云计算中的数据安全研究综述

【摘要】云计算是一种以服务为特征的计算模式，近年来已发展成为当前互联网领域的研究热点。随着云计算的普及，如何提供安全的云数据是云计算中亟待解决的问题。本文将探讨云计算所带来的数据安全风险，并从传输安全、存储安全、数据残留、数据审计等四个方面阐述数据安全策略，确保云计算平台用户数据的完整性和安全性。

【关键词】云计算；数据安全；安全策略

一、引言

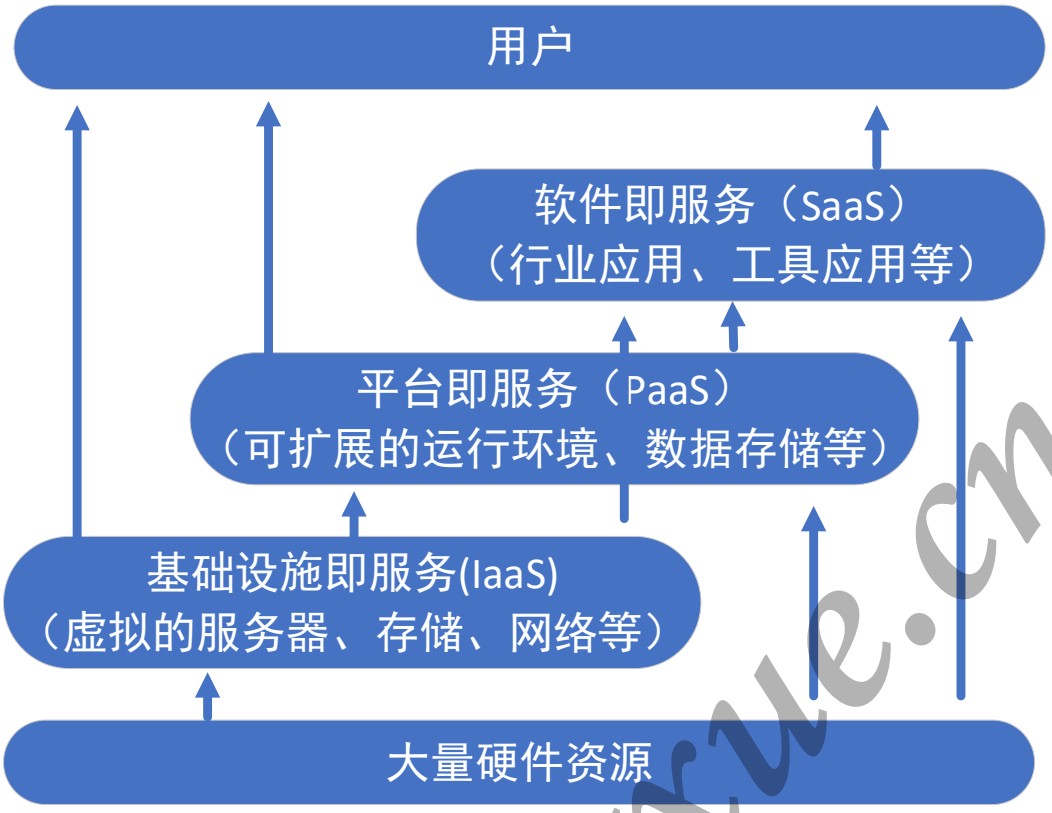
云计算是指服务的交付和使用模式，通过网络以按需、易扩展的方式获得所需的服务。它通过对所有资源进行抽象后以新的业务模式提供高性能、低成本的持续计算、存储空间及各种软件服务，支撑各类信息化应用。

目前，云计算的主要服务形式有三种：

1）软件即服务（SaaS）：提供给客户的服务是服务商运行在云计算基础设施上的应用程序，可以在各种客户端设备上通过瘦客户端界面访问。客户不需要管理或控制的底层的云计算基础设施，包括网络、服务器、操作系统、存储，甚至单个应用程序的功能。

2）平台即服务（PaaS）：提供给客户的是将客户用供应商提供的开发语言和工具，创建的应用程序部署到云计算基础设施上去。客户不需要管理或控制的底层的云基础设施，包括网络、服务器、操作系统、存储，但客户能控制部署的应用程序，也可能控制应用的托管环境配置。

3）基础设施即服务（IaaS）：提供给客户的是出租处理能力、存储、网络和其它基本的计算资源，用户能够部署和运行任意软件，包括操作系统和应用程序。客户不管理或控制的底层的云计算基础设施，但能控制操作系统、储存、部署的应用，也有可能选择网络组件。



