**云计算及其安全技术分析**

# ****云计算和云计算安全****

云计算（cloud computing）是基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源。云是网络、互联网的一种比喻说法。过去在图中往往用云来表示电信网，后来也用来表示互联网和底层基础设施的抽象。狭义云计算指IT基础设施的交付和使用模式，指通过网络以按需、易扩展的方式获得所需资源；广义云计算指服务的交付和使用模式，指通过网络以按需、易扩展的方式获得所需服务。这种服务可以是IT和软件、互联网相关，也可是其他服务。它意味着计算能力也可作为一种商品通过互联网进行流通。

云计算由于用户和资源的高度集中,面临着更多的问题，而安全问题首当其冲。在近几年来，随着云计算的不断普及,安全问题的重要性呈现逐步上升趋势,已成为制约其发展的重要因素。Google, Microsoft，Amazon等公司的云计算服务均出现过重大故障，例如,2009 年3 月,Google 发生大批用户文件外泄事件,2009 年2 月和7 月,亚马逊的“简单存储服务(simple storage service,简称S3)”两次中断导致依赖于网络单一存储服务的网站被迫瘫痪等等。

不断爆出的各种安全事故导致用户的信息服务受到影响，进一步加剧了业界对云计算安全的担忧。因此,要让企业和组织大规模应用云计算技术与平台,放心地将自己的数据交付于云服务提供商管理,就必须全面地分析并着手研究云计算所涉及到的安全技术。

总体来说，云计算技术主要面临以下五个安全问题，如下图所示：

(1).    用户身份管理/访问控制

(2).    网络安全

(3).    数据安全

(4).    管理安全

(5).    虚拟化安全

# ****云计算安全技术分析****

## ****用户身份管理与访问控制技术****

1.1身份管理

用户身份管理就是要对用户的身份采用相应的技术进行管理，这样用户每次要求访问资源的时候都要进行认证，可以增强安全性。典型的身份认证技术如下：

(1).    口令认证

这是一种最为简单的认证技术。它的缺陷也很明显，一般情况下，用户所设计的口令都比较简单，容易被猜测。

(2).    Kerberos认证协议。

Kerberos是基于可信赖第三方（TrustedThird Party，TTP）的认证协议。该协议实现集中的身份认证和密钥分配，通信保密性、完整性。但是该协议对时钟同步的要求挺高，并且由于它是针对对称密钥的设计，不适合大规模的应用环境。

(3).    公开密钥体系结构**PKI**

**PKI**技术采用证书管理公钥，通过第三方的可信任机构**CA**把用户的公钥和用户的其它标识信息**(**如名称、**e-mail**、身份证号等**)**捆绑在一起，在**Internet**网上验证用户的身份。

(4).    基于生物特征的身份认证

由于每个人具有唯一的生理特征，我们根据这些生理特征进行身份认证，典型的技术有指纹识别，虹膜识别，语音识别。

1.2访问控制技术

访问控制（AccessControl）指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源能力的手段。典型的访问控制技术如下：

(1).自主访问控制(DAC)

l  介绍：

自主访问控制（Discretionary Access Control，DAC）是一种接入控制服务，通过执行基于系统实体身份及其到系统资源的接入授权。包括在文件，文件夹和共享资源中设置许可。用户有权对自身所创建的文件、数据表等访问对象进行访问，并可将其访问权授予其他用户或收回其访问权限。允许访问对象的属主制定针对该对象访问的控制策略，通常，可通过访问控制列表来限定针对客体可执行的操作。

l  优点：

DAC提供了适合多种系统环境的灵活方便的数据访问方式，是应用最广泛的访问控制策略。

l  缺点:

DAC提供的安全性相对较低，无法对系统资源提供严格保护。

(2).强制访问控制(MAC)

l  介绍：

强制访问控制（MAC）是系统强制主体服从访问控制策略。是由系统对用户所创建的对象，按照规定的规则控制用户权限及操作对象的访问。

l  优点:

MAC常用于多级安全军事系统，对专用或简单系统较有效.同时强制访问控制提供了一个不可逾越的、更强的安全保护层，以防范偶然或故意地滥用DAC。

l  缺点：

对复杂的商业系统并不适用，因此它并不适用云计算。

(3).基于角色的访问控制(RBAC)

