# 浅谈云安全

方杰

（廊坊师范学院信息与计算科学系　　廊坊 065000）

**摘要：**本文将对云计算技术进行简单介绍，探讨了云安全的特点、模式、现状及前景。

**关键词：**云计算　云安全　云安全探针　服务器集群

## 引言

任何技术概念都不是空穴来风，许多概念本身都是有关联的，技术都有或远或近的亲缘关系。云计算是个宏观的概念，其具体实施，可能与 Web Servise、SOA、XmlPRC、SaaS 都有关系。云计算即将把互联网上的各种计算资源整合在一起，例如 PC、手机、掌上电脑及其他移动终端，实现计算的无处不在、无时不在，在云计算时代，“网络就是计算机”有望成为可见的东西。

## 一、从云计算到云安全

1.云计算的含义

云计算（Cloud computing），是指基于互联网的超级计算模式。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。即把存储于个人电脑、移动电话和其他设备上的大量信息和处理器资源集中在一起，协同工作。它是一种新兴的共享基础架构的方法，可以将巨大的系统池连接在一起以提供各种 IT 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，通常为一些大型服务器集群，包括计算服务器、存储服务器、宽带资源等等。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。用户只需能够接入互联网，就可以通过电脑、手机等终端设备，在任何地点方便快捷的使用数据和服务，而不需关心存储或计算发生在哪朵“云”上（如图 1 所示）。可见，云计算将改变传统以个人计算机为基础的生产模式，Web 将成为交往聚合与设备聚合的中枢，最终改变人们获取信息、分享内容和互相沟通的方式。主要的 IT 厂商，如谷歌（Google）、微软（Microsoft）、IBM、雅虎（Yahoo）、亚马逊（Amazon）等，都已经具有并正在建设“云”。在云计算中，用户所处理的数据并不存储在本地，而是保存在互联网上的数据中心，用户所需的应用程序并不运行在用户的个人电脑、手机等终端设备上，而是运行在互联网上大规模的服务器集群中。提供云计算服务的企业负责管理和维护这些数据中心的正常运作。

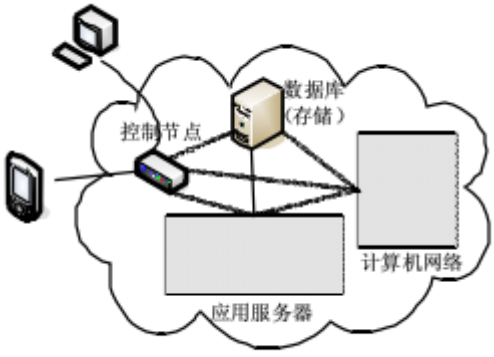



图 1 云计算系统图

2.云计算的特点和优势

（1）可靠、安全的数据存储

云计算提供了最为可靠安全的数据存储中心，数据（如文档和媒体）将会自动同步，通过 Web 可在所有的设备上使用。这样避免了用户将数据存放在个人电脑上可能造成的数据丢失或病毒等问题。同时，云计算通过严格的权限管理策略支持数据的共享。

（2）方便、快捷地云服务

云计算时代，用户将不需要安装和升级电脑上的各种应用软件，只需要具有网络浏览器，就可以方便快捷地使用云计算提供的各种服务。这将有效地降低技术应用的难度曲线，进一

步推动 Web 服务发展的广度和深度。

（3）强大的计算能力

云计算为网络应用提供了强大的计算能力，可以为普通用户提供每秒 10 万亿次的运算能力，完成用户的各种业务要求。这种超级运算能力在普通计算环境下是难以达到的。

（4）经济效益

据预计，相对于机构自身运营的数据中心而言，云计算服务提供商的存储成本一般只有其十分之一，而带宽成本只有二分之一，计算处理能力成本只有三分之一。这将帮助一些机构以比较低廉的架构成本进行运作。

3.云安全

紧随云计算、云存储之后，云安全也出现了。云安全是我国企业创造的概念，在国际云计算领域独树一帜。“云安全（Cloud Security）”计划是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到 Server 端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。未来杀毒软件将无法有效地处理日益增多的恶意程序。来自互联网的主要威胁正在由电脑病毒转向恶意程序及木马，在这样的情况下，采用的特征库判别法显然已经过时。云安全技术应用后，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理。整个互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。

云安全的概念提出后，曾引起了广泛的争议，许多人认为它是伪命题。但事实胜于雄辩，云安全的发展像一阵风，瑞星、趋势、卡巴斯基、MCAFEE、SYMANTEC、江民科技、PANDA、金山、360 安全卫士、卡卡上网安全助手等都推出了云安全解决方案。瑞星基于云安全策略开发的 2009 新品，每天拦截数百万次木马攻击。趋势科技云安全已经在全球建立了 5 大数据中心，几万部在线服务器。据悉，云安全可以支持平均每天 55 亿条点击查询，每天收集分析 2.5 亿个样本，资料库第一次命中率就可以达到 99%。借助云安全，趋势科技现在每天阻断的病毒感染最高达 1000 万次。但建立这样的云安全系统并非易事。