通过云计算原理不难看出云计算有以下特点：

1）虚拟化：支持用户在任意位置、使用各种终端获取应用服务；

2）高可靠性：使用了数据多副本容错、计算节点同构可互换等措施来保障服务的高可靠性；

3）通用性：云计算不针对特定的应用，同一个“云”可以同时支撑不同的应用运行

4）高可扩展性：“云”的规模可以动态伸缩，满足应用和用户规模增长的需要；

5）按需服务：“云”是一个庞大的资源池，可以按需购买。

二、云计算给数据安全带来的风险

云计算在迅猛发展的同时，云安全问题也受到越来越多的关注。作为一种全新的服务模式，其面临的安全威胁也是前所未有的，其中公认最核心的问题是数据安全问题。云计算的一个关键特征就是其服务是通过网络来提供的。所有用户的数据都存放在云端，并将计算结果通过网络回传给客户端。如果在这个过程中受到恶意用户攻击，则将导致数据安全受到威胁，如数据被篡改、删除、窃取等。

总结起来，云计算服务给数据安全带来的风险有以下几个方面：

1）虚拟化带来的安全风险

虚拟技术已经广泛应用于云计算中，它能使不同节点的服务器数据在同一个平台上工作，根据不同访问者的要求进行虚拟机的初始化和云数据计算。由于多个虚拟机在同一个平台上运行，原有数据脱离了硬件的保护，用户通过虚拟化技术共享 CPU、内存、硬盘和网络带宽，存在争夺服务器数据资源的风险。如果用户非法获取虚拟机权限，就有可能威胁到同一台物理服务器上的其他的虚拟机。

2）动态的信任边界

云计算环境中，其工作方式模糊了传统网络中边界的概念，因此既有的硬件安全手段也随之削弱甚至失效，包括网关在内的安全手段都难以依赖。存储和计算资源高度整合使边界无序化，企业的信任边界是动态的，企业无法确定信任边界的变动情况。客户在使用云计算时，可能无法确切地知道数据到底被托管在什么地方，这些数据可能遍布在不断变化的一组主机和数据中心中，因此使得安全设备的效果大打折扣。

3）数据泄露

数据泄露可能发生在数据传输、存储、应用的各个环节。一方面，由于云服务平台的关键数据高密度聚合，给潜在的攻击者带来极大的诱惑，黑客将会在不安全的客户端上运行木马程序或控制客户端，导致数据泄露或者被篡改；另一方面，由于云服务提供商对数据存储所采取的隔离防护措施不当或策略失效，云服务平台也可能被非法用户访问，导致数据被篡改甚至丢失。

三、云数据面临的安全威胁及应对策略

数据安全指的是通过一些技术或非技术手段来保证数据访问受到合理控制，并保证用户数据不被窃取、修改或删除。以下将从传输安全、存储安全、数据残留、数据审计等四个方面阐述数据安全策略。

1）传输安全

通常情况下，企业数据中心保存有大量的企业私密数据，这些数据往往代表了企业的核心竞争力，如企业的客户信息、财务信息、关键业务流程等等。在云计算模式下，企业将数据通过网络传递到云计算服务商进行处理时，面临着几个方面的问题：一是如何确保企业的数据在网络传输过程中严格加密，保证数据即使被窃取也无法还原；二是如何保证云计算服务商在得到数据时不将企业保密数据泄露出去;三是在云计算服务商处存储时，如

何保证访问用户经过严格的权限认证并且是合法的数据访问，同时须保证企业在任何时候都可以安全访问到自身的数据。

数据安全防护策略是：数据传输中采用端到端的数据加密技术，保证重要数据信息不被窃取、监听、篡改，并且通过网络协议栈各个层次的加密技术，如 IPSec、SSL 等加密协议进行传输加密。目前保障数据传输安全的主要方法是数字签名和数字证书，这都属于数据加密。比较流行的加密算法主要有对称加密和非对称加密等，例如以 AES 等为代表的对称加密因为速度较快而被普遍应用于大数据传输，却无法实现签名功能，安全性低；以 RSA 为代表的非对称加密可以用来完成密钥分配、数字签名等功能，安全性高，但非对称加密在处理大量数据时耗时较多，所以不适合大规模数据加密。而把这两种加密算法结合使用（如涉及机要数据的云计算采取非对称加密，而大数据量云存储采取对称加密）则可以在很大程度上提高云计算安全。

