拟机是否可信。若不可信，通知虚拟机用户采取措施。

本文提出的基于改进期望值决策法的虚拟机可信审计方法，只需要将添加的模块放在虚拟机的安全的区域即可，在 Xen、KVM、VMWare ESX/GSX/Workstation 等都是适用的，以 Xen[24]为例，如图 1 所示，设计了基于改进期望值决策法的虚拟机可信审计方法的系统架构。根据用户对虚拟机的安全倾向，用户将选中的安全状态，采用加密机制经用户模块→加密模块→管理模块→可信审计模块传送到可信审计模块得到为用户虚拟机选择的审计方案，利用 VMI 模块获取审计需要的数据，在可信审计模块中根据选择的审计方案判定虚拟机的可信性，并将审计用的数据存入可信证据模块中用于事后追责。

系统主要由远程用户模块、可信代理模块、虚拟机自省模块 3 部分构成。可信代理模块（trusted agent module）包括 vTPM 管理器、可信审计模块、可信证据模块、可信协同模块。其中，vTPM 管理器（vTPM manager）主要负责 vTPM 实例、非对称密钥对、对称密钥对的创建与管理，为用户虚拟机与 vTPM 实例间提供了通信信道。当创建一个虚拟机时，虚拟 TPM 管理器便会产生一个 vTPM 实例以及一对非对称密钥对，并将其与新建的虚拟机关联，将密钥信息传送给可信审计模块。可信审计模

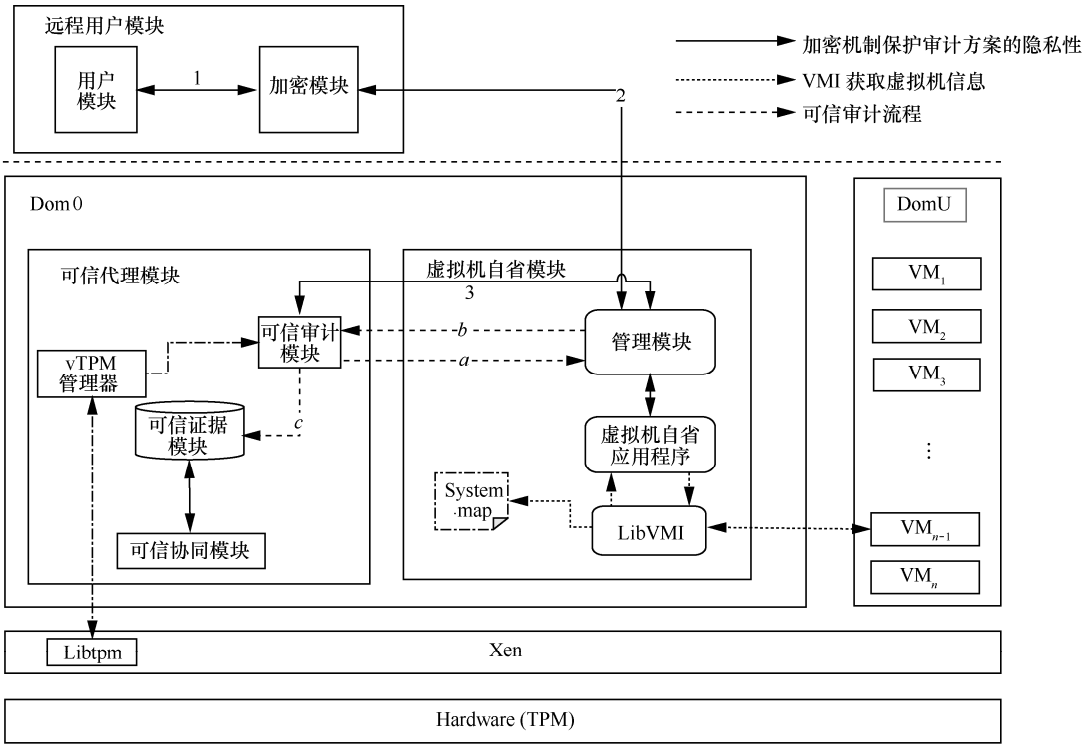


图 1　基于改进期望值决策法的虚拟机可信审计方法的系统架构

块：根据用户的输入参数为用户选择符合其安全性要求的最佳审计方案，负责维护用户的密钥信息；可信证据模块：存储审计的证据，用于事后追责和取证，可信协同模块：用于交互各个虚拟机的安全信息。

3.2 获取审计方案需要的审计数据

虚拟机自省技术 VMI：在一个虚拟机中监控另一个虚拟机的内部运行状态，并且可以获取该虚拟机底层的二进制状态数据。二进制语义和高层语义存在语义鸿沟的问题，无法直接将二进制语义信息转换为高层语义信息，需要利用语义转换工具 LibVMI 解决语义鸿沟问题，将二进制语义翻译为高层语义。

根据虚拟机用户为虚拟机选用的安全保护级别，确定符合虚拟机用户需求的最优审计方案，根据审计方案中审计策略确定需要审计用户虚拟机底层状态数据的种类，利用虚拟机自省技术获取该种类的二进制信息。如图 2 所示，利用 VMI 获取用户虚拟机信息的步骤如下。

1) 虚拟机自省应用程序（VMI application）请求查看内核符号。

2) LibVMI 从监控虚拟机内核符号表中读取需要被监控虚拟机的虚拟地址信息，如果内核符号表与被监控虚拟机的内核符号表不匹配，则通过网络查找对应的被监控虚拟机的内核符号表。

3) 根据审计方案中的审计策略确定需要获取被监控虚拟机底层数据的信息，首先查找虚拟地址对应的内核页目录信息获取对应的页表，进而查找到正确的数据页。

4) 通过数据页中物理地址，找到用户虚拟机的内存数据，其中内存数据是以二进制的形式存在。

5) 将得到的二进制形式的内存数据返回给 LibVMI 模块，由其解析出高层语义。

6) LibVMI 模块将数据返回给 VMI Application。

3.3 运行时审计方案的选取

为了讨论方便，对相关术语解释如下。

审计策略 $b_i(i=1,2,\cdots,m)$：云计算环境中，根据虚拟机用户的安全需求，采取相应的方式、手段和技术来保护虚拟机安全的解决方案总称。

审计方案 $B_k(k=1,2,\cdots,l)$：包含审计策略 $b_1,b_2,\cdots,b_m$ 中的一种或多种。若包含审计策略 $b_i(i=1,2,\cdots,m)$，则 x_i=1，反之 x_i=0。

