大数据云计算环境下的数据安全

王 勇
杭州瑞检软件科技有限公司 浙江 杭州 310000

摘 要：目前，随着我国大数据模式的不断发展，数据安全存储难的问题已经逐渐展现出来，研究者提出了将分布式数据存储在云环境中，以保证其信息存储安全。但近年来数据外泄问题不断发生，其造成的社会公共安全事故数量居高不下。为此，研究者提出了针对分布式数据的安全加密技术，但根据用户反馈的信息可知，现有的计算机安全存储技术不仅无法实现对网络中安全隐患的高精度辨识，甚至会对互联网安全通信过程造成不良影响。为避免分布式数据丢失或出现异常，提高互联网的安全性与可靠性，本文将在此次研究中，引进云计算技术，以分布式数据为例，设计一种全新的安全存储方法。希望通过此次设计，为我国多个高机密企业运营与发展提供核心技术支撑，进一步优化互联网用户的上网环境。

关键词：大数据；云计算环境；数据安全

引言

云计算技术的快速发展与广泛应用不仅是信息化时代的必然产物，更为社会发展提供了有效的助力。但数据安全问题也随之而来，从而给云计算的发展造成了严重的负面影响，在此背景下，构建数据安全防御体系就显得尤为重要。文章从云计算技术简述与发展为切入点，分析了云计算技术的主要特征以及数据安全属性等问题，提出了几点基于云计算技术的数据安全防御措施。

1 大数据和云计算概述

大数据一般是指在有限时间内难以利用常规工具或是信息化软件，对大量的目标数据及相关信息完成采集、整理和分析的数据集合。大数据技术是指必须凭借分布式云存储、分布式数据库和高性能超算系统对巨大规模的结构或非结构数据进行传输存储、规则定义、计算挖掘的新型数据处理方式，科研中的生物基因组学、日常生活中的天气预报就是大数据技术的具体应用。大数据技术突破了以往人们对于数据及信息采集、整理、分析的固有思维，具有超越传统数据处理类软件的实践能力，实现了对海量数据及信息高效准确地收集、整理、分析，并且可以结合其他现代信息技术来实现数据及信息的可视化，有助于数据及信息分析结果使用效率的提升。云计算属于一种基于虚拟化网络、分布式储存、并行处理、负载均衡、冗余技术的分布式计算处理技术。云计算技术依托于庞大但无法可视的储存介质，即支撑此项技术的是计算资源共享池“云”。通过诸多计算资源整合，利用计算软件实现自动化管理应用，使计算资源可以快速转化为可应用且具有价值的资源，例如，用户需要大量数据时可通过付费在“云”中获取资源，用户所投入成本较少，但能够迅速获取强大的计算能力支持。云计算技术是信息时代又一重大突破和飞跃，其核心可将许多软硬计算资源统筹整合在一起，使用户参与网络活动时能够获取充足的资源支持，且获取资源不受时间、空间限制。

从技术应用角度分析，实现大数据和云计算的技术虽有不同，但大数据应用中由于处理的数据体量大且十分复杂，含有结构数据、半结构数据、非结构数据，必须采取分布式硬件和软件架构，因而必须依托云计算的分布式计算模式，完成数据上传、存储、加工、计算等操作。

2 云计算技术的主要特征

云计算技术有效地结合了传统分布式计算思想与技术，能够为广大用户群体提供相应的数据服务，促使广大用户能够根据自身的实际需求选取相应的云计算资源。云计算技术能够按照工作量的实际情况对资源进行动态分配，与此同时可以根据服务平台中的资源变化现象做出及时的响应，为广大用户提升了信息数据利用效率。云计算技术的主要特点表现在以下几个方面。

2.1 按需服务与弹性服务特点

云计算技术按需服务与弹性服务的特点主要指通过服务的形式，在客户端提供满足广大用户需求的基础设施、计算机程序以及数据存储等众多资源，与此同时能够根据用户的自身需求特点进行科学、合理的资源分配活动。