2）存储安全

企业的数据存储是非常重要的环节，其中包括数据的存储位置、数据的相互隔离、数据的灾难恢复等。 用户把私有数据外包给云计算服务器，也就意味着失去了对数据的物理控制途径，数据在云服务器中经历了哪些操作，用户也不得而知。云计算平台在高度集合的云存储服务中心内，按需分配一定量的存储空间给用户使用，但实际上用户并不知道自有数据被放置在哪个国家、哪一服务区域。在这种数据存储空间共享的模式下，虽然使用了数据加密机制，但是云平台如何保证各数据区间的有限隔离性。同时，云端的存储数据在用户不知情的情况下有可能被第三方监听，甚至遭受黑客的恶意攻击，数据信息可能存在被非法访问和使用的问题。

传统的企业信息系统搭建在企业内部数据中心，可以通过防火墙来保证数据安全。但云计算中数据可能被存储到非常分散的地方，使得数据泄密的风险大大增加。尽管目前在公有云平台还没有很好的数据隐私解决方案，但是企业可以选择构建私有云或者混合云的方案来解决数据隐私问题。无论私有云部署在什么地理位置，企业都拥有完全的 IT 资源控制能力。通过网络控制和独享的防火墙保护，私有云上的企业数据能够得到和传统 IT 架构下企业数据相同级别的安全保障。

云计算系统中，广泛采用的是“多租户”架构（Multi-Tenancy），所有企业的用户数据都共享在“云”中，通过三种架构可以帮助解决数据隔离问题：

a. 共享表架构：即所有软件系统共享相同的数据实例和数据库表，只是通过一个特定的字段来标示数据的从属关系。这种架构的优势是最大化利用了数据实例的存储能力，因

此硬件成本低廉；劣势是大大增加了业务逻辑的复杂程度，导致容灾备份成本较高。

b. 分离数据库架构：即每个软件系统拥有单独的数据库实例。与共享表架构相反，这种架构能够高效实现数据隔离和容灾备份，但是硬件成本也相应高昂。

c. 分离表架构：即软件系统只共享相同的数据实例，但每个客户都拥有自己的一系列数据库表。这种架构是一种折中方案，实现数据隔离和容灾备份相对共享表架构要容易一些，并且硬件成本相对分离数据库架构要低。

3）数据残留

数据残留是数据在被以某种形式擦除后还会有所残留，数据被擦除后可能留有一些物理特性使数据能够被重建。因此，数据残留更有可能会使得一些敏感信息被无意中泄露出去。云服务提供商应能保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除，无论这些信息存放在硬盘上还是在内存中。SNIA（Storage Network Industry Association）标准组织有关于这方面的研究，例如通过销毁加密数据相关介质、存储介质销毁、磁盘擦拭、内容发现等技术和方法来保证数据的完全清除。

4）数据审计

实际工作中，为了保证数据的准确性和有效性往往会引入第三方的认证机构进行数据审计。在云计算环境下，云计算服务商必须确保不对其他企业的数据计算带来风险的同时，又提供必要的信息支持，以便协助第三方机构对数据的产生进行安全性和准确性的审计，实现企业的合规性要求；另外，企业对云计算服务商的可持续性发展进行认证的过程中，如何确保云计算服务商既能提供有效的数据，又不损害其他已有客户的利益。在实施审计的过程中，还需保证审计机构不泄漏相关企业的敏感数据。

为了保证数据的准确性和有效性，往往会引入第三方的认证机构进行数据审计，在实施审计的过程中，还需保证审计机构不泄露相关企业的敏感数据。第三方的审计产品会对双方的业务操作及交易过程执行客观、公正的安全审计，尤其在高度 IT 化的云计算市场环境下，还要求这种审计可以持续地开展。换言之，由独立第三方向业务用户执行监控评估，针对云计算提供商运维管理操作提供的安全审计报告，这对于保证云计算服务必不可少。

四、结束语

云计算是互联网行业发展的一次革命，它在给社会带来创新和变革的同时，对安全问题提出了更高的要求。相信在不久的将来，云计算数据安全问题将会有更加科学的应对策略及完善的解决方案，使每一个互联网参与者都能够真正做到安全、舒适的“云中漫步”。

参考文献：

[1]杨旭.基于云计算的数据安全性研究[J].移动通信,2013,37(09):69-72.

[2]王金红,许倩.云计算环境下的数据安全[J].金融科技时代,2018(08):50-52.