大数据云计算环境下的数据安全分析

秦世炜　安吉元　马　玥
北京太极信息系统技术有限公司　北京　100012

摘　要：在当前形势下，我国人民的所有信息都在大数据计算环境下的发展下被一步步的数字化。信息被数据化固然有优势，这不仅证明着我国信息化水平越来越高，也将各种各样的资源以数字化的方式去呈现，更加简洁和便利。但很多情况下，大数据都会存在一些安全隐患，导致人民的信息数据流失，所以大数据不能只顾一味的开发，增添新的功能，最重要的是要采用合理的挖掘技术来保证群众个人信息的安全。

关键词：大数据；云计算；数据安全

1 大数据云计算介绍

作为一种新的计算模式，大数据云计算是分布式处理、网络存储、负载均衡、并行处理、虚拟化等传统计算机技术和网络技术发展融合的产物。大数据云计算将计算资源分布在远程大量计算机组成的资源池上，计算机和存储系统可以由用户根据自己的需求来链接。用户利用这些“大数据云”通过终端接入数据中心，按照自己的需求进行计算。大数据云将无数多台计算机整合成一个具有强大计算能力计算机系统是通过虚拟化来实现的，并且借助iaas、paas、saas等先进的服务模式，将这些强大的能力分散到用户手中。通过不断提高“大数据云”的处理能力减少终端用户的负担，这是大数据云计算的核心优点[1]。

2 大数据云计算的特点

2.1 比较低的成本获得很高的处理能力

通过分布式处理、网络技术、集群技术等设备联合在一起工作，这是大数据云存储的特征。用户可以通过大数据云将终端与idc相联，通过统一的应用程序登陆大数据云来获取资源。通过大数据云，大量的资源可以以非常快的速度获得信息，人们可以因此而突破资源限制。

2.2 采用虚拟技术，管理灵活，使用方便

大数据云通过软件或人工管理将计算资源联合起来，用户能够在任何地点和时间登陆大数据云。用户无需关心资源在哪里，只需要通过虚拟平台将要求交给大数据云同时自由使用资源，大数据云就返回用户所要的结果。在这个反馈机制里面，用户随时可以通过一个终端获取需要的服务和资源，因此对于计算机硬件要求不高，使用起来也非常方便，大量降低了用户成本[2]。

3 大数据云计算的优势与重要性分析

3.1 投入成本低，资源覆盖广

传统的计算机处理技术需要投入高昂的资金成本，大数据云计算技术集成了最新的计算机网络技术，将所有的数据信息集中到一个系统平台中，方便用户处理个人信息。大数据云计算在对数据进行操作的时候是联合多种计算机技术进行集中工作，打破了资源的限制，提高了用户的资源查找效率，降低大量的时间、运营成本。另外，云计算属于一个大型的资源池，可以实现大量计算机资源共享，云计算采用网络的连接方式，客户通过网络获取计算机资源中的信息，规模庞大，覆盖范围广。

3.2 管理方便，操作灵活

大数据云计算的一项关键技术就是虚拟技术，利用互联网来连接所有的数据资源，然后借助相应的数据管理工具来对数据进行管理，这样可以节约用户的时间。在对数据的实际应用过程中，大数据云计算环境下的数据信息具有动态性，可以按照实际情况进行伸缩，还可以借助虚拟技术，抽象化底层架构，实现云统一管理与应用[3]。在对数据资源进行操作这一过程中，用户只需要将资金的实际需求提供给大数据云计算平台就可以得到自己所需的结果，操作简单，用户不需要关心除了结果以外的任何信息，用户只需要为自己所需要的内容进行付费，有效降低运营费用。除此之外，大数据云计算环境下的虚拟技术，对硬件要求也很低，操作灵活方便，可以降低实际用户成本。

3.3 大数据云计算环境下数据安全重要性分析

大数据云计算环境下的数据安全问题是由于网络开放性、共享性等特征所导致，加上我国的计算机网络技术起步较晚，发展较快，很多设施都不完善，尤其是网络安全防御机制，这就导致网络安全问题频发，制约了计算机网络技术的普及。大数据云计算作为新型的计算机技术，整合了传统计算机技术与分布式技术、虚拟技术、网络工程等，具有超强的计算能力，可以对海量数