l  介绍：

通过对角色的访问所进行的控制。使权限与角色相关联，用户通过成为适当角色的成员而得到其角色的权限。

l 优点：

目前应用最为广泛的访问控制技术。它减小了授权管理的复杂性，降低管理开销，提高企业安全策略的灵活性。

## ****网络安全****

2.1云计算中的网络问题

网络安全指的是在网络环境下识别和消除不安全因素的能力。云计算环境中存着在多种网络安全威胁问题，主要是以下两种攻击方式。

(1).    拒绝服务攻击

拒绝服务攻击指攻击者想办法让目标服务器停止提供服务甚至主机死机。如攻击者频繁地向服务器发起访问请求，造成网络带宽的消耗或者应用服务器的缓冲区满溢：该攻击使得服务器无法接收新的服务请求，其中包括了合法客户端的访问请求。例如。一个黑客劫持了Web服务器，使其应用服务停止运行，导致服务器不能提供Web服务。在云计算中，黑客对服务器开展拒绝服务攻击时，会发起成千上万次的访问请求到服务器，导致服务器无法正常工作。无法响应客户端的合法访问请求。针对这种攻击，可以采用的应对策略是减少连接到服务器的用户的权限，这将有助于降低拒绝服务攻击的影响。

(2).    中间人攻击

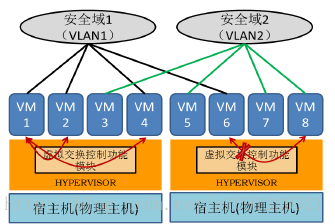
中间人攻击是另一种网络攻击手段。攻击者通过拦截正常的网络通信数据。并进行数据篡改和嗅探，而通信的双方却毫不知情。在网络通信中，如果安全套接字层(SSL)没有正确配置，那么这个风险问题就有可能发生。例如，如果通信双方正在进行信息交互，而SSL没有正确地安装，那么所有双方之间的数据通信，都有可能被黑客侵入获取。针对这种攻击手段，可以采用的应对措施是正确地安装配置SSL。而且使用通信前应由第三方权威机构对SSL的安装配置进行检查确认。

2.2安全域划分

正是因为存在这些网络问题，我们需要划分安全区域，保证网络安全。安全域是指同一环境内有相同的安全保护需求、相互信任、并具有相同的安全[访问控制](http://zhidao.baidu.com/search?word=%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6&fr=qb_search_exp&ie=utf8" \t "https://blog.csdn.net/a1091220321/article/details/_blank)盒边界控制策略的网络或系统。如今市场上主要有以下两种划分安全域的技术。

(1).利用**Hypervisor**实现安全域划分

以VMware为代表的虚拟化厂家，在Hypervisor层或主机服务器的特定虚拟机部署和执行VLAN划分策略，实现VLAN划分。如下图：

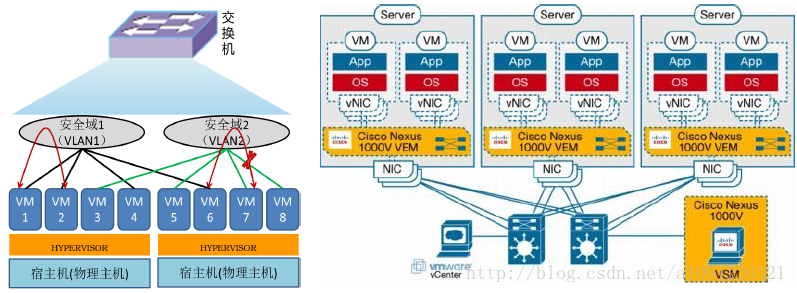


该模式用VM将每个安全域划分成几个模块，然后存在逻辑关机的模块寄宿在物理主机上面，通过虚拟交换控制模块进行监控保障安全。

该方式主要有以下缺点：实现业务系统VLAN划分的Hypervisor层虚拟交换控制功能或主机服务器中特定虚拟机将大量消耗物理主机内的计算资源，从而挤占业务系统可用资源；实现安全功能的虚拟机也将成为信息交换的性能瓶颈，而且业务系统虚拟机在不同物理主机服务器间做迁移时，安全策略需要同步迁移。

(2).借助物理交换机实现虚拟安全域划分

以Cisco、HP等交换机厂家将虚拟机的网络流量通过引出到传统网络设备(防火墙、交换机等)，由物理交换机进行VLAN的划分。如下图：



Cisco：利用VN-TAG标记来唯一标识虚拟机，物理交换机根据这一标识来区分不同的虚拟机流量，并进行虚拟机安全策略的配置、管理。

 HP：通过修改“生成树协议”，并定义新的VLAN标记来标识虚拟机，进而使物理交换机通过这一标记实现对虚拟机的监控、管理。

(3).两种安全区域划分对比

VMware为代表虚拟化厂家解决方案，将传统安全防护设备虚拟化，与Hypervisor（虚拟化管理）功能整合，通过其内部的逻辑端口监测虚拟机间数据流量， 实现对虚拟机的安全管理。该方式无需改造交换机，但消耗资源多，不便于灵活实施安全策略；

