基于虚拟化技术的入侵容忍系统

云计算将计算任务分布在大量计算机构成的虚拟资源池上，使各种应用系统能够根据需要获取计算能力、存储空间和各种软件服务。云计算带来的服务整合与按需供给能够显著提高计算资源的利用率，降低每服务的能耗量，并且有效屏蔽计算资源的出错问题。然而云计算依然面临着云计算平台的容忍入侵性和新企业数据中心数据的容忍入侵性。国内外许多研究机构和组织对容忍入侵的研究大多是在真实硬件平台上采用门限密码学、秘密共享以及分布式冗余复制等技术；都要求系统具有高计算能力和高存储能力，并且这些资源一般不能分割，是针对特定应用而设计，因此资源利用率低，难以管理，通用性差；另外系统对冗余组件的数目与质量也有较高要求，并且冗余组件恢复时严重影响服务的可用性。因此，这样高昂代价的容忍入侵对于云计算服务提供商和用户来说是很难接受的，并且不适用于云计算的虚拟化。

为解决云计算平台和新企业数据中心数据的容忍入侵性问题，本文通过研究现有的虚拟化技术和秘密共享，构建了一种基于云计算的虚拟化容忍入侵系统，并基于此提出了一种基于虚拟攻击结构的云计算数据中心敏感数据容忍入侵保护的方案。该系统使用了异构容错模型、活动与被动副本、状态更新与状态转移、积极恢复和多样性策略，初步实现了在N=2F+1个副本中容忍F个副本的错误；并保证系统在无人入侵时只有F+1个活动副本在执行，其余副本置于被动模式，这样大量减少了云平台资源的消耗。最后我们验证了敏感数据的容忍入侵方案通过秘密共享实现了关键数据或敏感数据的重构特性和保密特性。

**引言**

云计算将计算任务分布在大量计算机构成的虚拟资源池上，时各种应用系统能够根据需要获取计算能力、存储空间和各种软件服务。云计算带来的服务整合与按需供给能够显著提高计算资源的利用率，降低每服务的能耗量，并且有效屏蔽计算资源的出错问题。云计算具有超大规模、虚拟化、高可靠性、通用性、高扩展性、按需服务、极其廉价等优点。但云计算依然面临着以下问题：

1. 数据的容忍入侵性：云计算最重要的两个问题是保密性和安全性。企业把企业信息、客户信息等敏感的商业数据存放到云计算服务提供商手中，通过减少对某些数据的控制来节约经济成本，因此企业必然会担心数据放在云端安全吗？会不会被泄密和窃取？
2. 云计算平台的容忍入侵性：云计算模式下，所有的业务处理都将在服务器端完成，因此云计算平台就成为入侵者攻击的核心；另外云计算平台自身也面临着各式各样无法预料的错误，比如2010年上半年，Amazon云计算服务就因为人为失误和意外停电事故出现故障，致使美国东部的少量用户失去服务并导致极少数据丢失。因此如果服务器一旦出现问题，就将导致所有的服务无法正常运行，数据无法访问。

对于云计算面临的保密性、完整性、可用性和可靠性等问题，传统的安全技术如入侵检测、防火墙、加解密等都无法完全保证，但是一种可生存技术即容忍入侵技术可以很好的弥补。本文将通过研究相关的容忍入侵技术来解决云计算平台和新企业数据中心敏感数据的容忍入侵问题。

容忍入侵主要思想就是利用分布式系统中的硬件或者软件容错技术屏蔽任何入侵或者攻击对系统功能的影响，保证系统关键功能的安全性和连续性。国内外许多研究机构和组织对容忍入侵的研究大多是在真实硬件平台上采用门限密码学、秘密共享以及分布式冗余复制等技术；这些方案都要求系统具有高计算能力和高存储能力，并且这些资源一般不能分割，是针对特定应用而设计，因此资源利用率低，难以管理，通用性差；另外系统对冗余组件的数目与质量也有较高的要求，并且冗余组件恢复时严重影响服务的可用性。当前秘密共享方案大多基于存取结构，但在设计容忍入侵系统时，要想根据系统的配置（属性）及其安全性需求确定出相应的存取结果十分困难，原因在于存取结构描述的是系统中的合格（授权）子集，而系统配置及安全性需求等描述的则是系统面临的威胁和自身的漏洞，以及在该配置下应达到的安全性目标等。另外，如果在真实硬件平台上实现秘密共享要求每个参与方都是一个真实的服务器节点，对于运行关键业务的大型平台来说，秘密共享则需要大量物理机节点的参与，这对资源的消耗和浪费是相当大的。因此这样高昂代价的容忍入侵对于云计算服务提供商和用户来说是很难接受的，并且不适用于云计算的虚拟化。