审计策略收益值 a_{ij}：在安全保护级别 $\theta_j(j=1,2,\cdots,n,n\leqslant 5)$ 下，采用审计策略 b_i 可以避免虚拟机用户发生安全事件造成损失 $loss_i$ 和降低用户虚拟机发生安全事件的概率 p_{ij} 的乘积，即 $a_{ij}=p_{ij}loss_i$。损失 $loss_i$ 和降低安全事件的概率 p_{ij} 可划分为 3 个等级：高、中、低，$loss_i$ 选择使用 y_1、y_2、y_3 作为打分的范围，p_{ij} 选择使用 z_1、z_2、z_3 作为打分的范围。

审计方案收益值：在用户虚拟机中，各种审计策略之间可能会相互影响，审计方案收益值不仅包

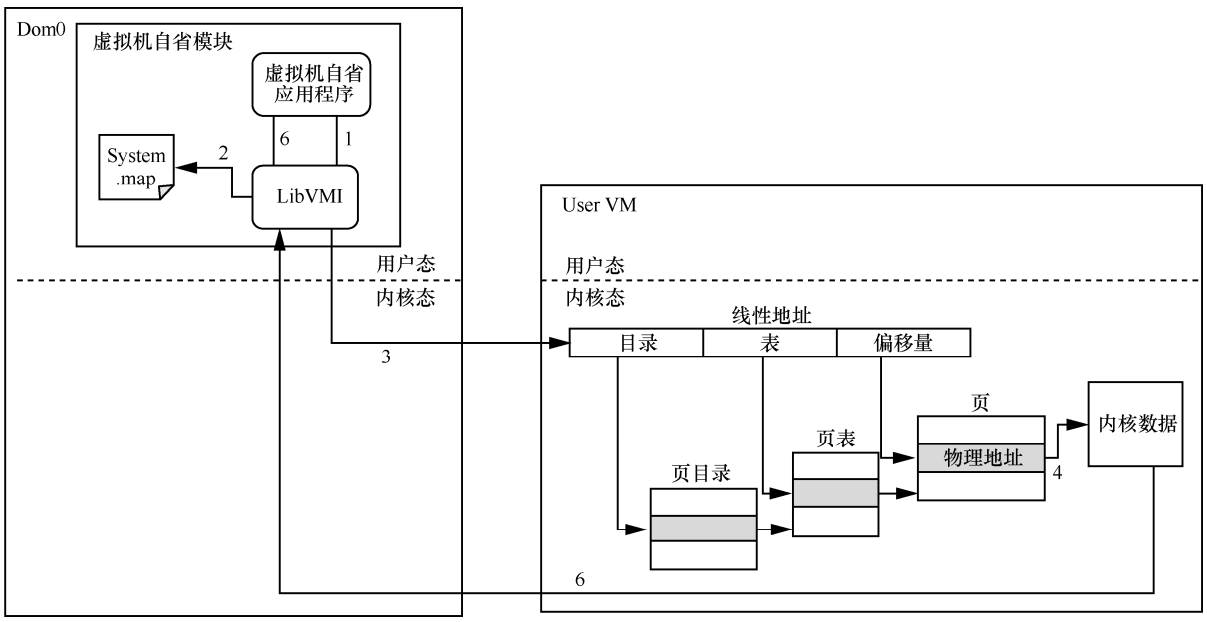


图 2 VMI 模块获取虚拟机的内存数据

含单个审计策略收益值的累加和，而且还包含审计策略之间交互作用的额外收益值。

审计策略额外收益值 $\xi(b_ib_j)$：表现为协同、蚕食、无关性。其中，协同是 2 种审计策略组合的收益值大于 2 种审计策略单独收益值之和。蚕食是 2 种审计策略组合的收益值小于 2 种审计策略单独收益值之和。无关性是 2 种审计策略组合的收益值等于 2 种审计策略单独收益值之和。因此，令协同 $\xi(b_ib_j)=u_1$，蚕食 $\xi(b_ib_j)=u_2$，无关性 $\xi(b_ib_j)=u_3$。

审计策略成本 $cost(b_i)$：采用审计策略 b_i 需要耗费用户虚拟机的资源成本值。可以利用性能测试工具获得，具体是把虚拟机的内存资源和 CPU 资源划分成百分制的区间，利用性能测试工具测试采用审计策略 b_i 后，它耗费的资源值分别在内存资源和 CPU 资源的哪个百分制区间，将其加和求平均值得到审计策略 b_i 耗费的资源成本为 $cost(b_i)$，它指的是用户虚拟机资源的百分之一。

审计方案成本界限值 $cost(limit)$：审计方案耗费用户虚拟机资源成本的最大值。

3.3.1　期望值决策法

一个离散型的随机变量 X，它的数学期望为

$$\mathrm{E}(X)=\sum_{i=1}^{n}x_ip_i \tag{1}$$

其中，$x_i(i=1,2,\cdots,n)$ 表示随机变量 X 的各个取值，p_i 表示 $X=x_i$ 的概率，即 $p_i=P(x_i)$。随机变量 X 在概率意义下的平均值可以用期望值表示。利用期望值决策法计算各方案的期望收益值，并以它为依据，选择平均收益最大的方案作为最佳决策方案。