 以主流交换机制造商为代表的解决方案，标识虚拟机并将其流量引出，通过物理交换机实现流量监测。交换机与Hypervisor层紧耦合，需采用新型交换机及更高处理能力的网络设备，但能实施较灵活的虚拟机流量监控策略，可扩展性强，成为业界主流方案。

## ****数据安全****

3.1数据加密机制

(1).基于属性的加密

基于属性的加密体制是基于身份加密的延伸，身份用一系列描述性的属性表示；也是基于模糊身份加密体制的具体应用，同时添加了一个更具灵活性的访问结构。它最突出的优点就是很适用于分布式环境下解密方不固定的情况。加密方加密信息时不需要知道具体是谁解密，而解密方只需要符合相应条件便可以解密。它的这种灵活性使得它在许多特定领域有比基于证书，甚至基于身份的密钥体制更好的适用性。

(2).KP-ABE算法

KP-ABE(密钥策略的基于属性的加密体制）它主要是针对现在很多用户的敏感信息都存储在第三方网站上而难于灵活地控制其访问权限的问题而提出。这个方案就可以避免用户直接将密钥告诉授权用户，而是授权用户可根据自己的属性恢复出密钥，而这个密钥只可以解密那些他有权限访问的加密数据。

(3).CP-ABE算法

CP-ABE(密文策略的基于属性的加密体制) 该方案中，密文中嵌入了访问控制结构，即加密之后就确定了哪些用户能够对它进行解密而不需要借助可信服务器来实现这种控制。因此，加密方可以控制主动权，只有满足密文策略的访问者才能获得解密密钥的权利。基本原理是：必须提供自己的用户属性给服务器端，在服务器端，将用户提供的属性通过由资源属性组成的访问控制树来判断用户是否能获得访问资源的私钥。一旦用户通过访问控制树，则用户能访问服务器端的资源。

3.2基于代理重加密

在代理重加密中，一个半可信代理人通过代理授权人产生的转换密钥Rk把用授权人Alice的公钥Pa加密的密文转化为用被授权人(Delegatee)Bob的公钥Pb[加密](http://www.cksis.com/" \t "https://blog.csdn.net/a1091220321/article/details/_blank)的密文，在这个过程中，代理人得不到数据的明文信息，从而降低了数据泄露风险。而这两个密文所对应的明文是一样的，使Alice和Bob之间实现了数据共享。所谓的半可信，指的是只需相信这个代理者Proxy -定会按方案来进行密文的转换。

(1).云计算中使用代理重加密实现授权管理  
当云计算的用户需要为其他用户授权时，需要取得对方的公钥，针对每个用户生成对应的转换密钥，并通过安全的信道传递给云端。这样，云端对于每一个被授权的用户都生成一份重加密密文，对于未被授权用户没有对应的重加密密文。即使未被授权用户得到针对其他用户的重加密密文，也无法解密出明文。也可以将基于属性的加密(ABE，Attribute-based Encryption)理念应用于代理重加密，使用这样的代理重[加密算法](http://www.cksis.com/blog/category/jiamisuanfa" \t "https://blog.csdn.net/a1091220321/article/details/_blank)，可以一次为多个具有同样一组属性的用户授权。

(2).    云计算中使用代理重加密实现访问控制  
用户请求访问数据文件时，云端通过对该用户的身份认证及权限认证，判断用户是否可以读取该数据文件，如果用户拥有这一权限，云端将根据用户公钥向其返回数据密文和对应的密钥密文，用户可以通过依次解密这两个密文文件得到数据的明文。如果云端没有对应于用户公钥的密钥密文，则用户没有被文件所有者授予访问这一数据文件的权限。