4.云安全系统的难点

要想建立“云安全”系统，并使之正常运行，需要解决四大问题：

（1）需要海量的客户端（云安全探针）。只有拥有海量的客户端，才能对互联网上出现的恶意程序，危险网站有最灵敏的感知能力。一般而言安全厂商的产品使用率越高，反映应当越快，最终应当能够实现无论哪个网民中毒、访问挂马网页，都能在第一时间做出反应。

（2）需要专业的反病毒技术和经验。发现的恶意程序被探测到，应当在尽量短的时间内被分析，这需要安全厂商具有过硬的技术，否则容易造成样本的堆积，使云安全的快速探测的结果大打折扣。

（3）需要大量的资金和技术投入。“云安全”系统在服务器、带宽等硬件需要极大的投入，同时要求安全厂商应当具有相应的顶尖技术团队、持续的研究花费。

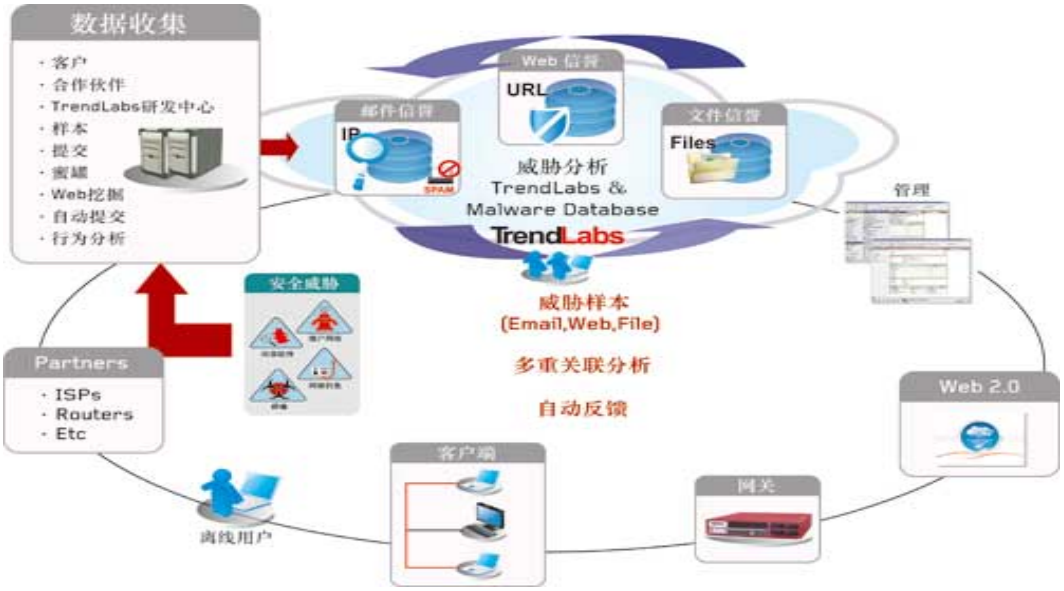
（4）可以是开放的系统，允许合作伙伴的加入。“云安全”可以是个开放性的系统，其“探针”应当与其他软件相兼容，即使用户使用不同的杀毒软件，也可以享受“云安全”系统带来的成果。

## 二、两种云安全模式

当前已经出现的云安全实现原理大概可以分为两种：

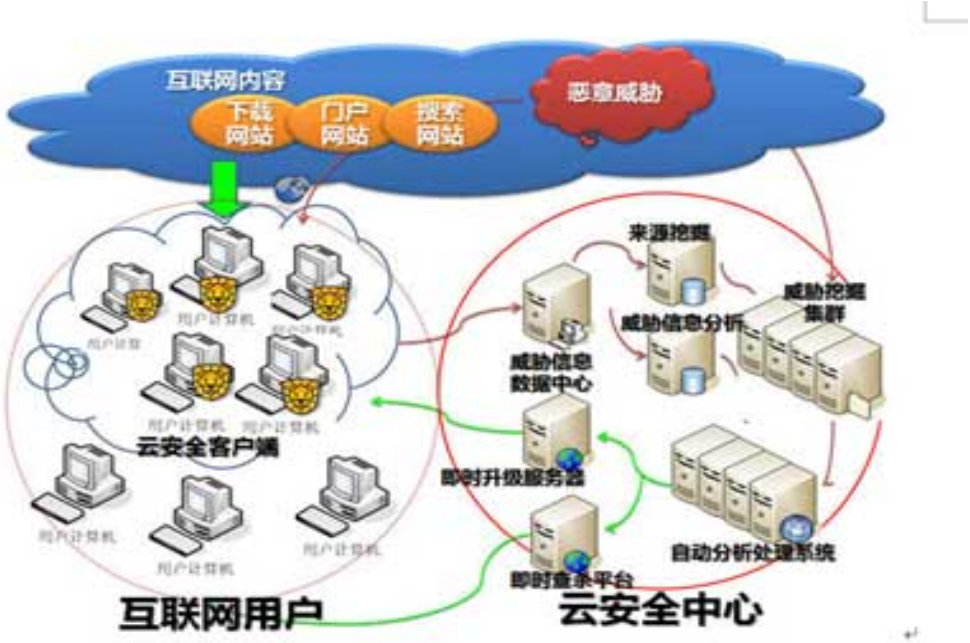
一种是由趋势科技提出的“Secure Cloud”，以Web信誉服务(WRS) 、邮件信誉服务(ERS)和文件信誉服务(FRS)为基础架构的云客户端安全架构，把病毒特征码文件保存到互联网云数据库中，令其在端点处保持最低数量用于验证。其核心在于两点：(1)对复合式攻击的拦