据进行筛选、分析，给人们提供了很大方便，因此数据安全问题就显得尤为重要[4]。

4 大数据云计算的安全问题

4.1 数据访问安全

数据在云计算系统中的资源安全问题本质上是一个数据访问控制问题，主要表现为用户非法访问数据，这种威胁包括两类，即内部威胁和外部威胁。当一个用户应用大数据技术将数据托管到云平台，或将数据存储在远程服务器中，云计算服务提供商可以优先获得数据或应用程序，如果内部人员失职，没有建立安全防护系统，系统会出现黑客攻击或崩溃瓦解等问题，导致用户数据丢失。在一些极端的情况下，内部人员违反安全规定，没有按照要求实施数据安全管理，数据计算、储存等其他操作也未在标准条件下进行，甚至有管理人员销售用户数据，这些问题都将严重影响大数据云计算环境下的数据安全，如何限制用户的数据访问权限和管理权限，提高用户对大数据云计算技术使用信心、加速相关技术发展是需要解决的一个重要问题[5]。

4.2 数据隔离存在的安全隐患

数据隔离安全隐患是大数据云计算环境下数据共享操作出现的安全隐患，主要是企业机构等集体性用户。随着科学技术的快速升级，大数据云计算技术从起初的企业、政府等领域开始拓宽，深入应用到各个领域，数据隔离安全问题越来越严重。尤其是企业机构在运营中资源是共享的，因此要保证数据资源的流动性，资源流动性越强，数据加密程度就越弱。如果在外部做不好数据隔离，就会给黑客提供攻击的机会，损坏信息资源，导致信息泄露等。这里需要注意的是，共享的资源是一对一的，但是目前缺乏完善的隔离体系，会导致第三方可以查阅，这就会造成大数据云计算出现严重的隔离问题，从而影响数据的安全。

4.3 数据被销毁或被容灾

大数据云计算环境下，数据需要经历一个较为复杂的操作过程，一些数据被读取和使用之后，必须要进行销毁处理，避免被其他用户访问。作为数据处理的最后一个环节，数据销毁尤为重要，如果无法在终端进行完全销毁，那么数据就可能被盗取、泄露。在大数据云计算环境下，数据销毁环节的处理对象比较大，有时一个销毁过程需要耗费十几分钟的时间，这就会导致在数据销毁的过程中，出现数据被窃取问题，或是大批量数据销毁不彻底，导致应被销毁的数据被其他用户非法恢复。从根本上来讲，数据被销毁或被容灾的原因在于销毁过程耗时过长，以及数据销毁不彻底，存在数据残留问题[1]。

4.4 病毒查杀清理不到位

在当前很多的安全隐患中，病毒查杀的清理也是很大的一个问题。一些工作人员对病毒木马的查杀做的不规范，经常容易疏忽，导致一些病毒的出现，从而影响了大数据云环境下的数据安全。而且在大数据中一些数据隔离问题，也存在一些安全隐患。例如在大数据云环境中，政府和企业部门都会经常采用云计算的方式来统计信息数据和资料。那么在一些过程中，对于数据的保存和传输的过程中没有做好数据的隔离防护，数据信息的加密处理没有到位。这就会导致一些病毒侵入到系统中，从而使数据的保密性和安全性失去了保障。在一般的传输过程中，一般系统都会有自动备份的功能，或者云盘一类的功能。目的是为了防止数据因不小心误删存留的备份，但这又给一些不法之徒带来了一些“机会”[2]。

5 大数据时代云计算环境下数据安全相关对策分析

5.1 完善互联网防范系统

为了使我国的信息数据在大数据云环境下能够更加安全和完善，通过严谨的分析和调查，研究出了一些安全防范策略。首先就是要将数据防范的安全体系切实的深入到每一个群众当中，让他们的个人信息能得到合理的保护。对于用户的身份认证技术是最基本的安全防范，同时也是最好的保障。身份认证系统一般可以通过手机号、身份证号、人脸识别、指纹识别的方式来给个人信息数据进行加密。为了使人民的信息数据可以更加的安全，在后续提升中可以继续采用更细化的认证识别系统。比如生物特征识别，采用本人眼睛的虹膜识别、身体内的静脉和DNA这些独特又无法复制的数据来进行信息安全的保护。在一些相对更机密的单位企业都会采用这种方式，可以在日后的完善中将这项技术应用到每家每户，从而保障信息数据的安全[3]。