3.3海量密文数据环境下快速检索机制

         云计算服务商能实现密文数据状态下的快速检索，海量密文数据环境下快速检索机制中方法如下：

(1).    安全索引

a)        核心思想

所用密钥事先生成逆hash序列，然后由该序列生成多个陷门，然后检测。对返回的文档解密就得到原文。

b)        优点

解决了简单索引方式易受统计攻击的问题。

c)        缺点

需要生成大量的密钥，随着检索次数的增加，计算复杂度也会增加。

(2).    基于关键词的公钥搜索

a)        核心思想

首先生成公钥和私钥，对明文关键词用公钥加密，生成密文信息。

b)        优点

解决了存储、计算资源分布的不对称性。同时解决了用户在移动情况下的需求。

c)        缺点

适用在海量环境中，还需进一步优化。

(3).    相关排序的加密索引

a)        核心思想

对文档中关键词词频加密，检索时服务器先检索出相关文档，然后进行排序，返回评价值最高的加密文档。

b)        优点

把最可能相关的文档返回给用户。

c)        缺点

不适用一个查询中包含多个查询词的情况，并且无法利用词的逆文档频率。

(4).    基于全同态加密的检索方法

a)        核心思想

计算检索出的文档与查询信息之间的相关度，然后统计词频和文档频率，然后用全同态方法对文档加密并建立索引

b)        优点

既保护了用户的数据安全，又提高了检索性能。

c)        缺点

适用在海量环境中，还需进一步优化。

## ****管理安全****

4.1安全管理模型

不同的云计算服务提供模式创建了不同的安全管理边界,以及由运行商和用户共享责任的安全管理模型。比如对SAAS，主要由运营商担负安全管理责任；对PAAS，由运营商和用户共同分担安全管理责任；对IAAS，运营商仅负责网络、云平台等基础设备安全管理，而用户负责业务系统安全管理。面对不同的数据、应用、平台以及网络，用户和运营商各自承担的管理责任不同，从而得到更好安全管理模型。

4.2安全管理标准

         安全管理标准，规定了安全管理边界的界定条件，运营商和用户联动方式等。从而实现云服务的可用性管理、漏洞管理、补丁管理、配置管理以及时间应急响应等。

## ****虚拟化安全****

虚拟化技术是实现云计算的关键核心技术,使用虚拟技化术的云计算平台上的云架构提供者可以向其客户提供安全性和隔离保证。

虚拟化技术是将各种计算及存储资源充分整合和高效利用的关键技术。虚拟化是为某些对象创造的虚拟化（相对于真实）版本，比如操作系统、计算机系统、存储设备和网络资源等。

5.1安全运行

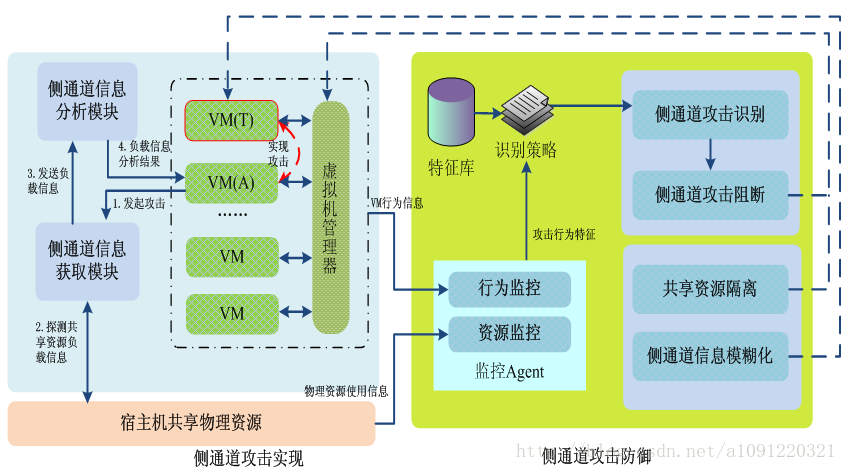
虚拟化技术是表示计算机资源的抽象方法，通过虚拟化可以用与访问抽象前资源一致的方法访问抽象后的资源，从而隐藏属性和操作之间的差异，并允许通过一种通用的方式来查看和维护资源，从而保证系统可以安全运行。

5.2安全隔离

虚拟化技术将应用程序以及数据，在不同的层次以不同的面貌加以展现，从而使得不同层次的使用者、开发及维持人员，能够方便的使用开发及维护存储的数据、应用于计算和管理的程序。通过采用云存储数据隔离加固技术和虚拟机隔离加固技术，可以使数据和服务端分别隔离，确保安全。

5.3安全监控

基于虚拟化技术，可以进行安全监控。以侧通道攻击监控为例进行说明。如图所示，左半部分是多虚拟机环境下基于Cache的侧通道攻击的实现，右半部分是基于虚拟化技术的安全监控。



在虚拟化技术基础上，采用基于行为监控的侧通道攻击识别方法和基于VMM的共享物理资源隔离算法，可以达到安全监控的目的。流程如下：

          i.    通过虚拟机管理器采集VM行为信息，并将得到的行为信息传递给监控模块；同时采集物理资源使用信息传递给监控模块；

        ii.    在监控模块，将行为监控和资源监控获取的信息进行分析，将得到的攻击的行为特征；

       iii.    基于已有的特征库，对攻击行为特征进行识别策略；

       iv.    识别出测通道攻击，进而阻断测通道攻击；

        v.    最后进行共享资源隔离和侧通道信息模糊化的实现

# ****总结****

   云计算所涉及到的安全技术，包括用户身份管理/访问控制，网络安全，数据安全，管理安全，虚拟化安全五个方面，云计算是当前发展十分迅速的新兴产业，具有广阔的发展前景，同时其面临的安全技术挑战也是前所未有的。未来与云计算安全相关的技术也会在以上这几个方面有更深的发展。