虚拟化技术自1960s诞生以来发展已经相当成熟了，但其应用大多仍是关于资源的高效管理，实际上虚拟化技术也可以用来构建安全系统，如Hans P.Reiser, Rudiger Kapitza 等人就在虚拟化技术上研究过容忍入侵系统。随着云计算的提出，研究虚拟化技术上云计算的安全性变得至关重要。

为了解决云计算平台的容忍入侵性问题，本文提出了一种基于云计算的虚拟化容忍入侵（Virtualization Intrusion Tolerance Based on Cloud Computing,CC-TIV）方案，该方案能在N=2F+1个副本中容忍F个副本的错误，并保证系统在无入侵时只有F+1个活动副本在执行，其余副本处于被动模式，这样大量减少了云平台资源的消耗。而传统的Byzantine容错算法容忍F个错误副本需要N=3F+1个副本。

对于云计算新企业数据中心敏感数据的容忍入侵性问题，本文基于CC-VIT模型提出了一种基于虚拟攻击结构的云计算数据中心敏感数据的容忍入侵保护方案，该方案将敏感数据分割成片段（划分）分发给每个参与方，保证使得只有合法的参与者才能联合他们的划分重构敏感数据，同时非法的参与者联合他们的划分不能获得关于敏感数据的任何信息。该方案中所有的参与方都是运行于虚拟机监控器上的虚拟机，因此节省了大量的物理机服务器。最后我们验证了敏感数据的容忍入侵方案实现了敏感数据的重构特性和保密特性，即该方案能有效保证敏感数据的安全性和完整性，并能有效降低物理资源的消耗。

1. **绪论**
   1. 本文背景

从2007年下旬开始，“云计算”变成了炙手可热的一个词。Google 、Amazon、IBM、微软和Salesforce等巨头们以其前所未有的速度和规模推动云计算技术及其产品的普及，一些学术活动迅速将云计算提上议事日程，支持和反对的声音不绝于耳。

从图1.1中Google对关键词“Cloud Computing”的搜索趋势反映出，“Cloud Computing”是2007年第4季度才兴起的一个词汇，并从此成为世人搜素和关注的热点。

我国对云计算的关注和研究也较早，业界和政府有关部门高度重视这一新兴的技术。为了把握云计算的实质内涵及发展趋势，探讨云计算对产业、教育和社会发展的影响，交流国内外云计算的最新研究成果，分享云计算应用的实践经验，在中国工业和信息化部、教育部、中国科协及相关部委的指导下，中国电子学会于2009年5月22日在北京中国大饭店隆重举办首届中国云计算大会，到2011年5月20日已是举办第三届中国云计算大会。每届中国云计算大会都云集了大批两院院士、IT企业精英高管、各大科研院所的专家学者等，可谓是群英荟萃，举世瞩目的盛会。

虽然云计算在中国的发展时间并不长，但最新数据显示，其发展已经具备了一定的规模，且呈现上升之势。2010年5月21日第二届中国云计算大会上，由埃森哲卓越绩效研究院与中国电子学会云计算专家委员会推出权威的云计算调研报告《中国云计算发展的务实之路》，该报告给出了当前中国云服务供应商名单节选。

在报告名单节选中，八百客位居SaaS供应商之首，是当之无愧的中国SaaS业第一品牌。800APP在企业的应用也作为唯一的CRM案例成功入选报告。其中SaaS即云计算的软件即服务（software as a Service ,SaaS）。

* + 1. 云计算的出现与发展

云计算是一种新兴的商业计算模型。它将计算任务分布在大量计算机构成的资源池上，使各种应用系统能够根据需要获取计算力、存储空间和各种软件服务。这种资源池称为“云”。“云”是一些可以自我维护和管理的虚拟计算资源等等。云计算将所有的计算资源集中起来，并由软件实现自动管理，无需人为参与。这使得应用提供者无需为繁琐的细节而烦恼，能够更加专注于自己的业务，有利于创新和降低成本。

资源池之所以称为“云”，是因为它在某些方面具有现实中云的特征：云一般都较大；云的规模可以动态伸缩，它的边界是模糊的；云在空中飘忽不定，我们无法也无需确定它的具体位置，但它确实存在于某处。资源池之所以称为“云”，还因为云计算的鼻祖之一亚马逊公司将曾经大家称作网格计算的东西，取了一个新名称“弹性计算云（EC2），并取得了商业上的成功。

http://xueshu.baidu.com/s?wd=paperuri%3A%28b48a224b73e0c5a1052f93c5c6f5e862%29&filter=sc\_long\_sign&tn=SE\_xueshusource\_2kduw22v&sc\_vurl=http%3A%2F%2Fwww.doc88.com%2Fp-9562751613796.html&ie=utf-8&sc\_us=9898530859111783519