5.2 做好身份认证，强化访问控制

大数据云计算环境下，网络系统、应用程序等服务范围都会扩大，很多权限都被分散，云平台呈现出来的数据库包含了每个人都可以使用的数据，很难对其进行控制，这就使得信息管理与控制模式之间存在巨大的困难。这就需要做好身份认证来对终端用户进行鉴别，完善身份认证技术，将个人信息与常用终端进行绑定，并进行网域划分，做好系统访问权限设置，针对账号进行管理，确保账号安全登录。除此之外，还要强化数据访问控制，尤其是大数据云计算环境下，针对复杂的环境就要强化访问控制措施，以便于更好地开展维护控制工作。

大数据云里的数据是共享的，大数据云却是虚拟

的，大数据云用户的控制已经无法满足大数据云的安全性，因此要和网络安全技术相结合，通过密码技术来保证书的安全。同时，大数据云还需要做一个统一的全局的身份认证技术，通过这个身份认证技术实现统一的和用户身份管理，同时通过用户身份管理统一访问管理，增强大数据的安全性能。

5.3 完善病毒防御系统

完善病毒防御系统可以很好的阻碍在大数据云环境下数据安全中会发生的问题，主要是因为我国内部的病毒防御系统没有做到很好的完善，才使黑客有机可乘，从而获取了一些重要的信息数据。病毒的防御系统不能只用于数据库中，应该在任何部门任何区域都加密，保证病毒不会从任意区域来盗取内部的重要信息。在内部，可以多安装一些查杀病毒软件来防止病毒的侵袭，和电脑中的360安全管家查杀病毒的方式大同小异[4]。但安装查杀病毒软件以后，还要进行定期的检查和清理。相关技术人员在每一次的检查和清理时，都要做好对应的检查和记录，将每一次的发现漏洞和解决方案都有一个完整的工作记录，在后续相似问题出现时也可以减少一部分的工作量，直接按照此次方法解决加密即可。防火墙的正确应用也可以阻止一些黑客侵犯企业内部的信息，完善的病毒防御系统应该是像一个完整的保护罩一样，把所有的信息都能保护的很好。通过这种方式来阻止各个不法分子的攻击，给大数据云计算环境下的数据建立一个盔甲，保护所有信息都能安全的传输和分享。

5.4 优化大数据云计算环境下的数据加密技术

大数据云计算环境下，数据信息都具有社会公用属性，用户无法确定数据是否被保存妥当。因此在进行数据共享的时候要对其进行加密处理，用户先对数据进行加密，然后将加密过的数据信息发送到云数据中心，使用者利用密钥来对其进行解密处理，从而增加数据信息的安全性。常见的数据加密方式有属性基加密，在密文中增加用户信息和时间信息，用户可以打印不同时间段的日志[5]。

5.5 审计措施和相关的监控措施

当用户准备把自身积累的数据提交给大数据云时，用户必须要把验证交给具备专业技术和安全保护措施的第三方认证。相关的专业第三方必须拥有一套属于自己的全面的技术评估体系，这套评估体系里面对于大树君云中的负荷管理、软件配置、服务器等进行安全测试和实时监控，在实时监控的过程当中一旦发现问题，就会实时报警，以便于能够随时有效的应对出现的问题并且进行妥善的处理。

结语

总而言之，我国的信息技术虽然在不断的改正和更新换代，但对于信息数据的安全保障方面，还有待提升。在防范策略方面，可以采用完善互联网防范系统、完善病毒防范系统、加强数据监管力度三个方面来进行我国信息数据的安全保障。虽然在大环境下的云计算为人们的生活和工作都提供了很多便利，但还是存在着一些等待完善的安全隐患，所以相关技术人员要对此事引起高度重视。保证人民的信息安全不再受到损害。

参考文献

[1]陈雪娟.大数据云计算环境下的数据安全[J].电子技术与软件工程,2021(02):245-246.

[2]苗莉.大数据云计算环境下的数据安全[J].科技资讯,2021,19(02):31-33

[3]王凤领.大数据云计算环境下的数据安全分析与对策研究[J].网络安全技术与应用，2020（06）：88-91.

[4]刘恩军.大数据云计算环境下的数据安全分析[J].网络安全技术与应用，2019（05）：56-58.

[5]何强胜.大数据云计算环境下的数据安全研究[J].轻纺工业与技术，2020（1）：87-88.