2.2 资源透明化与池化特点

从云计算技术提供商角度而言，相关的网络、存储与计算等底层资源原有的异构性被有效地屏蔽，从而促

使各种资源在一定程度上解除了传统的束缚，进而实现了信息资源共享，最终实现了资源池的统一管理。在此模式的基础之上，云计算技术充分利用自身所具有的虚拟技术，能够将信息资源有效地分享给有多样化需求的广大用户，在此过程中，所有资源的分配与管理都比较透明。

2.3 高可靠性与高扩展性特点

云计算技术的应用有效提升了信息数据的存储与处理能力，从而可以灵活、迅速以及安全地满足广大用户的多样化需求。这项服务功能的实现前提必须是由强大的基础技术架构作为重要支撑，基础技术架构必须具备高弹性与大容量的重要特点，并在实际运行的过程中具备能够及时与快速处理故障的能力。因此，只有具备科学、完善的用户管理与安全管理措施才可以充分确保云计算技术的健康、可持续发展。

3 云计算平台面临的数据安全问题

3.1 隐私安全问题

云计算平台通过网络向用户提供弹性可变的IT服务，包括用户属性信息、身份信息、行为信息等。在核心软硬件设备对海量大数据进行读取、存储、分析、应用的过程中，易造成用户隐私泄露。云端系统需要用户采用账号登录，只有确保使用者身份的合法性，系统才能提供相应服务。但云计算平台存在配置错误、操作系统漏洞等问题，用户在云计算服务提供商处上传数据资料后，失去了对数据资源的控制，再加上密钥管理机制不完善，密码技术正确性、合规性、有效性得不到保障，导致身份认证机制易产生风险隐患，会出现对资源的越权访问现象，或通过网络窃取用户信息。隐私信息保密性是云计算平台的首要问题，会严重影响信息资源的所有者隐私数据安全。

3.2 面向大数据的云计算安全问题

大数据分析技术可以保护数据，并防止入侵者访问数据。大数据安全问题包括4个方面：一是保护大数据；二是为大数据分配和取消分配磁盘存储空间；三是维护公共云中大数据的日志文件；四是防止未经授权用户的访问。

为了有效保护大数据，云服务提供商在开发安全系统的过程中，需要维护数据的完整性、保密性和可用性。加密技术是云计算中常用的一种技术，它可以保证数据的安全，保护数据的机密性，防止因授权和未授权数据计算而造成的数据丢失，并使授权用户可以使用数据。

3.3 大数据和云计算的网络系统稳定性有待提升

在大数据和云计算环境下，云体系内部的存储网络和业务网络结构更为复杂，功能模块更丰富，数据计算平台系统所暴露的安全风险点也更多，例如，网络系统通信管理功能存在漏洞，若用户使用电子邮件进行工作学习时，出现功能管理漏洞、弱口令漏洞、钓鱼风险，则黑客可能利用此类漏洞风险针对用户数据进行入侵，盗取信息或删除用户邮件。而在以往的单机计算机中，数据的传输存储、分析加工、共享应用都是在单个节点下完成，计算机系统安全性将影响用户数据是否完整、真实、安全。在大数据和云计算网络环境下，用户信息和计算数据托管在第三方云端，用户使用数据时，云端网络安全技术水平直接影响云计算应用的可靠性。因此，有效实现网络安全技术已然成为提升大数据和云计算网络系统稳定性的关键。

4 大数据云计算环境下的数据安全措施

4.1 确保基础设施的安全性

在云环境中，网络黑客与恶意用户会对数据信息进行更为猛烈的攻击，因此，应当对数据信息进行实时监控，及时对各种漏洞进行全方位修补，建立更为完善与全面的实时数据监控制度，从而有效地抗击外部攻击给数据安全带来的负面影响。例如，可以针对黑客入侵研发与提升相关的检测技术，运用检测技术对主机、网络或是各种违规操作进行全面检测，并能够及时修补安全漏洞。与此同时，还应当着重提升系统自身的定期病毒扫描功能，从而全方位查找安全漏洞，并进行及时的修补与提升。除此之外，还应当构建多个实时数据处理中心，从而在云环境或是传统网络环境中都可以充分确保信息数据的安全性。由于数据安全不仅会遭受外界攻击的风险，还会遭受突发风险，例如不可抗力的自然灾害或是突发断电等情况，都会导致云数据中心停止运行，从而导致数据服务中断。因此，应当构建多个实时数据处理中心，并将区域进行合理区分，避免在同一供电或地理区域当中，从而有效确保数据的安全性。