假设某个关于风险型决策的问题，有 m 个方案 $b_1,b_2,\cdots,b_m$，有 n 个状态 $\theta_1,\theta_2,\cdots,\theta_n$，各状态的概率分别为 $p_1,p_2,\cdots,p_n$。如果在状态 θ_j 下采取方案 b_i 的收益值为 $a_{ij}(i=1,2,\cdots,m,\ j=1,2,\cdots,n)$，则方案 b_i 的期望收益值为

$$\mathrm{E}(b_i)=\sum_{j=1}^{n}a_{ij}p_j,i=1,2,\cdots,m \tag{2}$$

其中，有

$$\sum_{j=1}^{n}p_j=1 \tag{3}$$

如果引入下述向量

$$\boldsymbol{b}=\begin{bmatrix}b_1\\b_2\\\vdots\\b_m\end{bmatrix},\mathbf{E}(\boldsymbol{b})=\begin{bmatrix}\mathrm{E}(b_1)\\\mathrm{E}(b_2)\\\vdots\\\mathrm{E}(b_m)\end{bmatrix},\boldsymbol{P}=\begin{bmatrix}p_1\\p_2\\\vdots\\p_n\end{bmatrix}$$

及收益值矩阵 $\boldsymbol{A}=\begin{bmatrix}a_{11}&\cdots&a_{1n}\\\vdots&\ddots&\vdots\\a_{m1}&\cdots&a_{mn}\end{bmatrix}$，则矩阵运算形式为

$$\mathbf{E}(\boldsymbol{b})=\boldsymbol{AP} \tag{4}$$

3.3.2　改进的期望值决策法

期望值决策法以期望收益值为依据，在众多风险处理方案中，选择符合用户需求的方案。期望值决策法没有判断虚拟机是否可信的手段，不能直接用于云计算环境下判断虚拟机是否可信。将期望值决策法和可信审计结合起来，依据虚拟机用户为虚拟机选用的安全保护级别，为虚拟机用户选择符合其安全要求的最佳审计方案，用于云计算环境下判断虚拟机是否可信。根据上述提及的要点，将风险决策方法中的期望值决策法加以改进，使它计算出的结果能够作为审计方案的选取依据。

对期望值决策法的改进如下。

1) 针对期望值决策法各种方案的成本、收益值不易计算的问题，重新定义了期望值决策法的使用场景，提出了审计方案成本和收益值的计算方法，将抽象的审计方案选取问题具体化，用户根据此方法即可选取符合用户需求的最佳审计方案。

2) 针对期望值决策法只是使用单一的方案计算收益值、适用性差的问题，将多种审计策略组成一个审计方案，并且考虑了审计策略间相互作用的问题，用审计策略额外收益值的大小来表示审计策略间的几种关系，即协同、蚕食、无关性。

3) 针对期望值决策法各种状态发生概率不易计算的问题，使用正态分布公式计算各个安全保护级别的概率，不仅着重突出了用户对虚拟机选择的安全保护级别，同时也兼顾了其他安全保护级别下审计方案选取的状况，使选取的审计方案不仅符合用户需求，而且更加安全高效。

改进后的期望决策法为：假设审计方案选用问题有 l 个审计方案 $B_1,B_2,\cdots,B_l$，有 m 个审计策略 $b_1,b_2,\cdots,b_m$，有 n 个供虚拟机用户选用的安全保护级别 $\theta_1,\theta_2,\cdots,\theta_n$，各个安全保护级别对应的概率分别

为 $p_1,p_2,\cdots,p_n$。若在安全保护级别 θ_j 下采用审计策略 b_i 的收益值为 $a_{ij}(i=1,2,\cdots,m,j=1,2,\cdots,n)$，则审计方案 B_k 的期望收益值为

$$\mathrm{E}(B_k)=\sum_{i=1}^{m}\sum_{j=1}^{n}x_i a_{ij}p_j+\sum_{j=1}^{n}\sum_{i=1}^{m-1}\sum_{q=i+1}^{m}x_i x_q\xi(b_i b_q)p_j,k=1,2,\cdots,l \tag{5}$$

满足条件

$$\sum_{i=1}^{m}x_i cost(b_i)<cost(limit) \tag{6}$$

$$\sum_{j=1}^{n}p_j=1 \tag{7}$$

如果引入下述向量

$$\boldsymbol{B}=\begin{bmatrix}B_1\\B_2\\\vdots\\B_l\end{bmatrix},\mathbf{E}(\boldsymbol{B})=\begin{bmatrix}\mathrm{E}(B_1)\\\mathrm{E}(B_2)\\\vdots\\\mathrm{E}(B_l)\end{bmatrix},\boldsymbol{P}=\begin{bmatrix}p_1\\p_2\\\vdots\\p_n\end{bmatrix}$$

及收益值矩阵 $\boldsymbol{\beta}=\begin{bmatrix}\beta_{11}&\cdots&\beta_{1n}\\\vdots&\ddots&\vdots\\\beta_{l1}&\cdots&\beta_{ln}\end{bmatrix}$，其中

$$\beta_{kj}=\sum_{i=1}^{m}x_i a_{ij}+\sum_{i=1}^{m-1}\sum_{q=i+1}^{m}x_i x_q\xi(b_i b_q)p_j \tag{8}$$

则矩阵运算形式为

$$\mathbf{E}(\boldsymbol{B})=\boldsymbol{\beta P} \tag{9}$$

为了验证安全保护级别的概率采用正态分布公式计算是合理的，使用 Metasploit[25]模拟虚拟机安全威胁，采用基于改进期望值决策法的虚拟机可信审计方法检测虚拟机的安全威胁。具体做法为：改变安全保护级别，发现随着安全保护级别的提升，能够检测的安全威胁种类是逐渐增加的；随着安全保护级别的提升，能够检测的安全威胁种类的增加量呈现先增后减的趋势；描绘直方图发现两头低、中间高、左右大致对称，因此可近似认为随着安全保护级别的提升，检测出安全威胁种类的增加量符合正态分布。

假设安全保护级别 θ_j 处于众多安全保护级别的中间位置。令 $T(\theta_j)=\theta_j$，则正态分布式为

$$f(x)=\frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{\frac{-(x-u)^2}{2\sigma^2}} \tag{10}$$

当 $x=T(\theta_z)(z=1,2,\cdots,j,\cdots,n)$ 时，计算得到 $f(x)$，其中，$u=T(\theta_j)$，$\sigma=1$。将所有的 $f(x)$加和，并计算出每个安全保护级别 θ_z 所占的比例，即每种安全保护级别对应的概率 p_j。此外，令 $u=0$，$\sigma=1$，当 $x=T(\theta_j)$ 时，耗费资源成本的界限值 $cost(limit)=\delta cost(unit)\sum_{j=1}^{x}p_j$。