截。通过对疑似病毒组件各部分外延属性进行检查，判断威胁程度；(2)瘦客户端。大量的病毒特征码保存在云数据库中。简言之，趋势科技云安全技术基于其拥有庞大的服务器群和并行处理能力，构架了一个庞大的黑白名单服务器群，用于客户端查询，在 Web 威胁到达最终用户或公司网络之前即对其予以拦截。




趋势科技云安全架构图

另一种就是由国内安全厂商瑞星提出，与趋势科技服务器群“云”不同，瑞星的“云”则建立在广大的互联网用户上。通过在用户客户端安装软件监控网络中软件行为的异常，将发现的疑似木马、恶意程序最新信息推送到瑞星的服务器进行自动分析和处理，然后再把病毒和木马的解决方案分发到每一个客户端。




瑞星云安全架构图

以上两种云安全概念采用的是两种完全不同的模式。趋势科技强调的是阻止外来威胁，基础是庞大的服务器群；瑞星强调的则是对用户计算机上业已存在的未知威胁进行感知，基础是必须拥有大量的客户端用户。两者虽模式不同，但都存在一定缺陷。趋势科技忽略了对

本机威胁的收集，而瑞星的云安全则只能被动防守，不能在未知威胁进入到电脑前进行拦截。另一方面，现在的信息安全公司还没有建成 Google 那样数以万计的服务器群和非常成熟的并行处理技术，还需加强对基础硬件的投入和升级，或者加大与第三方云计算服务提供商的合作。

## 三、我国云安全技术现状

云安全，其实就是从过去传统的单机杀毒模式，转换成网络化的主动防毒。杀毒软件利用互联网强大的网络支持，通过互联网实时监控用户主机，在用户即将访问有害网页或病毒程序前提醒用户。新模式与传统杀毒方式的最大转变正在于，从过去由用户受到攻击之后再杀毒到现在的侧重于防毒。云安全中的很多技术其实早已应用到企业安全领域，而过去受市场环境限制，这项技术并未向个人用户推广。但随着近几年家庭和个人互联网用户数量的不断增加，对信息安全要求越来越高，云安全开始走进普通大众视眼。在去年各大厂商做足概念后，今年云安全将进入全面产品化和推广阶段。

由于病毒木马变得更加隐蔽，不像过去那样会让用户电脑鸡飞狗跳或完全瘫痪，更多的是驻留在用户后台，秘密窃取信息，比如银行帐号信息、游戏卡、游戏币以及个人信息。

因此在应对措施上，一方面杀毒软件厂商需要大力推进云安全技术，使用最新的基于主动防御的保护技术，采取例如对中央数据库的在线访问申请，下载软件时限制访问权限，安全更新管理系统以及可信任程序列表等措施，这些方法都能有效地加强传统的基于签名方式的反病毒保护效果。

而在另一方面，大多数用户还未充分意识到当前 Web 安全威胁和风险对信息安全的巨大影响，有很多用户在不知不觉中容忍着各种间谍软件、傀儡程序、键盘记录软件、广告软件在主机中运行，给个人电脑和企业信息安全带来巨大的安全风险。尤其对于企业来说，加强终端安全防护和网关建设，以及提高内部数据安全管理的工作已经刻不容缓。

## 结语

云计算是未来 IT 互联网产业发展的趋势，虽然目前还存在各种难以普及的问题，但是无论微软、oracle 等企业多么希望死守桌面软件，这种成本低廉、性能超群的云计算还是会普及，而趋势科技等企业的“云安全”已经可以为普通用户提供服务，带来价值。并让人们看到了“云计算”应用到安全领域后，将会为安全领域带来巨大的变化。有理由相信，“云安全”将是大势所趋，而“云安全”时代的到来，也必将伴随着安全行业的一场巨大变革。

**参考文献：**

[1]王萍. 张际平. 云计算与网络学习. 现代教育技术. 2008 年第 11 期. 第 18 卷

[2]Ammon.云计算简介[EB/OL].
http://soft.yesky.com/info/333/8065833.shtml,2008-04-06/2008-06-26.

[3]吴珍. 漫步云端——探秘云安全.《信息安全与通信保密》. 2008 年 11 期