4.2 数据存储加密

云计算平台管理层大量采用分布式存储和集群管理技术，提供数据分块存储、数据加密、密钥管理、建立数据索引、数据加密、密钥管理，制定有针对性的技术来降低安全隐患。数据分为动态数据和静态数据。文档、报表等不参与计算的数据为静态数据，参与计算检索的数据为动态数据。数据加密机制可利用DES、IDEA、RSA、RC5、RC6等加密算法对数据进行加密。密钥管理方案可采用分层密钥管理、公私钥管理。分层是“金字塔”式密钥管理体系，这种密钥管理只需将顶层密钥分发给数据节点，数据节点只需保管少数密钥就

可对大量密钥加以管理，数据需要对应私有密钥才能解密。用私有密钥加密数据，要有对应的公开密钥进行处理才能完成解密。密钥保护技术通过传送保护、注入保护、存储保护、使用保护等方式将用户数据置于一个加密的状态，强化云服务在用户隐私以及数据方面的安全性。云计算平台采用加密传输密钥的认证管理方式，解决了数据传输过程保密性问题。密钥除了需要进行认证，还要进行统一管理，它是数据加密的核心部分，负责密钥的生成、分发和销毁。密钥在KMS中一般可以分为三级：三级密钥负责对数据进行加密，二级密钥加密三级密钥，一级密钥也称为根密钥，加密二级密钥，用以提高密钥保护的安全性，降低密钥管理成本。云计算技术的核心价值在于数据分析和利用。云平台海量数据催生了大规模分布式采集、存储模式，不可避免增加了数据安全风险。因此，需要完善的数据加密、身份认证、数据完整性保护等安全机制来解决数据丢失、数据损坏、数据泄露等问题。在管理机制中，对用户的身份认证是数据库管理系统向用户提供的外层安全保护措施，输入ID和密码后，系统审查核实用户身份。数据库系统要对每个用户定义存取权限，进行访问控制，保证用户只能存取有权存取的数据。数据库审计可对用户操作机制进行监视和记录。审计机制可记录用户操作、跟踪的信息，追究有关责任，消除安全方面的隐患和漏洞。要根据云计算平台数据特点及应用需求，记录一切与系统安全有关的活动，严格控制数据挖掘操作权限，防止信息的泄露。

4.3 加强网络安全环境监管

网络安全环境监管是大数据和云计算下网络技术有效实现的必要内容，对于管控用户网络行为、净化网络生态环境、保障用户数据安全具有不可或缺的作用。加强网络安全环境监管需要依赖政策法规提供顶层支持，严肃处理破坏网络安全环境的违法分子，引导用户规范用网、依法用网，共同营造健康、和谐的网络安全环境。与此同时，要在网络安全监管技术方面加强、加快创新和应用，既要充分运用第三方网络服务商业机构自我规范，持续改善网络环境，切实保障网络安全，减少网络问题出现，又要利用拥有不可篡改性的网络安全技术和信息管理技术严格监管数据资料动向，保障用户数据资料安全。

结束语

综上所述，计算机网络技术在电子信息工程及相关系统中有着较高的应用价值。同时，在当前的电子信息工程建设与发展中，计算机网络技术的应用范围与场景相对较广，依托两者的联合发展，推动电子信息工程发展提速，实现信息资源和数据的快速共享，提升信息资源以及数据传输的质量与效率，助推新型设备的持续性开发与升级。

参考文献

[1]胡会南，李秀丽.基于云计算技术的数据安全防御体系建设[J].通信电源技术，2022(1):183-185.

[2]谭可，乔雷，秦怡，等.大数据云计算环境下的数据安全分析[J].通讯世界，2022(4):40-42.

[3]张莲蓉.云计算中数据资源的安全加密机制[J].电子技术与软件工程，2022(5):29-32.

[4]刘晓东.大数据云计算环境下的数据安全问题与防护举措探究[J].物联网技术，2022(7):77-79.