针对耗费资源成本界限值的问题，用户往往希望用最小的投入获得最大的收益，但这在实际情况中是不可能的，经过多次实验分析发现，当耗费资源成本的界限值 $cost(limit)=\delta cost(unit)\sum_{j=1}^{x}p_j$ 中取 $\delta=20$ 时，往往能获得较高的投入产出比，所以在 4.2.1 节中取 $\delta=20$。

3.3.3 审计方案的安全性保护

虚拟机用户根据自己的需求为虚拟机选用某种安全保护级别，当用户选用的安全保护级别被窃取时，可能会导致为用户虚拟机选用的审计方案泄露，攻击者会针对审计方案实施特定的攻击，造成虚拟机的安全隐患。因此，采用加密机制保护用户选用安全保护级别的安全性，从而保护审计方案的安全性。

每个用户虚拟机都有一对非对称密钥和对称密钥，由 vTPM 管理器负责创建和管理。为了保护审计方案的安全性，需要保护用户选用安全保护级别的安全性，本文采取公钥加密对称密钥，对称密钥加密用户命令的方式来保证用户选用安全保护级别的安全性。将用户为虚拟机选用的安全保护级别的标识信息赋给 cmd，其中，UUID 表示本次加密传输的唯一标识，UNAME 表示用户名，VMIP 表示虚拟机 ip，SK 表示对称密钥，PK 表示公钥，Result 表示是否成功传输的结果，具体流程如图 3 所示。

1) 用户将 UNAME、VMIP、cmd 传送给加密模块对 cmd 进行加密。

2) 加密模块为本次加密传输生成唯一标识 UUID，并将 UUID、UNAME、VMIP、SK{cmd}、PK{SK}传送给管理模块。

3) 管理模块利用 UNAME、VMIP 查找是否有匹配的虚拟机，若有则将 UUID、UNAME、VMIP、

SK{cmd}、PK{SK}传送给可信审计。

4) 可信审计利用 UNAME、VMIP 得到虚拟机的专属私钥，用私钥解密公钥，用公钥解密对称密钥，用对称密钥解密出命令 cmd，通过改进的期望值决策法计算出为用户选用的审计方案。若成功将 Result 设为 YES，否则设为 NO，将 UUID、Result 返回给用户。

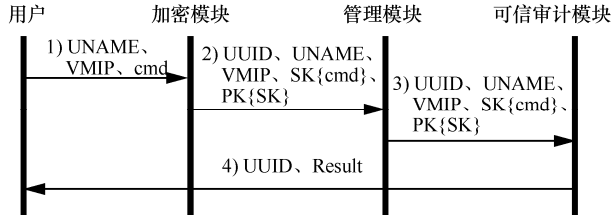


图 3　加密机制保护审计方案的安全性

4　实验和评价

下面，对审计方案的选取、有效性实验以及性能实验为目标进行分析。

4.1　实验环境

本文的实验利用软件 libtpm 模拟硬件 TPM，作为整个系统的可信根，使用开源 Xen 平台作为虚拟机管理器，实现 vTPM 对硬件 TPM 的仿真模拟。为每个虚拟机模拟一个 vTPM，使虚拟机和 vTPM 一一对应，用 vTPM 作为虚拟机的可信根。使用 VMI 开源工具 LibVMI 采用旁路的方式获取审计用户虚拟机的底层数据信息。实验中采用的部署配置信息如表 1 所示。

表 1　　配置信息

配置项	物理服务器	虚拟机
CPU	Intel Xeon X5650 2.66 GHz	Intel Xeon X5650
	单个 6 核，共 24 核	2.66 GHz
内存	单个 8 GB，共 32 GB	4 GB
缓存	12 MB	4 MB
硬盘容量	1 TB	30 GB

4.2　实验结果及分析

4.2.1　审计方案的选取及分析

假设有 5 种审计策略 $b_1,b_2,\cdots,b_5$，分别表示进程审计、模块审计、内存审计、文件审计、网络审计。审计方案 $B_i(i=1,2,\cdots,8)$包含一种或多种审计策略，具体为 $B_1(b_1,b_2)$、$B_2(b_1,b_2,b_3)$、$B_3(b_1,b_2,b_4)$、$B_4(b_1,b_2,b_5)$、$B_5(b_1,b_2,b_3,b_4)$、$B_6(b_1,b_2,b_3,b_5)$、$B_7(b_1,b_2,b_4,b_5)$、$B_8(b_1,b_2,b_3,b_4,b_5)$。为用户虚拟机提供的安全保护级别有 5 种，依次为 $\theta_1,\theta_2,\cdots,\theta_5$，分别表示底限级、低级、中级、高级、顶级。

审计策略占用的资源和检测率是一定的，所以在不同的安全保护级别下，它的成本值和降低安全事件概率是一定的。虚拟机安全对用户越重要，用户选用的安全保护级别越高，为虚拟机可信审计分配的资源越多，避免的损失就越多。根据经验[26]，y_1、y_2、y_3 分别取 9、3、1，z_1、z_2、z_3 分别取 $\frac{1}{3}$、$\frac{1}{9}$、$\frac{1}{27}$，u_1、u_2、u_3 分别取 1、−1、0 时，计算出的收益值体现出既保守又有较好区分度的特征。根据上述规则，各审计策略的成本值如表 2 所示，各审计策略在不同的安全保护级别下的收益值如表 3 所示。

表 2　　各审计策略的成本值

审计策略	内存资源	CPU 资源	平均值 $cost(b_i)$
b_1	3.10%	3.30%	3.20%
b_2	3.00%	3.10%	3.05%
b_3	3.30%	3.20%	3.25%
b_4	2.90%	2.80%	2.85%
b_5	3.20%	3.30%	3.25%

表 3　　各审计策略在不同的安全保护级别下的收益值（保留两位）

安全保护级别 θ	收益值				
	b_1	b_2	b_3	b_4	b_5
底限级	1.00	0.33	0.11	0.04	0.04
低级	3.00	0.33	0.33	0.04	0.04
中级	3.00	1.00	0.33	0.11	0.04
高级	3.00	1.00	0.33	0.11	0.11
顶级	3.00	1.00	1.00	0.11	0.33

假设虚拟机用户为虚拟机选用的安全保护级别 θ_3，审计策略 b_1、b_2、b_3 为协同关系。利用正态分布式得到各种安全保护级别对应的概率值 $p_1,p_2,\cdots,p_5$ 以及耗费资源成本的界限值 $cost(limit)=14.04cost(unit)$。在该安全保护级别下，审计方案必须采用所有基础审计策略和一种其他审计策略，并且审计方案的成本要小于耗费资源成本的界限值。同时符合策略选择要求和成本要求的审计方案有 B_2、B_3、B_5、B_6、B_7，计算这几种审计方案在各种安全保护级别下的

收益值。各个安全保护级别的概率及采用各个审计方案的收益如表 4 所示。

表 4 各个安全保护级别的概率及采用各个审计方案的收益

安全保护级别 θ	发生的概率	方案 B_2	方案 B_3	方案 B_5	方案 B_6	方案 B_7
底限级	0.054	4.44	2.37	4.48	4.48	2.41
低级	0.244	6.66	4.37	6.70	6.70	4.41
中级	0.404	7.33	5.11	7.44	7.37	5.15
高级	0.244	7.33	5.11	7.44	7.44	5.22
顶级	0.054	8.00	5.11	8.11	8.33	5.44

根据改进的期望值决策法得到，$\mathbf{E}(\boldsymbol{B})=\begin{bmatrix}7.05\\4.78\\7.14\\7.12\\4.85\end{bmatrix}$

符合策略选择要求和成本要求的审计方案中，B_5 的期望值收益值最大，所以 B_5 就是符合用户要求的最优方案。

4.2.2 有效性实验及分析

在云计算中，虚拟机用户根据自身需求的不同会对虚拟机进行不同的操作，例如，修改虚拟机配置，增删软件和应用服务等。这些操作会使程序对应的 Hash 摘要值发生改变，因此不能通过固定所有程序比较其 Hash 摘要值的方法来判定虚拟机的可信性。本文将风险决策和可信审计结合起来，利用可信计算技术保证虚拟机运行环境中不变组件的可信性，利用审计技术保证虚拟机运行环境中可变组件的可信性，利用风险决策法为用户选用可信审计方案，判定虚拟机的可信性。

Metasploit 是一款开源的安全漏洞检测工具，它提供了通用的漏洞攻击框架，集成了各平台上常见的溢出漏洞和流行的 shellcode。其主要原理是利用各种操作系统中存在的漏洞如本地缓冲区溢出、堆污染、整数溢出或格式串漏洞等进行攻击。攻击成功后可以在目标虚拟机中运行各种恶意脚本程序。

用 Metasploit 攻击安装 Windows 系统的虚拟机，攻击成功后在虚拟机中运行 FUTo 脚本程序。FUTo 是 FU rootkit 的新版本，它是一种恶意的程序，可以隐藏自身进程和恶意进程避免被宿主机发现，达到持续破坏的作用。FUTo 增加了一些新的功能，它采用 DKOM 技术隐藏 PspCidTable 中特定的对象。PspCidTable 是一个指向 HANDLE_TABLE 结构的指针，PspCidTable 相当于进程和线程 ID 的句柄表，每一个进程的 PID 都能在 PspCidTable 中找到它的对应。主流的安全检测工具，如 IceSword，主要通过扫描 PspCidTable 来获取运行环境的进程列表信息，它无法检测到 FUTo 隐藏的进程信息。如图 4(a)所示，采用主流的安全检测工具，不能发现 FUTo 创建的进程。

在本次实验中为用户选用的是审计方案 B_5，审计方案 B_5 包含进程审计和内存审计。进程审计可以通过判断进程内存页的使用情况检测隐藏的进程。进程运行时会在操作系统的内存页分配池中为进程分配进程内存页，当 FUTo 隐藏进程信息时，操作系统的内存页分配池中还有该进程的信息，通过扫描操作系统的内存页分配池对比进程列表可以发现隐藏的进程，如图 4(b)所示。

```
smss.exe          352  C:\Windows\System32\smss.exe
csrss.exe         540  C:\Windows\System32\csrss.exe
wininit.exe       644  C:\Windows\System32\wininit.exe
winlogon.exe      728  C:\Windows\System32\winlogon.exe
services.exe      772  C:\Windows\System32\services.exe
```

(a) 主要安全检测工具未能发现 FUTo 创建的进程

```
smss.exe          352  C:\Windows\System32\smss.exe
csrss.exe         540  C:\Windows\System32\csrss.exe
WINLOGON.EXE      523  C:\Windows\WINLOGON.EXE
wininit.exe       644  C:\Windows\System32\wininit.exe
winlogon.exe      728  C:\Windows\System32\winlogon.exe
services.exe      772  C:\Windows\System32\services.exe
```

(b) 本文可信审计方案发现 FUTo 创建的进程

图 4 使用主要安全检测工具和本文可信审计方案对比

4.2.3 性能实验及分析

根据本文提出的虚拟机可信审计方法，把用户选中的虚拟机安全保护级别的标识信息加密传送到可信审计模块，在该模块为用户虚拟机选用审计方案，根据审计方案的需求利用虚拟机自省技术来进行审计数据收集，通过审计方案制定的策略审计收集的数据，判定虚拟机是否可信。这些机制会给虚拟机带来额外的性能开销。因此，性能实验的目的是：通过对比可信机制不同，采用其他软件、硬件设施都相同的虚拟机来分析本文方法对用户虚拟机运行环境带来的额外代价。为了更细致地分析各个机制的引入对性能的影响，把用户虚拟机分成 3 种设置：采用审计方案的可信虚拟机、采用文献[10]中可信机制的虚拟机、采用非可信机制的虚拟机，并分析机器配置不同的虚拟机对审计方案中审

计数据收集和审计的性能影响。其中，采用审计方案的可信（audit-trust）虚拟机：引入可信链、加密机制、审计方案选择、审计数据收集和审计这些可信机制；采用文献[10]中可信机制的虚拟机（other-trust）：引入可信链、审计数据收集和审计这些可信机制；采用非可信机制（none-trust）的虚拟机：不引入任何可信机制。

审计数据的收集主要有 2 种方式：同步和异步。同步方式是先把需要审计虚拟机的内存信息存储到硬盘文件上，然后从文件中查找需要审计的信息，对虚拟机进行可信性审计；异步方式则不需要每次都把需要审计虚拟机的内存信息存储到硬盘上，可以细粒度地访问和获取特定虚拟机的内存信息，同时根据这些信息对虚拟机进行可信性审计。

虚拟机的配置对收集审计数据产生影响的因素主要有 2 种：虚拟机中内存的大小，虚拟机的 CPU 的核数，即单位时间内 CPU 计算数据的能力。首先，分析虚拟机的 CPU 核数对收集审计数据性能的影响。如图 5 所示，在虚拟机内存和其他配置不变的情况下，改变 CPU 核数，观察 CPU 核数对同步方式下审计数据收集完成时间的影响，可以发现，当限定虚拟机的内存大小、改变虚拟机 CPU 核数时，其对审计数据收集完成的时间几乎无影响。

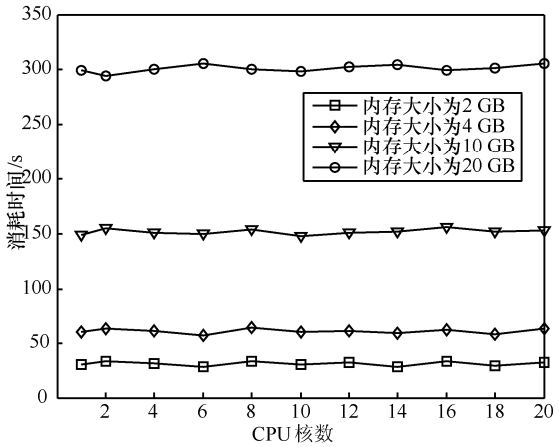


图 5　用户虚拟机 CPU 核数对审计数据收集消耗时间的影响

在同步方式下，统计了对虚拟机进行一次数据收集和审计操作所需要的时间，如图 6 所示。以 4 GB、4 核虚拟机配置为例，从图 5 和图 6 可以看到，审计数据收集花费的时间为 61.13 s，而进程审计花费的时间为 1.37 s，占前者 2.24%。由此可以说明图 6 中的情况，即对虚拟机进行可信数据收集和审计的完成时间与虚拟机中的内存大小基本呈正比关系，这是因为所需要的时间绝大部分花费在收集审计数据上。

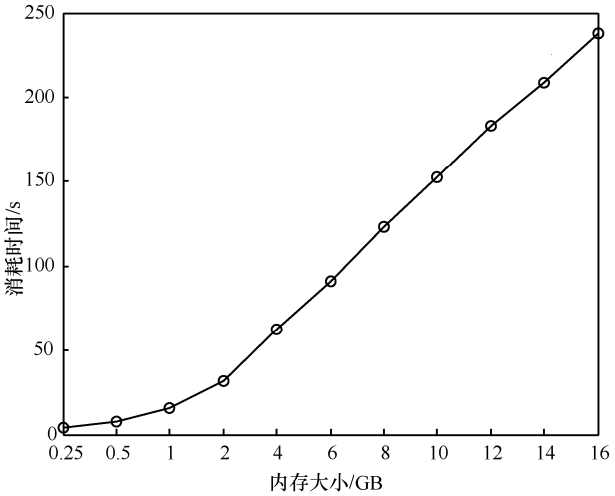


图 6　同步方式下，一次审计方案审计数据收集和审计操作在不同虚拟机内存配置下消耗的时间

审计操作主要对需要审计的数据进行数据结构和相关字符串搜索匹配，与需要存储到硬盘上的内存数据的大小没有关系，所以审计操作的完成时间和内存大小没有呈现出线性关系。从图 7 可以看出，异步方式下审计数据收集加上审计的总完成时间跟同步方式下审计的完成时间相差不多。这是因为异步方式可以直接细粒度地获取需要审计的内存数据，不需要把它先存储到硬盘上再进行审计，所以可以得出结论，即异步方式可以在很大程度上节省一次审计数据收集和审计的时间。

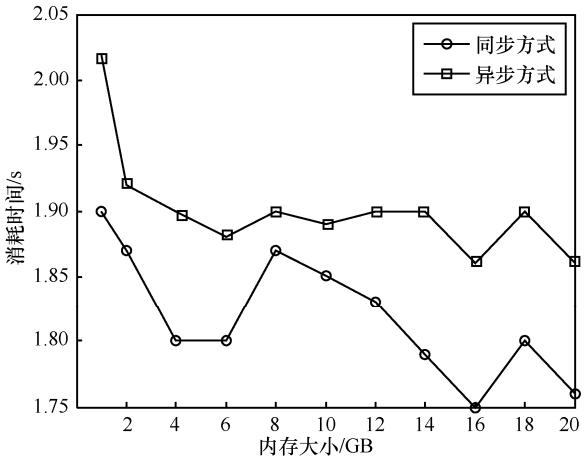
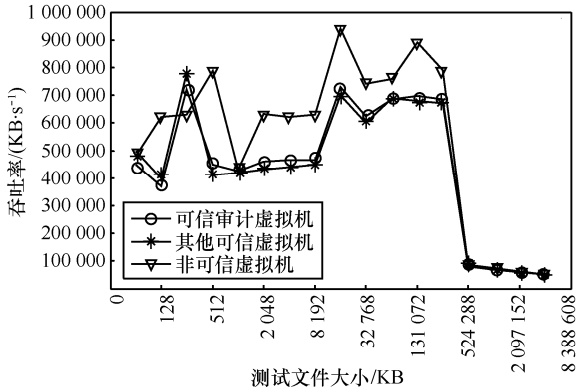


图 7　在异步方式下数据收集和审计的完成时间与同步方式下审计时间的对比

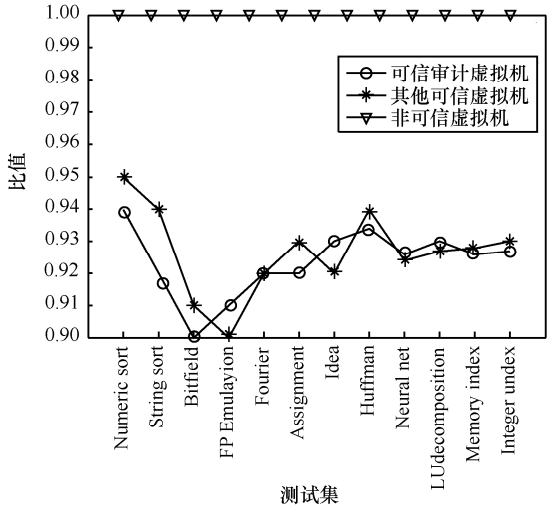
因为对虚拟机的可信审计可以用异步方式对用户虚拟机内存数据进行旁路操作，而审计方案的

选用只是一个简单的计算问题，获取审计数据、审计以及审计方案的选取时间都可以忽略不计。因此本文主要考虑可信链的引入和加密机制对虚拟机可信审计性能的影响。

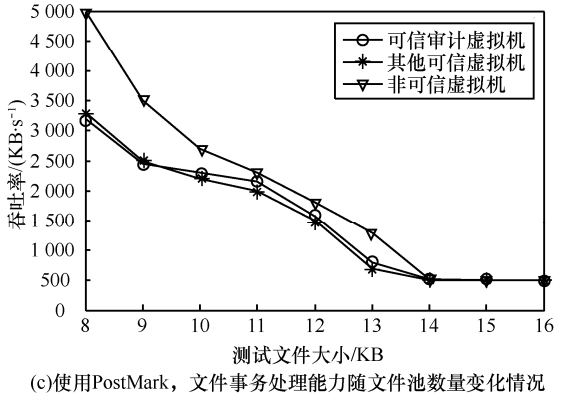
采用多种不同侧重的性能测试工具，对可信机制不同、其他配置都相同的虚拟机进行性能测试。图 8 是对虚拟机进行性能测试和对比的情况，性能测试工具的说明如表 5 所示。



(a)使用IOZone，在特定数据块大小时(64 KB)，I/O吞吐率随测试文件大小变化的情况



(b)使用ByteMark，在不同指标下对比虚拟机的计算能力



(c)使用PostMark，文件事务处理能力随文件池数量变化情况

图 8　使用性能测试工具对不同类型的用户虚拟机进行性能对比

表 5　性能测试工具的名称和功能描述

名称	功能描述
IOZone	IOZone 是一个 benchmark 工具用于文件系统，可以测试多种操作系统中文件系统的读写能力
ByteMark	ByteMark 利用多种计算密集型任务的算法，可以测试系统的处理器、高速缓存以及协处理器性能
PostMark	Postmark 用于测试存储系统的存储性能，主要针对进行频繁、大量存取小文件的存储系统。原理：构建一个测试文件池，然后进行事务的初始化，对每一个事务中读取/附加，创建/删除等所占的比例进行设置来模拟真实应用场景

使用 3 种测试工具测试不同类型虚拟机的性能状况。其中，IOZone 测试不同类型虚拟机的 I/O 性能；ByteMark 测试不同指标下虚拟机的计算能力；PostMark 测试不同类型虚拟机处理文件事务的能力。audit-trust 引入的额外性能代价在于加密机制和可信机制。对于可信机制，当执行某种操作时不仅需要计算 Hash 值还需要将该值扩展到 vTPM 的 PCR 寄存器中。因此每个操作的完成时间会有所增加，但是对处理相同的操作时，可信机制不需要再次进行 Hash、获取摘要、存放到 PCR 寄存器中。而加密机制只是在首次为用户虚拟机选用审计策略时使用。由图 8(a)可知，3 种可信机制不同，其他配置相同的用户虚拟机，它的读写能力（吞吐率）基本是一致的。随着测试文件大小的不断增加，磁盘 I/O 逐渐成为系统读写能力（吞吐率）的瓶颈后，加密机制和可信机制所产的性能开销可以忽略不计，运行环境读写能力（吞吐率）表现为磁盘 I/O 的速度，3 种类型虚拟机的读写能力（吞吐率）曲线基本一致。由图 8(b)可知，3 种类型虚拟机的计算性能相差不大，性能损耗基本可以忽略不计。由图 8(c)可知，未引入可信机制的虚拟机在每秒完成的事务数量高于引入可信机制的虚拟机，随着并发文件数的不断增加，相同的事务操作变得越来越多，二者之间的差距不断缩小。以上实验说明本文中的可信机制和加密机制不会引入过多额外代价。

5　结束语

虚拟机运行环境的安全可信是云计算被广泛应用的重要前提，国内外研究者对如何判定虚拟机运行环境是否可信进行了深入的研究，取得了重要的研究成果。本文针对现有研究方案中存在的问题，如过度使用安全策略浪费资源、需要改动虚拟机不利于推广、可扩展性差等，提出了基于改进期望值决策法的

虚拟机可信审计方法，为上述问题提供了一种可行的解决方案。根据虚拟机用户为虚拟机选用的安全保护级别，为用户虚拟机选取符合其安全需求的最佳审计方案，通过审计方案判定虚拟机运行环境的可信性，若用户虚拟机运行环境处于不可信状态，则及时通知用户采取相应措施。通过仿真实验的方法对审计方案的选取、有效性进行分析，结果表明，采用风险决策法的思想和可信审计方法相结合的机制针对典型的安全威胁是有效的；在实际应用中，只要虚拟机用户可以根据本文的方法得出审计方案的成本和收益值，那么本文提出的方案对该用户就适用。

参考文献：

[1] ALI M, KHAN S U, VASILAKOS A V. Security in cloud computing: opportunities and challenges[J]. Information Sciences, 2015, 305: 357-383.

[2] ABDELBAKI N, RADWAN T, AZER M A. Cloud computing security: challenges and future trends[J]. International Journal of Computer Applications in Technology, 2017, 55(2):158.

[3] KO R K L, JAGADPRAMANA P, MOWBRAY M, et al. TrustCloud: a framework for accountability and trust in cloud computing[C]//IEEE World Congress on Services. 2011:584-588.

[4] KHALIL I, KHREISHAH A, AZEEM M. Cloud computing security: a survey[J]. Computers, 2014, 3(1):1-35.

[5] KATZ G, ELOVICI Y, SHAPIRA B. CoBAn: a context based model for data leakage prevention[J]. Information Sciences, 2014, 262(3): 137-158.

[6] JANSEN W, GRANCE T. Guidelines on security and privacy in public cloud computing[J]. Journal of E-Governance, 2011, 34(3): 149-151.

[7] 赵新泉, 彭勇行. 管理决策分析[M]. 北京: 科学出版社, 2008.
ZHANG X Q, PENG Y X. Management decision analysis[M]. Beijing: Science Press, 2008.

[8] MICHAEL J B. Trusted computing: an elusive goal[J]. Computer, 2015, 48(3):99-101.

[9] BERGER S, GOLDMAN K A, PEREZ R, et al. vTPM: virtualizing the trusted platform module[C]// Conference on Usenix Security Symposium. 2006: 21.

[10] 刘川意, 王国峰, 林杰, 等. 可信的云计算运行环境构建和审计[J]. 计算机学报, 2016, 39(2):339-350.
LIU C Y, WANG G F, LIN J, et al. Practical construction and audit for trusted cloud execution environment[J]. Chinese Journal of Computers, 2016, 39(2):339-350.

[11] KURSAWE K, SCHELLEKENS D. Flexible muTPMs through disembedding[C]//ACM Symposium on Information, Computer and Communications Security. 2009:116-124.

[12] STUMPF F, ECKERT C. Enhancing trusted platform modules with hardware-based virtualization techniques[C]//Second International Conference on Emerging Security Information, Systems and Technologies. 2008:1-9.

[13] ENGLAND P, LOESER J. Para-virtualized TPM sharing[C]// International Conference on Trusted Computing and Trust in Information Technologies: Trusted Computing-Challenges and Applications. 2008: 119-132.

[14] 林杰, 刘川意, 方滨兴. IVirt: 基于虚拟机自省的运行环境完整性度量机制[J]. 计算机学报, 2015, 38(1):191-203.
LIN J, LIU C Y, FANG B X. IVirt: runtime environment integrity measurement mechanism based on virtual machine introspection [J]. Chinese Journal of Computers, 2015, 38(1): 191-203.

[15] SAILER R, ZHANG X, JAEGER T, et al. Design and implementation of a TCG-based integrity measurement architecture[C]// Conference on Usenix Security Symposium. 2004: 16.

[16] 杜瑞忠, 王少泫, 田俊峰. 基于封闭环境加密的云存储方案[J]. 通信学报, 2017, 38(7): 1-10.
DU R Z, WANG S X, TIAN J F. Cloud storage scheme based on closed-box encryption[J]. Journal on Communications, 2017, 38(7): 1-10.

[17] 郭晓勇, 付安民, 况博裕, 等. 基于收敛加密的云安全去重与完整性审计系统[J]. 通信学报, 2017, 38(S2):156-163.
GUO X Y,FU A M,KUANG B Y, et al. Secure deduplication and integrity audit system based on convergent encryption for cloud storage[J]. Journal on Communications, 2017, 38(S2): 156-163.

[18] 王惠峰, 李战怀, 张晓, 等. 云存储中数据完整性自适应审计方法[J]. 计算机研究与发展, 2017, 54(1):172-183.
WANG H F, LI Z H, ZHANG X, et al. A self-adaptive audit method of data integrity in the cloud storage[J]. Journal of Computer Research and Development, 2017, 54(1):172-183.

[19] KOLHAR M, ABU-ALHAJ M M, EL-ATTY S M A. Cloud data auditing techniques with a focus on privacy and security[J]. IEEE Security & Privacy, 2017, 15(1):42-51.

[20] RODRIGUEZ A, ORTEGA P, CONCEPCION R. An intuitionistic method for the selection of a risk management approach to information technology projects[J]. Information Sciences, 2017, 375: 202-218.

[21] 张玉清, 王晓菲, 刘雪峰. 云计算环境安全综述[J]. 软件学报, 2016, 27(6): 1328-1348.
ZHANG Y Q, WANG X F, LIU X F. Survey on cloud computing security[J]. Journal of Software, 2016, 27(6): 1328-1348.

[22] 叶厚元. 统计学原理与分析[M]. 武汉: 武汉理工大学出版社, 2012.
YE H Y. Statistical principle and analysis[M]. Wuhan: University of Technology Press, 2012.

[23] 李保珲, 徐克付, 张鹏. 虚拟机自省技术研究与应用进展[J]. 软件学报, 2016, 27(6):1384-1401.
LI B H, XU K F, ZHANG P. Research and application progress of virtual machine introspection technology[J]. Journal of Software, 2016, 27(6): 1384-1401.

[24] YU P, XIA M, LIN Q, et al. Real-time enhancement for Xen hypervisor[C]//IEEE. 2010.

[25] HOLIK F, HORALEK J, MARIK O, et al. Effective penetration testing with metasploit framework and methodologies[C]// IEEE, International Symposium on Computational Intelligence and Informatics. 2015: 237-242.

[26] ABBOTT M L, FISHER M T. The art of scalability: scalable Web architecture, processes, and organizations for the modern enterprise[M]. Addison-Wesley Professional. 2009.

[作者简介]

田俊峰（1965-），男，河北保定人，河北大学教授、博士生导师，主要研究方向为信息安全与分布式计算。

张永超（1991-），男，河北晋州人，河北大学硕士生，主要研究方向为信息安全与分布式计算。